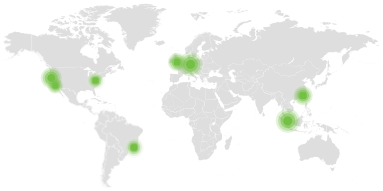


2022

APT Annual Landscape Report

Table of Contents

1. Executive Summary

In 2022, under the influence of factors such as the global economic downturn, the outbreak of geopolitical conflicts, and the sluggish cryptocurrency market, advanced threat events will show an overall trend of outbreak. In terms of the number of active groups, the number of attack incidents, the number of new attack tools, and other key indicators of advanced threats, this year's data performance is far higher than in previous years.

This year, NSFOCUS Fuying Lab conducted continuous observation and exploration of three representative advanced threat areas: cyber warfare threats, long-term APT threats, and ransomware threats dominated by civilian attack forces.

Cyber-attack capabilities have become a weapon resource capable of playing an important role in geopolitical conflicts. At various stages of the Russia-Ukraine conflict, Russia and Ukraine have carried out various cyber-attacks in cyberspace with the goal of stealing secrets, controlling and paralyzing them.

Cognitive confusion and control of public opinion have become an important part of cyber warfare. In the Russia-Ukraine cyber war, there have been a large number of cyber-attacks aimed at deceiving perceptions or inducing public opinion, such incidents have polluted the network information flow with a large amount of false information or partially wrong information by controlling propaganda platforms or abusing propaganda channels, so as to build a speech atmosphere favorable to the attacker's side.

APT attacks are more deeply tied to geopolitical conflicts, and the intensity of APT activities in conflict areas and sensitive areas such as Eastern Europe, South Asia, and the Middle East continues to increase. Regional APT groups that remained active this year include Gamaredon, Kimsuky, Lazarus, Patchwork, etc., reflecting the increased attention of relevant countries to conflict areas against the backdrop of increasing international tensions.

This year, China suffered a large number of APT attacks and extortion attacks, mainly from the United States, Vietnam and India. Most of these APT groups target Chinese universities and large enterprises and use N-day vulnerability exploitation or social engineering to invade organizations or facility targets and steal intelligence.

This year, the RaaS (Ransomware-as-a-Service) model in the ransomware field continued to develop rapidly, and major ransomware gangs began to enter a stage of more fierce and vicious competition. Smaller ransomware gangs are constantly trying to expand their influence by attacking large enterprises, and larger ransomware gangs are struggling to maintain their dominance due to homogeneous competition. Ransomware threats are returning to their earlier chaotic and dangerous state.

2. Cyber Warfare Threats

2.1 Overview

This year, with the outbreak of the Russia-Ukraine conflict, a highly intense and long-lasting cyber war has gradually been recognized by the public. Led by the cyber forces of Russia and Ukraine, as well as the organizations of both sides, the cyber war between Russia and Ukraine has become a large-scale high-level threat incident involving multiple forces such as state forces, APT groups, ransomware groups, civil hacker groups, and individual attackers, which has affected the operation of Russian and Ukrainian organizations and institutions, international public opinion, and even the direction of the war to varying degrees.

NSFOCUS has been paying close attention to the cyber war between Russia and Ukraine since the beginning of its preparations and has exclusively disclosed a number of cyber warfare-related APT attacks, DDoS attacks and attacks by non-governmental hacker groups in the process of continuous monitoring and research and has reported and analyzed the form and composition of modern cyber warfare from different perspectives from macro to micro. 123456

In this cyber war, the cyber forces of Russia and Ukraine have not only adopted a variety of attack methods such as cyber espionage, data erasure attacks, and denial-of-service attacks, but also flexibly adjusted their roles and positioning as the war situation changes and even began to take the lead in sabotaging facilities, manipulating public opinion, and creating panic.

The occurrence and development of cyber warfare between Russia and Ukraine shows that cyber warfare has become a strategic weapon that plays an important role in geopolitical conflicts, providing an important case study of cyber warfare for countries around the world, and has had a profound impact on the concept, method and status of cyberspace warfare, prompting countries to continuously strengthen cyber security defense and strengthen military operations capabilities in cyberspace.

2.2 Timeline of the Russia-Ukraine Cyber War

On February 24, 2022, the military conflict broke out in the Ukrainian region, and the contest between Russia, Ukraine and various behind-the-scenes forces attracted the attention of the world. As events unfolded, this real-world conflict affected all aspects of cyberspace for the first time ever. Based on the research results of NSFOCUS's global threat hunting system and threat hunting system, NSFOCUS Fuying Lab sorted out the cyber conflicts that occurred in Eastern Europe and sorted out the following timeline:

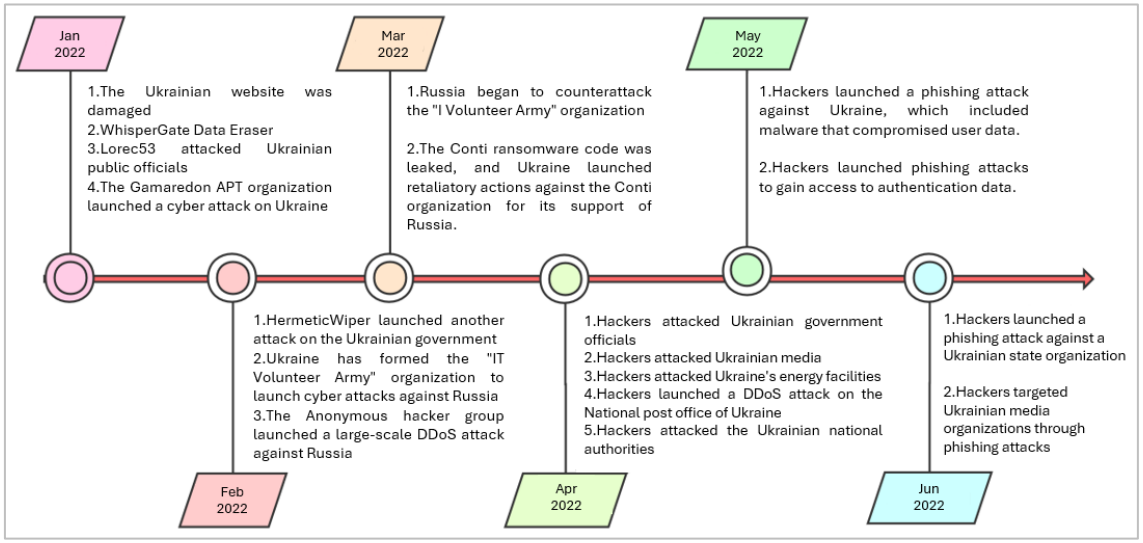


Figure 2.1 Timeline of the Russia-Ukraine cyber war

[1] http://blog.nsfocus.net/apt-lorec53-20220216/
[2] http://blog.nsfocus.net/cldap-ntp/
[3] http://blog.nsfocus.net/itw-privatbank/
[4] http://blog.nsfocus.net/it-ddos-31/
[5] http://blog.nsfocus.net/atp-whisperga-mbr/
[6] http://blog.nsfocus.net/ddos-apt-sec/

From the end of 2021 to the beginning of 2022, the situation between Russia and Ukraine was still unclear, and pro-Russian APT groups such as Lorec53 and Gamaredon who were active during this period played the role of cyber scouts, extending their tentacles to Ukraine's military, government, and enterprise fields, covering a more comprehensive area, collecting information such as the real network address, network resource situation, network topology, sensitive information storage location, and operation mechanism of high-value systems of the target network facilities.

Since April 2021, groups such as Lorec53 and Gamaredon have begun to target targets other than military units, attacking Ukrainian government departments, military targets, diplomatic departments, media and other individuals who may have high-value intelligence on Ukraine. It is clear that the Russian APT group of this period focused on the strategy of casting a wide net, actively collecting all intelligence that would be beneficial for subsequent military operations. The cyber espionage activities of the Russian APT group in Donetsk, Luhansk and other eastern Ukraine can be seen as part of the cyber special operation carried out by the Russian side with the goal of stealing secrets.

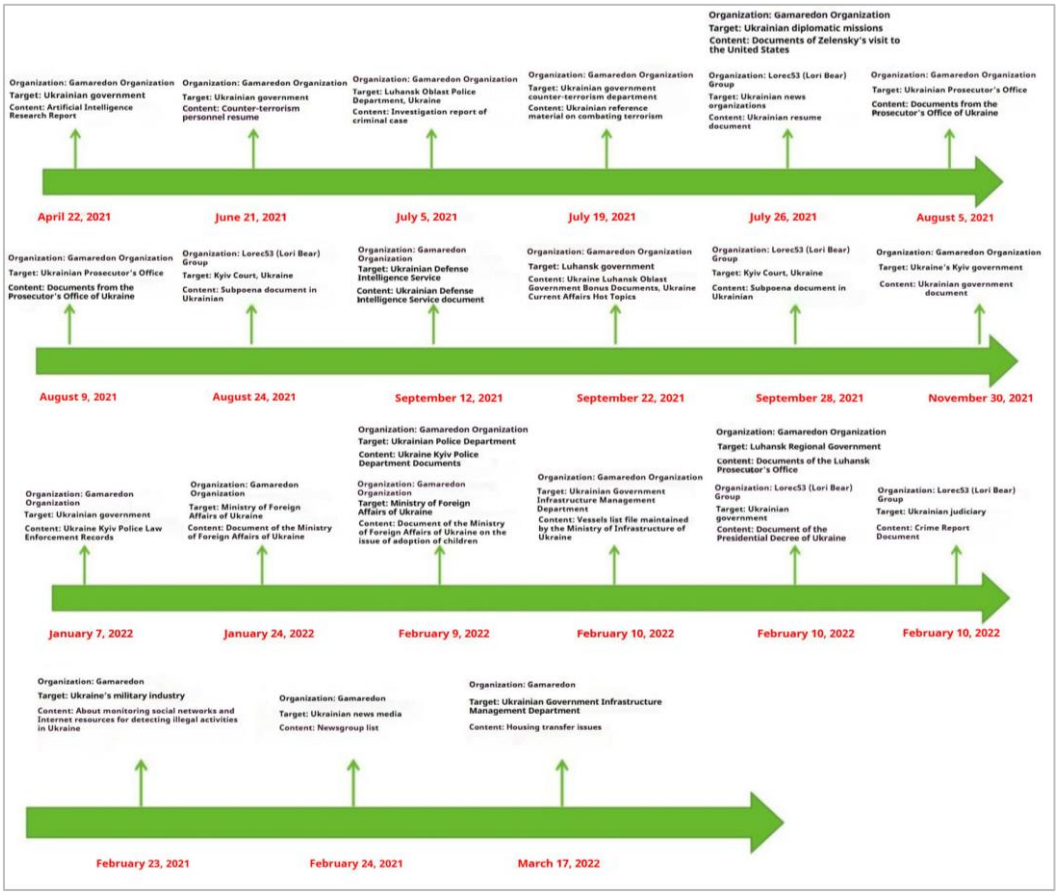


Figure 2.2 Timeline of the operations of the Russian APT group in the early days of the war

When the conflict between Russia and Ukraine officially broke out, the APT groups affiliated with Russia and the cyber forces affiliated with Ukraine immediately switched to fierce offensive and defensive confrontation activities and launched a cyber special operation with the goal of control. A typical case at this stage is that Russia and Ukraine have played up the atmosphere of war in an all-round way through online forums and offline media, emphasizing the invasion activities of one side against the other. By blocking media broadcast channels, controlling the world's discourse, and exaggerating the atmosphere of bullying the weak with the strong, military activities are defined as invasion attacks, occupying the commanding heights of public opinion. Through the control of public opinion, the attacking side is forced to give up the results of the battle, realize the goal of cognitive warfare, and achieve the goal of interfering with and controlling public opinion.

During the ongoing phase of the Russia-Ukraine conflict, pro-Russian APT groups and pro-Ukrainian cyber forces immediately turned into fierce offensive and defensive confrontation activities, typical cases of which were data sabotage activities on the Russian side and DDoS operations on the Ukrainian side. The Lorec53 group has developed a variety of data breaching software called WhisperGate, WhisperKill, WhiteBlackCrypt, and has led a number of destructive cyberattacks against multiple groups in Ukraine. The Sandworm group has carried out a number of data destruction operations against key facilities in Ukraine, such as power facilities, and developed and used a variety of data destruction software named HermeticWiper, HermeticRansom, CaddyWiper, AwfulShred, Industroyer2, etc., covering Windows systems, Linux systems, and industrial control systems.

The Gamaredon group also took part in the data destruction mission in the early days of the war. A type of data erasure software called IsaacWiper emerged in March that was suspected to have been used by Gamaredon attackers to attack an undisclosed entity in Ukraine.

On the other hand, Ukraine quickly took the lead in forming the IT ARMY of Ukraine, a cyber-attack group, after the outbreak of the war, which organized DDoS attacks against Russia. Leaders provided the group with a targeted checklist of 31 Russian critical infrastructure targets, a variety of DDoS attack tools and corresponding educational documents, and DDoS attack infrastructure located in Russia, allowing participants to quickly participate in DDoS attacks on Russia's critical network facilities. The targets of these DDoS attacks include Russian government agencies, three banks, and key Russian industries such as energy, steel, and metallurgy.

In addition, the international hacker group Anonymous also announced that it had joined the Ukrainian side shortly after the start of the war, cultivating and organizing a group of pro-Ukrainian hackers capable of launching cyberattacks in a short period of time. Anonymous organized direct sabotage of Russian online services by hacking databases, blocking Telegram sites, hijacking streaming media, etc., in order to organize the dissemination of Russian speech.

2.3 Russian - Ukrainian Cyber Warfare Participation Groups

Cyber warfare in the Russia-Ukraine conflict is a cyber force supported by the United States and Western countries to assist Ukraine in its game with Russia at the cyberspace level. The cyber forces supporting Ukraine, represented by Anonymous and the IT ARMY of Ukraine, have launched cyber special operations aimed at paralyzing Russia's government, defense, energy, and finance, mainly with DDoS-based attack methods. The cyber forces supporting Russia, represented by Gamaredon, Lorec53, Sandworm, APT29, etc., mainly launched cyber special operations aimed at stealing, controlling, and paralyzing Ukraine by means of data erasure attacks, DDoS attacks, ransomware attacks, and phishing attacks. Other cyber forces include multiple civilian hacking groups and multiple unknown threat actors that emerged during the war.

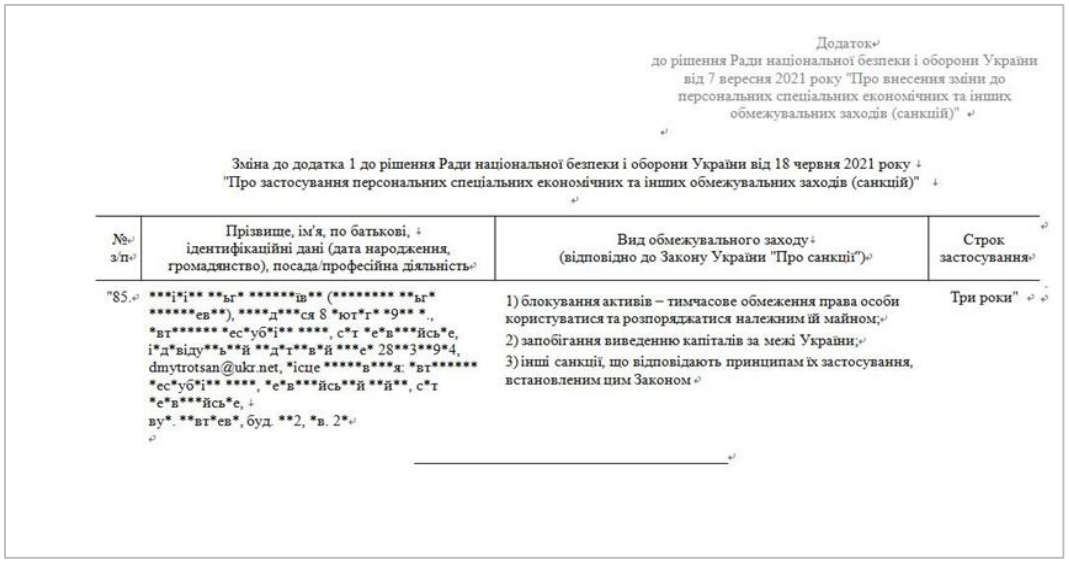
2.4 The Main Types of Attacks in the Russia - Ukraine Cyber War

After analyzing the various types of cyber-attacks that have emerged in the cyber war between Russia and Ukraine, NSFOCUS Fuying Lab found that these attack activities can be divided into three types: secret theft, control and paralysis. Among them, the cyber-attacks of stealing secrets mainly include espionage attacks initiated by APT groups and social network phishing activities initiated by civil hacker groups. Control cyber-attacks mainly include public opinion control cyber activities initiated by state and civil forces on both Russia and Ukraine; Paralyzing cyber-attacks include data erasure attacks launched by APT groups and DDoS hacker attacks launched by hacker groups at all levels.

2.4.1 Cyber Special Operations with the Goal of Stealing Secrets

For a long time, the main task of state-level APT groups has been to monitor specific targets for a long time and continue to collect intelligence, and these APT groups have been responsible for stealing secrets from enemy military targets during the war, collecting as much military intelligence as possible from the enemy through phishing, puddles, etc.

The initiators of Russia's attack on Ukraine are mainly APT groups Gamaredon and Lorec53. For example, Lorec53 launched spear-phishing attacks using personal financial sanctions as bait in the run-up to the war, targeting a wide range of governments and state-owned enterprises in eastern Ukraine. The phishing documents delivered by Lorec53 are used to download the corresponding spy Trojan program and steal various document files on the victim's host.



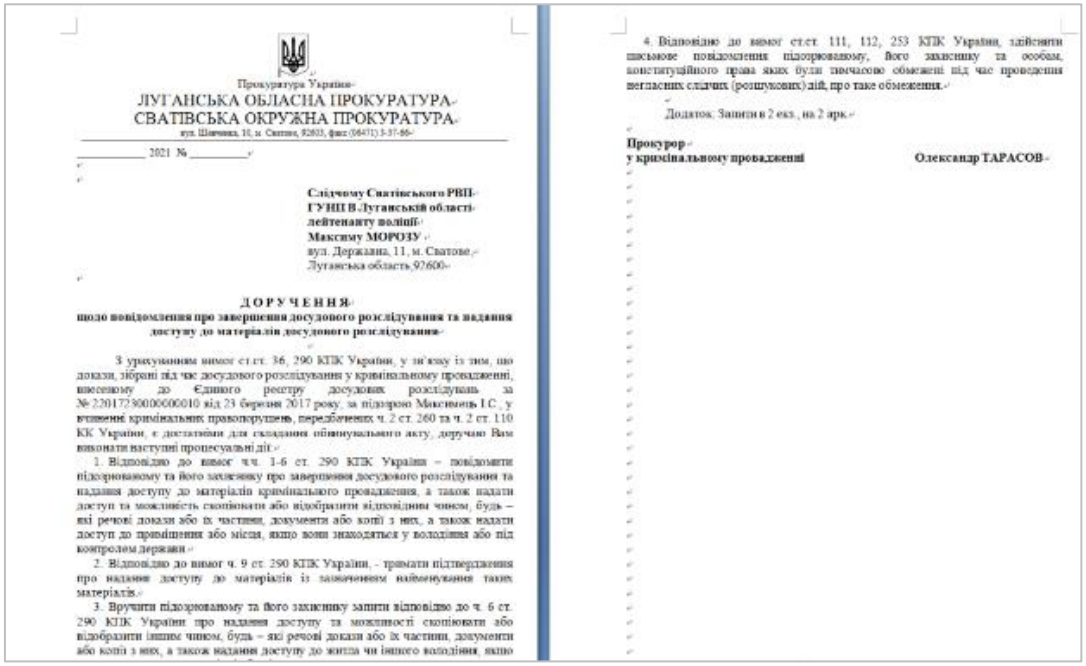
Додаток
до рішення Ради національної безпеки і оборони України
від 7 вересня 2021 року "Про внесення зміни до
персональних спеціальних економічних та інших
обмежувальних заходів (санкцій)"

Зміна до додатка 1 до рішення Ради національної безпеки і оборони України від 18 червня 2021 року
"Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)"

№ з/п	Прізвище, ім'я, по батькові, ідентифікаційні дані (дата народження, громадянство), посада/професійна діяльність	Вид обмежувального заходу (відповідно до Закону України "Про санкції")	Строк застосування
"85.	***і*і** **ьг* ******ів** (******** **ьг* ******ев**), ****д***ся 8 *ют*г* *9** *, *вт****** *ес*уб*і** ****, с*т *е*в***йсь*е, і*д*віду**ь**й **д*т**в*й ***е* 28**3**9*4, dmytrotsan@ukr.net, *ісце *****в***я: *вт****** *ес*уб*і** ****, *е*в***йсь**й **й**, с*т *е*в***йсь*е, ву*. **вт*ев*, буд. **2, *в. 2*	1) блокування активів – тимчасове обмеження права особи користуватися та розпоряджатися належним їй майном; 2) запобігання виведенню капіталів за межі України; 3) інші санкції, що відповідають принципам їх застосування, встановленим цим Законом	Три роки"

Figure 2.3 Phishing documents used by Lorec53

After the outbreak of the war, NSFOCUS Fuying Lab captured a large number of cyber-attack activities using Russian combat information or Ukrainian-language army dispatch information as bait. Most of these activities came from the APT group Gamaredon, which targeted the army, police and local governments in the eastern regions of Ukraine.



Прокуратура України
ЛУГАНСЬКА ОБЛАСНА ПРОКУРАТУРА
СВАТІВСЬКА ОКРУЖНА ПРОКУРАТУРА
вул. Шевченка, 10, м. Сватове, 92603, факс (06471) 3-37-86

_____ 2021 № _____

Слідчому Сватівського РВП
ГУНП В Луганській області
лейтенанту поліції
Максиму МОРОЗУ
вул. Державна, 11, м. Сватове,
Луганська область, 97600

ДОРУЧЕННЯ
щодо повідомлення про завершення досудового розслідування та надання доступу до матеріалів досудового розслідування

З урахуванням вимог ст.ст. 36, 290 КПК України, у зв'язку із тим, що докази, зібрані під час досудового розслідування у кримінальному провадженні, внесеному до Єдиного реєстру досудових розслідувань за № 22017230000000010 від 23 березня 2017 року, за підозрою Максимець І.С. у вчиненні кримінальних правопорушень, передбачених ч. 2 ст. 260 та ч. 2 ст. 110 КК України, є достатніми для складання обвинувального акту, доручаю Вам виконати наступні процесуальні дії:

1. Відповідно до вимог ч.ч. 1-6 ст. 290 КПК України – повідомити підозрюваному та його захиснику про завершення досудового розслідування та надання доступу до матеріалів кримінального провадження, а також надати доступ та можливість скопіювати або відобразити відповідним чином, будь – які речові докази або їх частини, документи або копії з них, а також надати доступ до приміщення або місця, якщо вони знаходяться у володінні або під контролем держави.

2. Відповідно до вимог ч. 9 ст. 290 КПК України, - прийняти підтвердження про надання доступу до матеріалів із зазначенням найменування таких матеріалів.

3. Вручити підозрюваному та його захиснику запити відповідно до ч. 6 ст. 290 КПК України про надання доступу та можливості скопіювати або відобразити іншим чином, будь – які речові докази або їх частини, документи або копії з них, а також надання доступу до житла чи іншого володіння, якщо

4. Відповідно до вимог ст.ст. 111, 112, 253 КПК України, здійснити письмове повідомлення підозрюваному, його захиснику та особам, конституційного права яких були тимчасово обмежені під час проведення негласних слідчих (розшукових) дій, про таке обмеження.

Додаток: Запити в 2 екз., на 2 арк.

Прокурор
у кримінальному провадженні Олександр ТАРАСОВ

Figure 2.4 Phishing documents used by the Gamaredon

These APTs are just the tip of the iceberg of the massive cyber theft campaign during the Russia-Ukraine war. More than 30% of the active APT incidents observed by NSFOCUS this year were from Eastern Europe, and most of these incidents were directly targeted at theft of secrets.

In addition, during the Russia-Ukraine cyber war, some secret theft attacks were carried out through social media, and the attackers were mostly civilian hacker groups or deep-camouflaged hacker groups. On March 1, 2022, NSFOCUS Global Threat Hunting System found that attackers sent phishing files to 10,000 members through a Telegram group impersonating 'IT ARMY of Ukraine'. The organizers posted multiple hacking tools within the group, including a file named 'ddos-reaper.zip.' The publisher advertises the tool's DDoS attack capabilities to induce members of the group to use it. After analysis, the tool is actually secret-stealing software, and when the user runs the tool, his own information will be leaked to the attacker, which can be described as 'As the predator stalks its prey, it forgets it may be prey itself.'

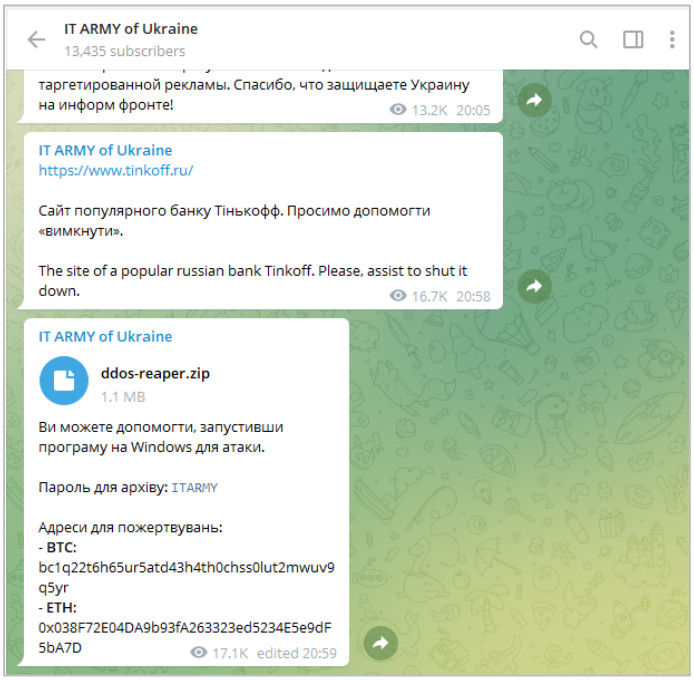


Figure 2.5 'IT ARMY of Ukraine' chat group

2.4.2 Cyber Special Operations with the Goal of Control

2.4.2.1 Pro-Russian Groups Control Public Opinion

In the Russia-Ukraine cyber war, some pro-Russian groups, composed of Russian civilian forces and superior organizers, launched public opinion control attacks against Ukraine and its allies through various channels. On the one hand, these pro-Russian groups suppress the spread of unfavorable news against Russia by attacking anti-Russian speech attack platforms; On the other hand, by launching a public opinion offensive, including publishing daily Russian frontline combat information on social platforms, refuting rumors and anti-Russian remarks, and publishing information on rebels, information confusion and public opinion manipulation are carried out to guide public opinion in a direction favorable to Russia.

Here's a timeline of cyberattacks by pro-Russian groups against hacker groups that support Ukraine, as well as state forces:

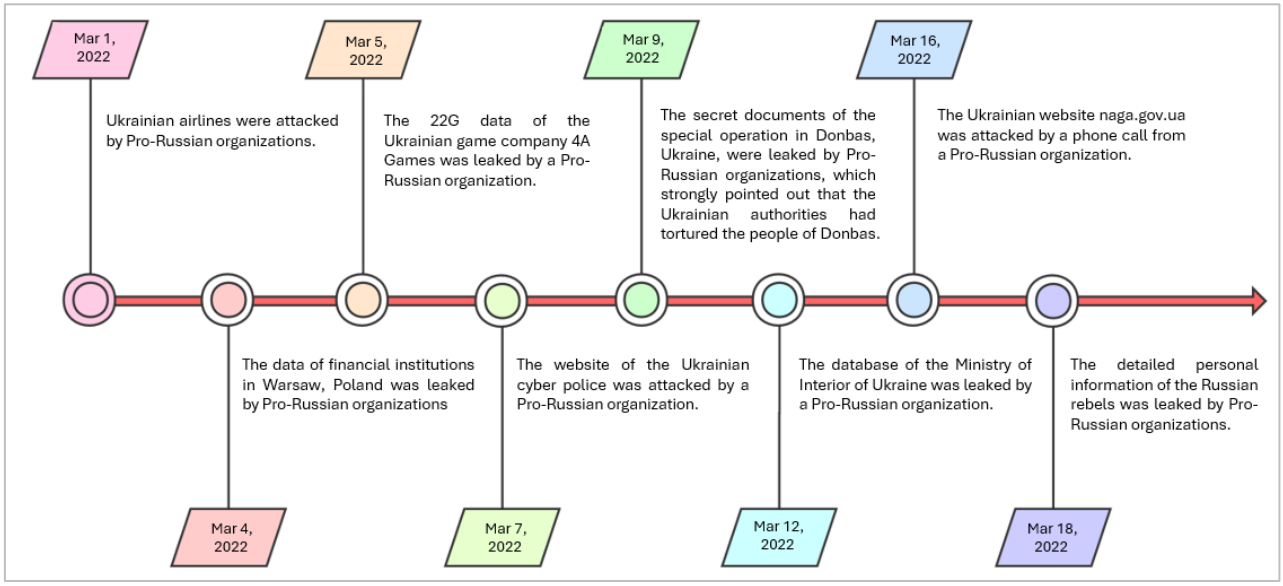


Figure 2.6 Timeline of attacks by Pro-Russian groups

2.4.2.2 Control of Public Opinion by Pro-Ukrainian Groups

NSFOCUS has found in its continuous monitoring of the Russia-Ukraine cyber conflict that after launching a large-scale DDoS attack on Russia, pro-Ukrainian groups took advantage of the gap in Russia's network infrastructure to communicate with the outside world in a timely manner to carry out public opinion control attacks. These groups claim that they have stolen a large amount of confidential Russian information and leaked documents on the Internet, creating an atmosphere of public opinion that Russia's IT infrastructure has been destroyed, and trying to mislead the Russian and Ukrainian people about the situation in the early stages of the war.

After the above-mentioned attacks, pro-Ukrainian groups set up anti-Russian speech attack platforms in which the public can freely participate, using stolen personal credentials such as personal phone numbers, email addresses, and WhatsApp accounts of Russian citizens to spread a large number of anti-Russian remarks to the Russian people through social platforms, creating an unfavorable social public opinion atmosphere for Russia, and trying to create public opinion tilt in Russia and the international community through this attack.

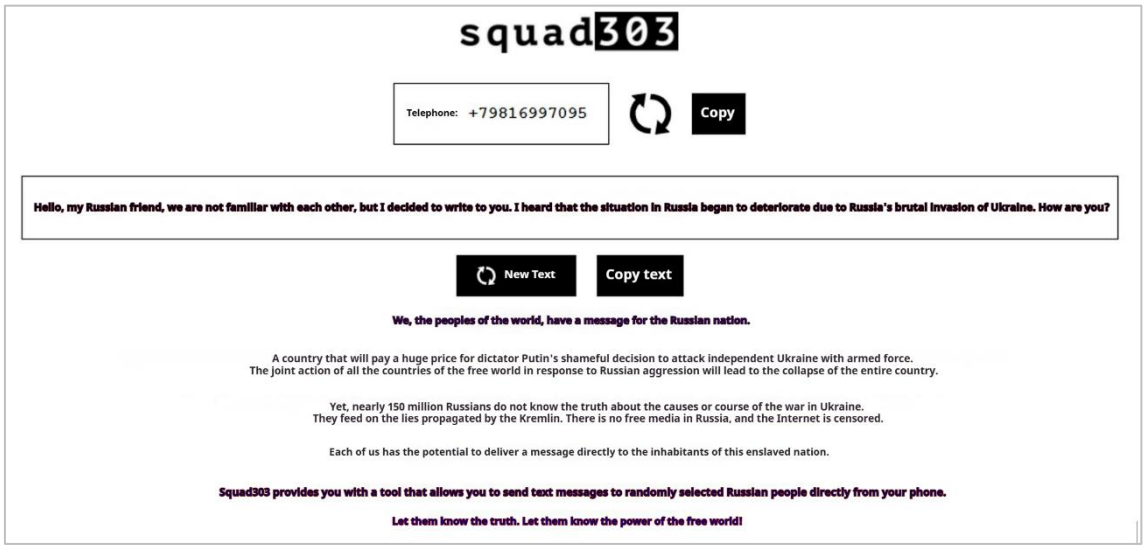


Figure 2.7 Pro-Ukrainian groups spread anti-Russian rhetoric

Here is a timeline of pro-Ukrainian groups conducting cognitive operations against Russia:

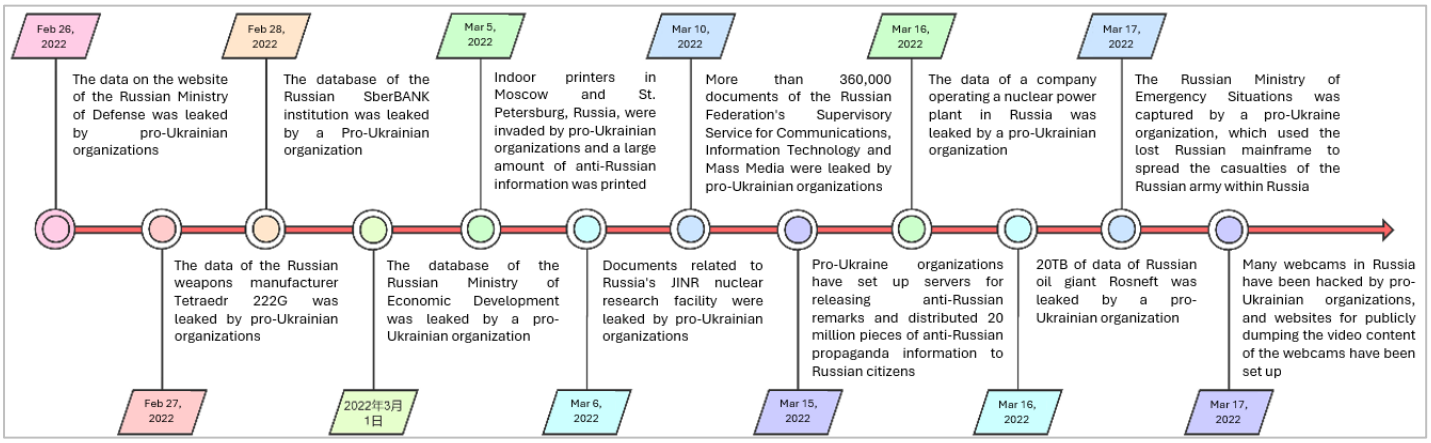


Figure 2.8 Timeline of attacks by Pro-Ukrainian groups

2.4.3 Cyber Special Operations with the Goal of Paralysis

2.4.3.1 Data-wiping Paralysis Attacks

On January 15, 2022, WisperGate's attack campaign against Ukrainian government departments was revealed. The attackers planted the WisperGate Trojan into the hosts targeted by the Ukrainian government and IT-related groups. NSFOCUS Fuying Lab analyzed the WisperGate Trojan and found that although the Trojan displays ransom and ransom information after it is run, the actual function of the Trojan is to directly overwrite the contents of all files on the victim host, which is a typical data-destroying Trojan. WhisperGate targets the government, non-profit groups, and information technology entities in Ukraine.

WhisperGate is actually a destructive wiping malware that is executed as a multi-stage attack with the sole purpose of destroying data, suggesting that the attackers are using WhisperGate as malware to compromise or paralyze the targeted group.

Another type of ransomware, known as HermeticRansom, has been used in Russia's cyber strikes against Ukraine following the outbreak of the Russia-Ukraine war. The analysis found that the ransomware is suspected to belong to the Sandworm group. HermeticRansom works in much the same way as regular ransomware, using the AES algorithm to encrypt file contents and leave a ransom note on the victim's host desktop. Analysis has shown that this ransomware could be used by attackers to cause trouble, making it necessary for the Ukrainian side to allocate efforts to deal with this type of threat, thus helping the Sandworm group achieve its real target.

In addition to the above Trojans, a variety of data destruction Trojans such as IsaacRansom, IsaacWiper, and Industroyer2 also appeared during the Russia-Ukraine cyber war. The development level of these Trojans is uneven, and the implementation effect has different emphasis, indicating that multiple advanced threat attackers in cyber warfare have used data-erasing paralysis attacks as an important attack method.

2.4.3.2 Denial-of-service Paralysis Attacks

On February 14, 2022, NSFOCUS's global threat hunting system detected abnormal DDoS traffic targeting Ukraine, and at the same time, the system detected attacks on financial websites, resulting in the bank's inability to provide services normally. On February 15, global media reported on the DDoS attack.

The attackers first launched a reflex DDoS attack on the State Civil Service of Ukraine (nads.gov.ua) and the Ukrainian government news website (old.kmu.gov.ua) at 4 a.m. on February 14, which lasted for a long time and caused a large amount of attack traffic, and on February 16, the monitoring system detected an attack on Privatbank (Ukraine's largest bank), which lasted for 2 hours, 28 minutes and 10 seconds. The Payload feature used by the attacker during the attack conforms to the established specifications of each service protocol and mainly targets ports 80 and 443 of the target.

At 2:25 a.m. on February 16, NSFOCUS Global Threat Hunting System detected a DDoS attack on Privatbank (Ukraine's largest bank), with 2.67 million attacks and an attack frequency of 290 PPS in 2 hours, 28 minutes and 10 seconds.

The main purpose of the above-mentioned DDoS attacks is to paralyze the online services of the target for a certain period of time, thereby creating a window for other types of cyber-attacks. DDoS attacks have appeared in large numbers during the outbreak of the Russia-Ukraine cyber war and have become an important means of paralyzing target network devices.

2.5 Insights

The main forms of current cyber special operations include cyber espionage activities, cyber sabotage, cognitive warfare, etc. The aim is to achieve control of the enemy's information and communication systems by conducting intrusive attacks on the enemy's network, weaken the enemy's military strength, and thereby achieve military strategic goals. With the development of cyber warfare attackers in terms of technical capabilities, organizational capabilities, etc., more intelligent, automated and collaborative attack methods may emerge in future cyber special operations.

Represented by the cyber war between Russia and Ukraine, it can be seen that the current composition of national cyber-attack forces is still dominated by APT activities. At a time when regional cyber warfare has emerged and the risk of large-scale cyber warfare has increased significantly, APT groups have played the role of cyber espionage on the one hand, and have used more advanced technical means to more effectively attack and control target networks, and steal high-value intelligence information beneficial to decision-makers in the fields of military, political, scientific and technological, and people's livelihood. On the other hand, it plays the role of a saboteur, and in the event of a geopolitical conflict, it remotely paralyzes the enemy's critical infrastructure through data destruction attacks to achieve battlefield support and network deterrence. APT groups will even control public opinion from the outbreak of war to the stalemate, taking advantage of the information gap to conduct ‘cognitive warfare’ against the enemy, disrupting the enemy's social order, and building an unfavorable public opinion environment for the enemy.

In 2014, the U.S. military promulgated the ‘Cyberspace Operations’ Joint Ordinance, which put forward measures for integrating cyberspace operations into joint operations in six links: command and control, intelligence, firepower, mobile deployment, support, and protection. In a 2018 webinar, the U.S. military proposed that cyber warfare can occur instantaneously, simultaneously, globally, and continuously. Success in this area will require whole-of-government action to integrate combat forces on interconnected battlefields.

General Secretary Xi Jinping once emphasized at the symposium on network security and informatization that the essence of network security is confrontation, and the essence of confrontation lies in the ability to compete at both offensive and defensive ends. Therefore, in the context of international tensions, in response to a possible cyber war, the defender needs to use a variety of strategies, including:

(1) Strengthen the construction of the national network security system, improve network security capabilities, and prevent and respond to attacks in cyber special operations.

(2) Strengthen cyber military drills and exercises, improve the military's cyber combat capability, and provide a strong guarantee for responding to the enemy's special cyber operations.

(3) Strengthen cooperation with allies to form joint combat capabilities and play a collective advantage and role in cyber special operations.

(4) Strengthen the military-civilian integration business, establish a sound network security military-civilian integration business policy system, promote the coordination and cooperation between the government and the market, increase the research and development of network security technology and personnel training, and improve the innovation ability of the network security military-civilian integration business.

(5) Intensify network security education and publicity, improve the public's awareness of network security, and promote the harmony and stability of the network society.

(6) Improve comprehensive cybersecurity emergency response plans and take rapid and effective emergency measures to restore network security and stability in the event of a cyber special operations incident.

(7) Establish a network security intelligence analysis mechanism to monitor network security threats in real time, detect abnormal behaviors in a timely manner, and take countermeasures.

(8) Improve the legal system for cybersecurity, regulate cyber special operations activities, and safeguard the public interest in cybersecurity.

(9) Strengthen international cyber security cooperation, carry out cyber special operations drills on the international stage, and provide targeted solutions.

(10) Increase R&D efforts and explore new cyber security technologies and methods to provide strong support for responding to new cyber special operations.

3. APT Threats

3.1 Overview

This year, NSFOCUS observed a large number of global APT activities or incidents, and the number of APT clues captured and confirmed APT events exceeded that of last year.

Among the global APT incidents captured or handled by NSFOCUS this year, the highest proportion of incidents were finally confirmed to be from the SeaLotus group. After adjusting its attack strategy, the SeaLotus group began to carry out cyber-attacks on China more actively, seriously endangering the data security of Chinese enterprises and organizations. At the same time, a number of APT groups launched attacks against Chinese universities, among which the NSA-TAO group attack was the most serious. Ransomware hacker groups have also targeted large enterprises in China, and the frequency and destructiveness of ransomware incidents from the enterprise side have increased significantly this year.

In terms of other global APT activities, groups in Eastern Europe, South Asia, the Korean Peninsula and the Middle East are active. Affected by the Russian-Ukrainian war, the APT groups in Eastern Europe have always maintained an attack state since the beginning of the year, and reconnaissance and sabotage in the early stage of the war were particularly frequent; The APT group on the Indian side continued its offensive that began at the end of last year, showing strong interest in Pakistan's military maneuvers and China-Pakistan cooperation projects. In addition to continuing cyber espionage activities based on national interests, the North Korean APT group has focused on increasing the attack intensity against the cryptocurrency industry; APT activities in the Middle East are still concentrated in countries on the eastern shores of the Mediterranean, and a number of new attackers have begun to take on espionage missions.

This year, NSFOCUS discovered a new APT group, MurenShark, which is active in Turkey and Northern Cyprus and has been attacking Turkish research institutes, military industries, and universities since from 2021. Another newly confirmed large-scale APT operation, DarkCasino, is suspected to have been initiated by a new hacker group belonging to the known APT group Evilnum, which has launched a long-term secret-stealing attack against online trading platforms in countries bordering the Mediterranean and Southeast Asian countries; NSFOCUS has also flagged multiple attackers from unidentified sources who have launched separate cyber-attacks against Russia, Belarus, Japan, Cyprus and other countries.

This year, NSFOCUS discovered a total of 483 APT clues, including various types of IoC information, of which 358 clues were first disclosed by NSFOCUS, as shown in the figure below.

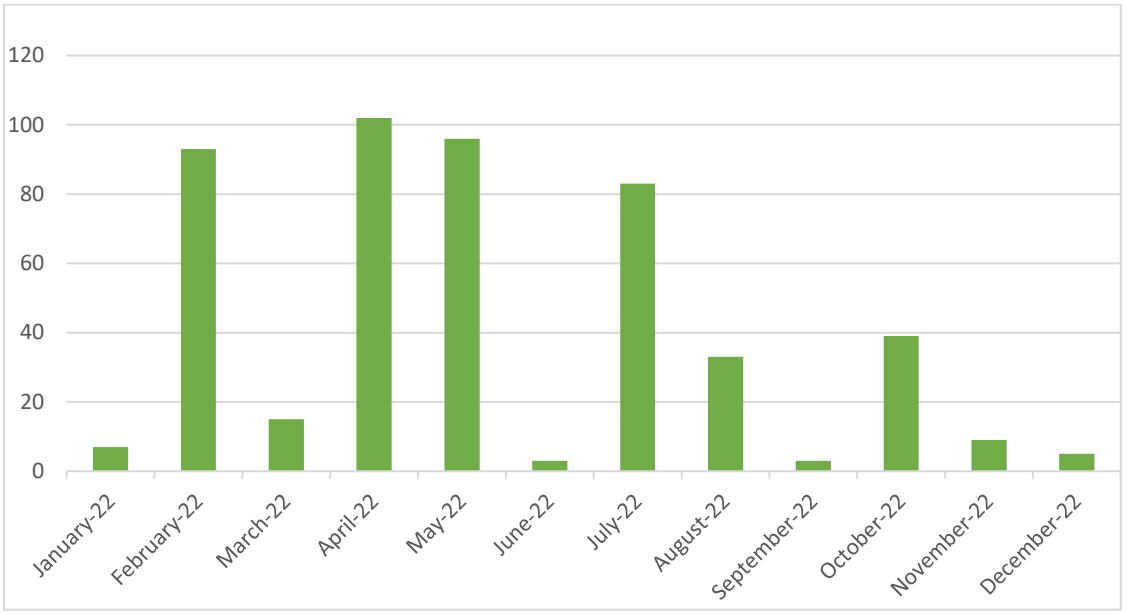


Figure 3.1 NSFOCUS APT clue discovery chart in 2022

It can be seen that a large number of APT clues were found in February, April and May in the first half of the year, and this phenomenon is directly related to the Russian Ukrainian war that broke out in February. The anomalous low frequency phenomenon in March may be due to the self-protection behavior of other APT groups during the cyber warfare.

After categorization, the above APT clues can be mapped to 85 APT events, and NSFOCUS has sorted out the timeline distribution of these APT events, as shown in the figure below.

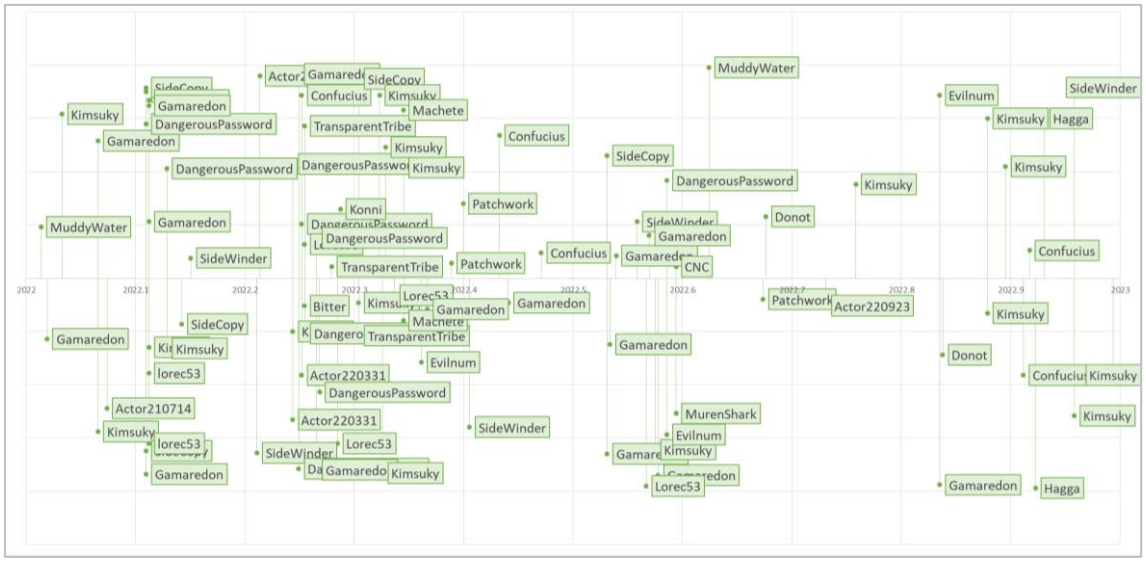


Figure 3.2 Timeline of NSFOCUS APT activities in 2022

As can be seen from the timeline distribution chart, the Gamaredon group, which is closely related to Russia's national interests, was active throughout 2022, and other Russia-related groups such as Lorec53 also acted frequently in the first half of the year; On the North Korean side, the Kimsuky group and the DangerousPassword group have also been active for a long time, targeting the South Korean government and the virtual currency industry, respectively. On the Indian side, multiple APT groups such as SideWinder, Patchwork, and Confucius became active after the second quarter, launching high-frequency cyber-attacks against the Pakistani government and army.

The above APT incidents came from 22 APT groups, of which 16 were confirmed groups and 6 were named or tagged by NSFOCUS. The statistics for APT activities this year are shown in the figure below.

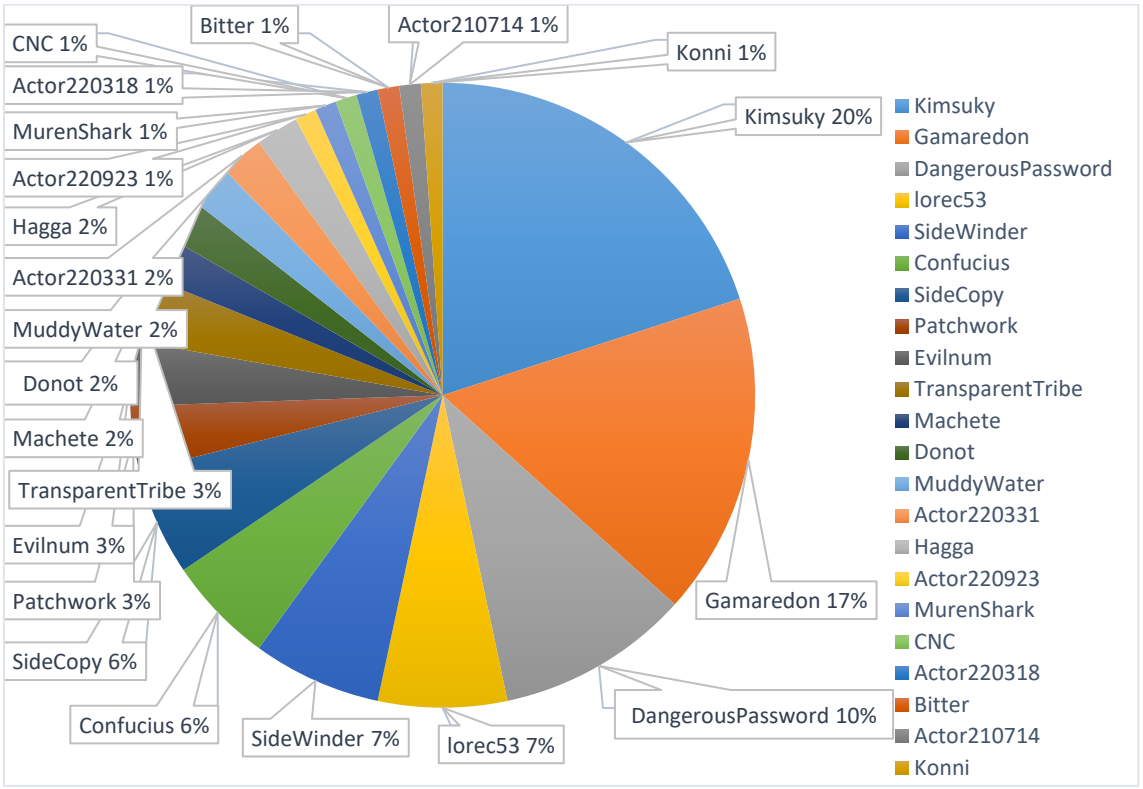


Figure 3.3 2022 NSFOCUS captures the statistical chart of APT activity attribution groups

3.2 APT Activities Against China

3.2.1 Attack from NSA-TAO

On June 22, 2022, Northwestern Polytechnical University issued a public statement saying that the university had been attacked by a global cyberattack. The handling unit's investigation of the incident revealed that the Office of Specific Intrusion Operations (TAO), a subsidiary of the National Security Agency (NSA), was the master of the entire cyberattack operation.

The U.S. National Security Agency (NSA) is the entity that corresponds to the known APT Equation, and the Office of Specific Intrusion Operations is the specific attack tool developer and perpetrator. The disclosed information indicates that in this attack on Northwestern Polytechnical University, TAO obtained the foothold points through exploitation of boundary device vulnerabilities, harpoon attacks and other methods, and then placed known formula group APT attack tools such as SUCTIONCHAR and NOPEN in the target network to collect network credentials within the domain. Then, through the FoxAcid vulnerability attack platform, a man-in-the-middle hijacking attack is carried out to further penetrate and control the network domain of the target unit. Most of the weapons and tools that emerged during this process correspond to the weapon functions described in the NSA's leaked documents, demonstrating the actual combat linkage capabilities of the TAO arsenal that previously existed in the documents and programs.

3.2.2 Attack from SeaLotus

This year, NSFOCUS caught a number of attacks by the Sea Lotus group against Chinese enterprises or institutions. In this series of incidents, the Sea Lotus attackers used a variety of different intrusion methods, actively trying to use software supply chain attacks, edge device vulnerability exploits, leaked credential exploits, phishing and other means to obtain a foothold in the target network, and then steal the credential information in the initial access node to enter the target unit's intranet, and finally steal important data of devices in the target domain by spreading commercial Trojans or homemade Trojans.

This is not the first time that the above-mentioned Sea Lotus attack pattern has appeared this year, and NSFOCUS has already monitored multiple attacks using this mode last year. While the attacker's exact route will be adjusted depending on the state of the target network, these events still expose consistent attack signatures that can be identified. Sea Lotus attackers maintain a high degree of vigilance during these attacks and are able to detect the investigation behavior of the defender and the disposer and respond in real time. These incidents also reflect the Sea Lotus's high understanding of the common cyber environment within Chinese enterprises or groups, and the group may have constructed a complete countermeasure strategy that can be applied to such attack activities. There is reason to speculate that the actual damage to the surface of Sea Lotus's current round of operations should be far beyond the scope of exposure.

3.2.3 Attacks from Other APT Groups

This year, NSFOCUS has captured a number of APT attacks against universities and other educational facilities in China. These APT attacks are carried out through phishing, in which the attackers often create highly credible email content to trick victims such as university professors into visiting watering hole sites disguised as email login pages, academic conference web pages, or paper submission pages, and then use further social engineering techniques to get victims to download and run Trojan horses. The ultimate goal of such attacks is to steal high-value files from the victim's host, and NSFOCUS has captured a variety of stealing Trojans that can be linked to known APT groups, indicating that such activities have become a common mode for attackers to infiltrate and investigate the current status of Chinese scientific research.

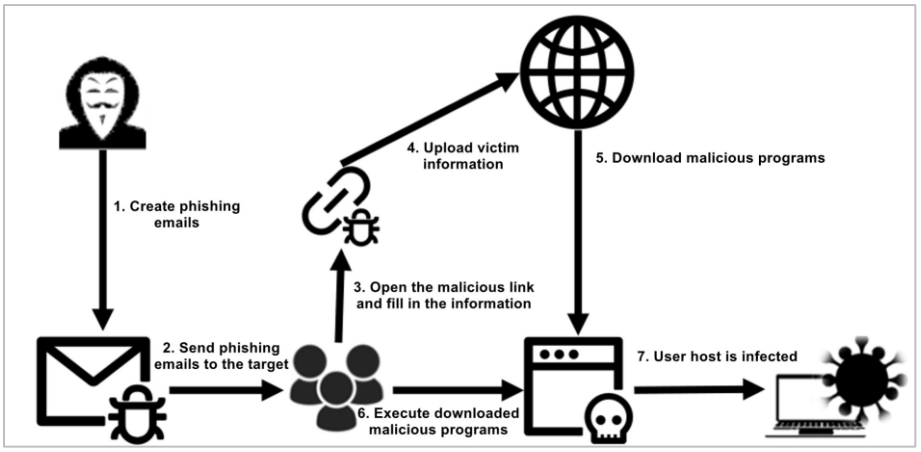


Figure 3.4 A typical process of an APT attack against a university in China

3.2.4 Attacks from Ransomware Groups

This year, NSFOCUS observed a number of ransomware attacks against Chinese companies.

Affected by the fierce competition of ransomware groups, a number of mainstream ransomwares hacking groups, including Conti, Hive, and Lapsus$, actively recruited attackers and expanded their attack surface this year, and began to set their sights on large enterprises in China. Of the ransom attacks that have been handled, the severity and destructiveness of the incidents from these large extortion groups have generally been greater.

Affected by the RaaS model, the current ransomware attacks against China have diverse forms of intrusion, depending on the attack ideas of specific attackers. However, NSFOCUS found that a large number of ransomware intrusions this year were done through compromised login credentials or edge device vulnerabilities. Attackers of ransomware groups have begun to focus on the frequent enterprise data breaches in recent years, by analyzing the personnel information contained in the leaked data, linking the login credential information with the work unit information, and then trying to enter the login portal exposed to the public network of the enterprise to obtain access to the enterprise intranet. Ransomware attackers have also begun to pay attention to the vulnerabilities of remote office tools such as cloud desktops and remote desktops, which have occurred frequently in recent years, and use vulnerability scanning to invade public network devices with vulnerabilities to further confirm the value of the devices and complete the ransomware attacks.

3.3 New APT Groups Confirmed This Year

3.3.1 MurenShark Targeting Turkey

In the second quarter of 2022, NSFOCUS Fuying Lab detected a series of cyberattacks against Turkey. Based on the area of activity of the threat entity and its recent target (Turkish Navy project 'MÜREN'), the Fuying Lab named it MurenShark.[7]

The observed activities of the MurenShark Group appeared in 2021, mainly targeting Turkey and Northern Cyprus, covering a number of sensitive targets in universities, research institutes and the military, with a clear interest in military projects. The exposed attack resources and deception methods indicate that the group has achieved its goals in cyberespionage operations against universities and research institutes.

The main attack tools include a malicious document generator called NiceRender, a C# backdoor Trojan LetMeOut, and a loader Trojan made by Donut, an open-source shellcode generation tool, UniversalDonut. The group's immediate goals include expanding attack resources, infiltrating target networks, stealing critical data, and more.

[7] http://blog.nsfocus.net/murenshark/

MurenShark attackers are good at hiding attack characteristics, hijacking legitimate sites, and disguising attack traffic as visiting the site and normal traffic. At the same time, the attack components are split to ensure that the payload at each stage does not produce attack behavior in an uncontrolled state. These measures have effectively enhanced the anti-traceability capability of the MurenShark.

Figure 3.5 A type of fishing document made by MurenShark via NiceRender

Investigations indicate that the exposed attacks are only the tip of the iceberg of the group's operations. The discontinuous evolution in both targets and attack components suggests that a large portion of the group's activities remains hidden in the shadows.

3.3.2 DarkCasino Targeting Online Trading Platforms

In the second quarter of 2022, NSFOCUS Fuying Lab captured a large-scale APT attack on DarkCasino. The campaign targeted online gambling platforms and targeted them to steal transaction credentials from service providers and consumers by attacking the active online transactions behind such services, thereby gaining illicit profits.

The DarkCasino series of events has a long duration and high frequency of attacks, and the victims are widely distributed in the countries bordering the Mediterranean and many countries in Southeast Asia. The attacker has been preparing for this series of activities for a long time, carrying out long-term iteration of the main attack process and core Trojan horse program, and stockpiling tools for batch generations of shellcode and steganography images to ensure that the attack campaign can be carried out on a large scale in a short period of time.

DarkCasino developers have taken the construction of attack processes seriously, and they use an override sideloading technique to directly build legitimate dll files such as side loaders with malicious code; The communication module of the Trojan program is designed using a classic VB socket window logic; A steganography pattern is also used to make steganography pictures.

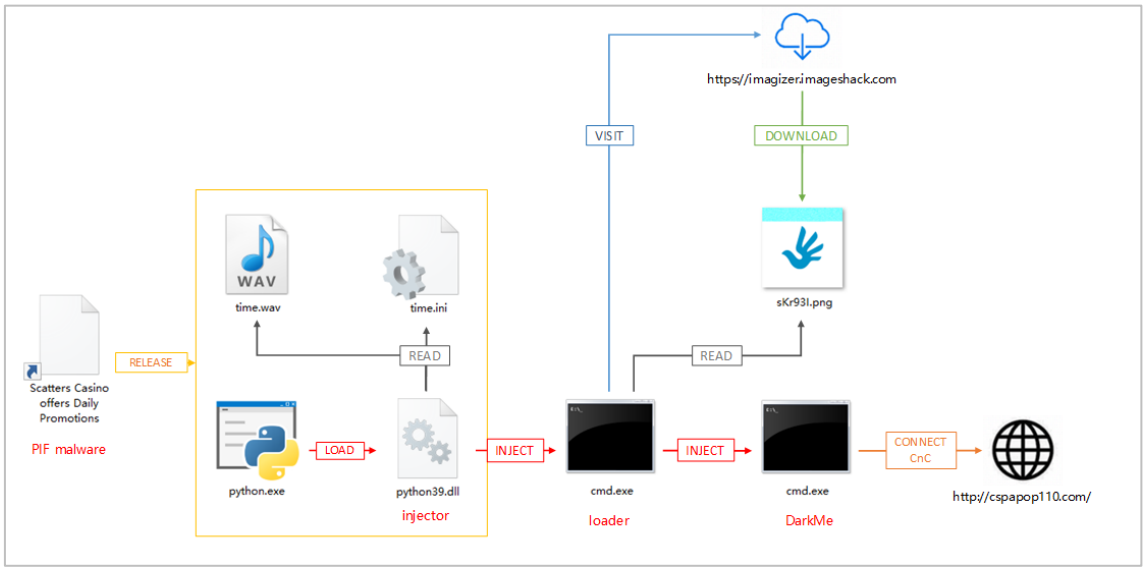


Figure 3.6 One of the main attack processes that emerged from DarkCasino' s operations

Follow-up continuous monitoring and analysis have shown that DarkCasino may be the new blood of the known financial APT group Evilnum, which makes the attacker have both the characteristics of the Evilnum group and its own unique characteristics. On the one hand, the DarkCasino attackers followed Evilnum' s signature attack process and development ideas, and on the other hand, they continued to iterate on self-made Trojan horses and attack techniques, and showed attack scope and attack inertia that did not match the characteristics of Evilnum group.

Until December, NSFOCUS was still able to observe the follow-up activities of the DarkCasino attackers.

3.3.3 Polonium Suspected to be from Lebanon

In June 2022, Microsoft revealed a new APT group called Polonium. The group, which is suspected to be from Lebanon, has targeted Israel's defense industry and manufacturing industry as its main target, and has targeted more than 20 entities.

Polonium will try to attack IT companies upstream of the supply chain and hack other companies downstream of the supply chain by hijacking the supply chain. It is presumed that the initial point of entry is a Fortinet device containing a specific vulnerability.

The group demonstrated strong adversarial capabilities in the attack campaign, with its main backdoor, CreepyDrive, using the Microsoft Graph API endpoint as a command communication channel, and another backdoor, plink, to build an SSH channel to reduce the risk of exposure to the communication process.

3.3.4 Metador for the Middle East and Africa

In September 2022, SentinelLabs disclosed a new APT group, Metador, targeting countries in the Middle East and Africa. The group targeted major telecommunications and Internet service providers in the region in an attempt to steal intelligence information.

In the disclosed campaign, Metador used Trojans called metaMain and Mafalda, as well as a Cryshell intranet penetrator. The Trojan horse used by Metador is built in the framework mode, and the attacker can flexibly switch the operation mode and attack mode according to the state of the target host, and can cooperate with special execution and persistence methods, showing a high level of attack technology. Metador uses a large number of adversarial methods such as code obfuscation, communication verification, and delayed execution in the attack campaign, which proves that the attacker tends to be cautious in attacking.

Metador has incorporated redundant information into its attack process, making it difficult for investigators to confirm the group's origin.

3.4 The Abuse of New Types of Vulnerabilities by APT Groups

This year, NSFOCUS observed multiple 0-day or N-day vulnerabilities being abused by APT groups. The 0-day vulnerabilities first used by APT groups include Internet Explorer script engine vulnerability, CVE-2022-41128, etc.; Misused N-day vulnerabilities include the Log4Shell vulnerability, which caused a huge impact. Affected by the emergence of some high-risk N-day vulnerabilities, APT groups showed an overall trend of decreasing 0-day use and increasing N-day attempts in terms of vulnerability exploitation this year.

3.4.1 Log4Shell

NSFOCUS observed that the 0-day vulnerability Log4Shell (CVE-2021-44228) exposed at the end of 2021 was used by a large number of known APT groups in cyber-attack activities this year.

The Log4Shell vulnerability is a 0-day vulnerability in the Java logging framework Log4j, which can implement arbitrary code execution and is very simple and stable to build. This feature caused the vulnerability to attract the attention of several national APT groups immediately after it was exposed.

As early as early January, the Charming Kitten group began to scan for Log4Shell vulnerabilities and used a public exploit tool to hack public network devices with vulnerability. The Lazarus group used the Log4Shell vulnerability in a series of attacks that began in February this year, successfully compromising VMware Horizon servers at several national energy companies; At the beginning of the year, the TunnelVision group also scanned and attacked Log4Shell vulnerabilities with Log4Shell vulnerabilities to execute ransomware attacks. Half a year after the vulnerability was disclosed, APT groups such as MuddyWater still gained a foothold on the target host by hacking into the unpatched SysAid server equipment.

3.4.2 Follina

In May 2022, the security community exposed a new Microsoft Office 0-day vulnerability, which analysts named Follina, and later received the designation CVE-2022-30190.

Follina is an Office remote template vulnerability, an attacker can add a special remote template link to a Word document and then build a long HTML file to make the MSDT process in Office software execute arbitrary powershell code.

Due to the high availability and unique form of this vulnerability, several phishing-based APT groups quickly began to build attack chains based on this vulnerability. During the 0-day exploitation of the vulnerability, NSFOCUS observed that groups marked as Actor220603 began to use the vulnerability to attack non-governmental groups and individuals in Belarus. After the vulnerability was made public, groups such as TA570 began to use vulnerability to strengthen their attack processes. NSFOCUS also caught a large number of phishing documents using this vulnerability in the second half of this year, but because attackers usually need to develop separate attack components for this vulnerability, most of the phishing documents cannot be associated with known APT groups, so this vulnerability has become an important channel for APTs to hide their own characteristics and launch anonymous attacks.

3.5 APT Activities in Key Areas

3.5.1 Eastern Europe

This year, a number of major APT groups in the Eastern European region have been involved in the cyber confrontation of the Russia-Ukraine war. Gamaredon, a Russian APT group, continued to be active from the preparation stage to the stalemate phase of the Russia-Ukraine war, playing the role of a scout and continuously monitoring the military movements of the Ukrainian side; The Sandworm group participated in the outbreak of the Russia-Ukraine war as an attacker, using a variety of data-erasing Trojans to carry out cyber-attacks aimed at destroying and paralyzing key enemy facilities. Lorec53, an emerging APT group, flexibly switched its attack roles and carried out different cyber-attacks such as cyber reconnaissance, data destruction, and continuous monitoring at different stages of the Russia-Ukraine war.

At the same time, the Russia-Ukraine war has also spawned a large number of cyber-attacks that have not confirmed the identity of the attackers, such as an unknown threat actor named Actor220331 marked by NSFOCUS launched a number of attacks against the Russian government's Ministry of Communications during the outbreak of the war; Another unknown group, flagged by global security firms, launched multiple cyberattacks against key facilities such as the Russian government's Ministry of Defense and Communications between the start of the war and mid-April. These unknown threat actors all possess a high level of attack capability and confrontation, and NSFOCUS deduces that they may be temporary attack teams evolved from known APT groups that are inconvenient to reveal their identities to participate in special missions during the war as independents.

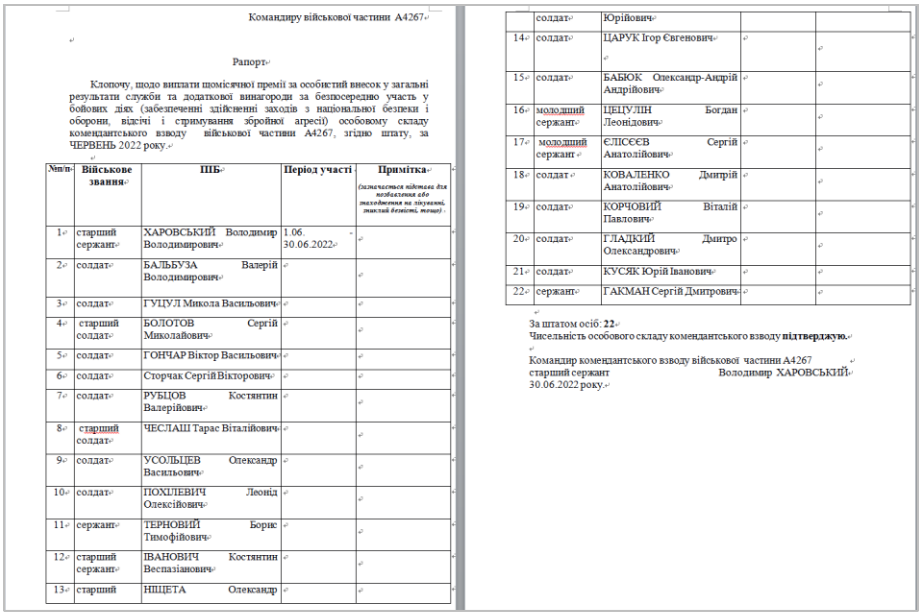
3.5.1.1 Gamaredon

The pro-Russian hacker group Gamaredon is an APT group that is constantly active. The group took on the role of intelligence gathering during the preparation stages of the Russian Ukrainian war, and there was a noticeable increase in the frequency of its activities. The captured events indicate that the group has carried out extensive attacks on government departments, police facilities, military personnel, and even large businesses in the eastern regions of Ukraine since the second half of 2021. Gamaredon' s attacks during this period targeted a wide range of people, including not only military personnel, but also government personnel, journalists, pro-American figures, and other individuals who were not directly related to military activities, but who may have high-value intelligence about Ukraine. It is clear that the Gamaredon group of this period focused on the

strategy of casting a wide net, actively collecting all intelligence that would be beneficial for subsequent military operations. The group's cyber espionage activities in eastern Ukraine, such as Donetsk and Luhansk, can be seen as part of the pre-war reconnaissance activities of the Russian side.

In the early days of the Russia-Ukraine war, the Gamaredon group also played the role of a saboteur, using a data-erasing software called IsaacWiper to carry out cyberattacks aimed at paralyzing key facilities in Ukraine.

After May, the Gamaredon group continued its cyberespionage activities, but the main targets were Ukrainian military personnel. The Gamaredon attackers used various documents on military operations in Ukraine as bait to carry out phishing attacks, focusing on collecting military information from the Ukrainian side during the period. Such attacks continued into the third quarter, proving that the Russian APT forces had shifted their focus to monitoring enemy activity.



Командиру військової частини А4267

Рапорт

Клопочу, щодо виплати щомісячної премії за особистий внесок у загальні результати служби та додаткової винагороди за безпосередню участь у бойових діях (забезпеченні здійсненні заходів з національної безпеки і оборони, відсічі і стримування збройної агресії) особовому складу комендантського взводу військової частини А4267, згідно штату, за ЧЕРВЕНЬ 2022 року.

№п/п	Військове звання	ПІБ	Період участі	Примітка (зазначається підстава для позбавлення або знаходження на лікуванні, зниклий безвісті, тощо)
1	старший сержант	ХАРОВСЬКИЙ Володимир Володимирович	1.06. - 30.06.2022	
2	солдат	БАЛЬБУЗА Валерій Володимирович		
3	солдат	ГУЦУЛ Микола Васильович		
4	старший солдат	БОЛОТОВ Сергій Миколайович		
5	солдат	ГОНЧАР Віктор Васильович		
6	солдат	Сторчак Сергій Вікторович		
7	солдат	РУБЦОВ Костянтин Валерійович		
8	старший солдат	ЧЕСЛАШ Тарас Віталійович		
9	солдат	УСОЛЬЦЕВ Олександр Васильович		
10	солдат	ПОХІЛЕВИЧ Леонід Олексійович		
11	сержант	ТЕРНОВИЙ Борис Тимофійович		
12	старший сержант	ІВАНОВИЧ Костянтин Веспазіанович		
13	старший солдат	НІЩЕТА Олександр Юрійович		
14	солдат	ЦАРУК Ігор Євгенович		
15	солдат	БАБЮК Олександр-Андрій Андрійович		
16	молодший сержант	ЦЕЦУЛІН Богдан Леонідович		
17	молодший сержант	ЄЛІСЄЄВ Сергій Анатолійович		
18	солдат	КОВАЛЕНКО Дмитрій Анатолійович		
19	солдат	КОРЧОВИЙ Віталій Павлович		
20	солдат	ГЛАДКИЙ Дмитро Олександрович		
21	солдат	КУСЯК Юрій Іванович		
22	сержант	ГАКМАН Сергій Дмитрович		

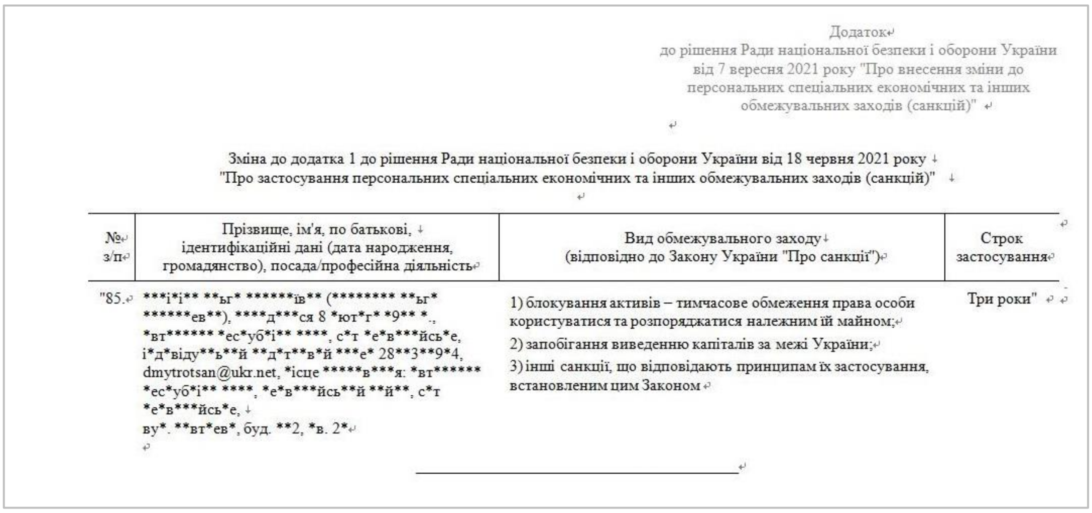
За штатом осіб: **22**
Чисельність особового складу комендантського взводу **підтверджую.**

Командир комендантського взводу військової частини А4267
старший сержант Володимир ХАРОВСЬКИЙ
30.06.2022 року.

Figure 3.7 The content of phishing documents against the Ukrainian army used by Gamaredon during the surveillance phase

3.5.1.2 Lorec53

Lorec53 also known as UAC-0056 or UNC2589, is a pro-Russian APT group that became active in 2020 and can be seen as a representative of the APT group's active role reversal in the early days of the war. Before the outbreak of the Russian Ukrainian war, the group exhibited similar characteristics to the Gamaredon group, using phishing mail and watering hole sites as the main means to collect intelligence on key Ukrainian personnel on a large scale.



Додаток
до рішення Ради національної безпеки і оборони України
від 7 вересня 2021 року "Про внесення зміни до
персональних спеціальних економічних та інших
обмежувальних заходів (санкцій)"

Зміна до додатка 1 до рішення Ради національної безпеки і оборони України від 18 червня 2021 року
"Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)"

№ з/п	Прізвище, ім'я, по батькові, ідентифікаційні дані (дата народження, громадянство), посада/професійна діяльність	Вид обмежувального заходу (відповідно до Закону України "Про санкції")	Строк застосування
"85.	***і*і** **ьг* ******ів** (******** **ьг* ******ев**), ****д***ся 8 *ют*г* *9** *., *вт****** *ес*уб*і** ****, с*т *е*в***йсь*е, і*д*віду**ь**й **д*т**в*й ***е* 28**3**9*4, dmytrotsan@ukr.net, *ісце *****в***я: *вт****** *ес*уб*і** ****, *е*в***йсь**й **й**, с*т *е*в***йсь*е, ву*. **вт*ев*, буд. **2, *в. 2*	1) блокування активів – тимчасове обмеження права особи користуватися та розпоряджатися належним їй майном; 2) запобігання виведенню капіталів за межі України; 3) інші санкції, що відповідають принципам їх застосування, встановленим цим Законом	Три роки"

Figure 3.8 The content of the phishing documents used by Lorec53 during the reconnaissance phase

After the outbreak of the war, the Lorec53 group temporarily stopped cyber espionage operations, developed a variety of data destruction software called WhisperGate, WhisperKill, WhiteBlackCrypt, and led a destructive cyber-attack operation against several groups in Ukraine.

Beginning in late March, Lorec53 also began to play the role of watchdog, frequently using a set of attack suites called GrimPlant and GraphSteel to attack Ukrainian government departments, and these attack tools can help Lorec53 attackers collect high-value content from victims' hosts and execute remote commands.

Throughout the entire course since the outbreak of the Russia-Ukraine war, the Lorec53 group has played multiple roles in cyber-attacks very well, helping the masterminds behind it achieve their tactical goals.

3.5.2 South Asian Subcontinent

During the year, several APT groups in the South Asian subcontinent remained active. NSFOCUS Fuying Lab observed that although relations between India and Pakistan have eased compared with the dangerous state in the past, the APT forces of the two countries have not reduced the frequency of cyber-attack activities.

Since the end of last year, India's main APT attack forces, SideWinder and Patchwork, have continued to carry out intensive cyber offensives against Pakistan, while Confucius, another APT group, has also resumed cyber-attacks against the country this year. All of these attacks have focused on the Pakistani army and Government.

Pakistan's main APT group, the TransparentTribe, was also active during the year, conducting phishing-focused operations against a wide range of targets, including the Indian government, military, educational institutions, and even individuals; Another APT group, SideCopy, also actively carried out various phishing attacks against the Indian army in the first half of this year, all of which followed one of the group's signature LNK file attack processes.

3.5.2.1 Patchwork

Patchwork, also known as Dropping Elephant, APT-C-09, is an established APT group with an Indian background. The current round of Patchwork's operations, which began at the end of last year and lasted until the beginning of '22, restarted a wave of attacks from May to the end of the year after a short break. In this round of activities, the Patchwork attackers still used a large number of the group's representative attack components, the BADNEWS Trojan, and a special CVE-2018-11882 vulnerability document building tool, and the targets of the attack included the Pakistani government army and some government departments in China.

In a patchwork attack captured this year, NSFOCUS discovered that the group had started developing and using a new BADNEWS variant Trojan. Compared with the old version of the Trojan, the new version of the program adds a spoofing address, simplifying the more complex and impractical functions of the old version, but the overall code structure has become larger.

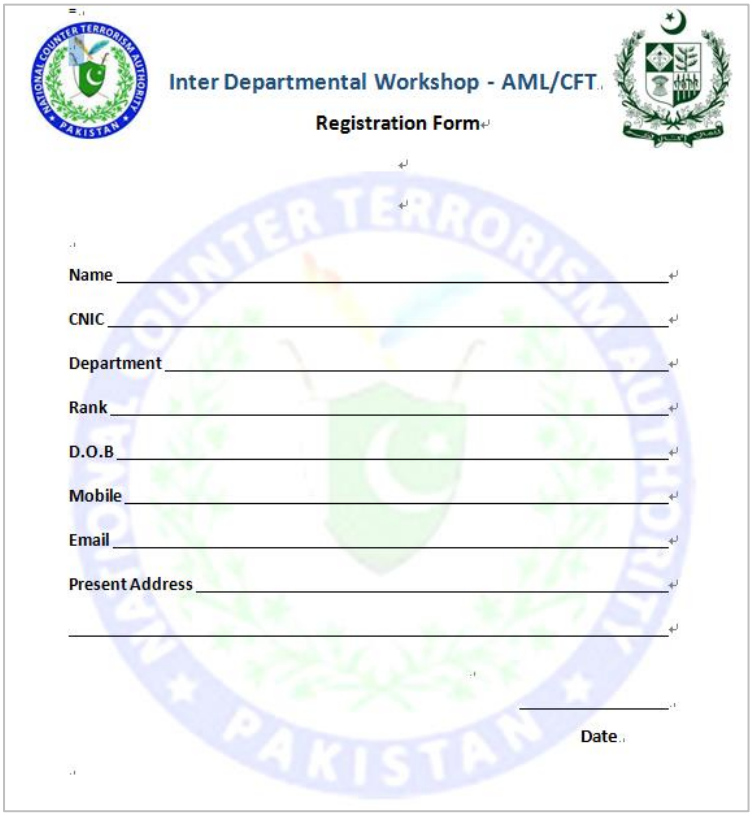


Figure 3.9 A Patchwork phishing document with a new BADNEWS Trojan

3.5.2.2 Confucius

Confucius, an Indian APT group, is a hacker group that has been active since 2013. This year's Confucius campaign cycle began in February and lasted until the end of the year, with attackers trying to trick the target group and collect high-value data on the victim's host by forging various lure documents with various Pakistani government letterheads and logos.

Compared to other Indian APT threat actors, Confucius is more creative in terms of attack methods and attack process design. This year, the Confucius attackers began to use legitimate network disks as a relay platform for attack payloads and added various mainstream countermeasure techniques to the main Trojans used for anti-identification and anti-analysis. In a Confucius operation captured by NSFOCUS this year, the attacker delivered a new version of the group's self-made C++ Trojan, which modified the features exposed by the previous version of the Trojan and began to use control flow obfuscation to try to protect the main functional code, demonstrating the sensitivity of the attacker and the developer in the confrontation between attack and defense.

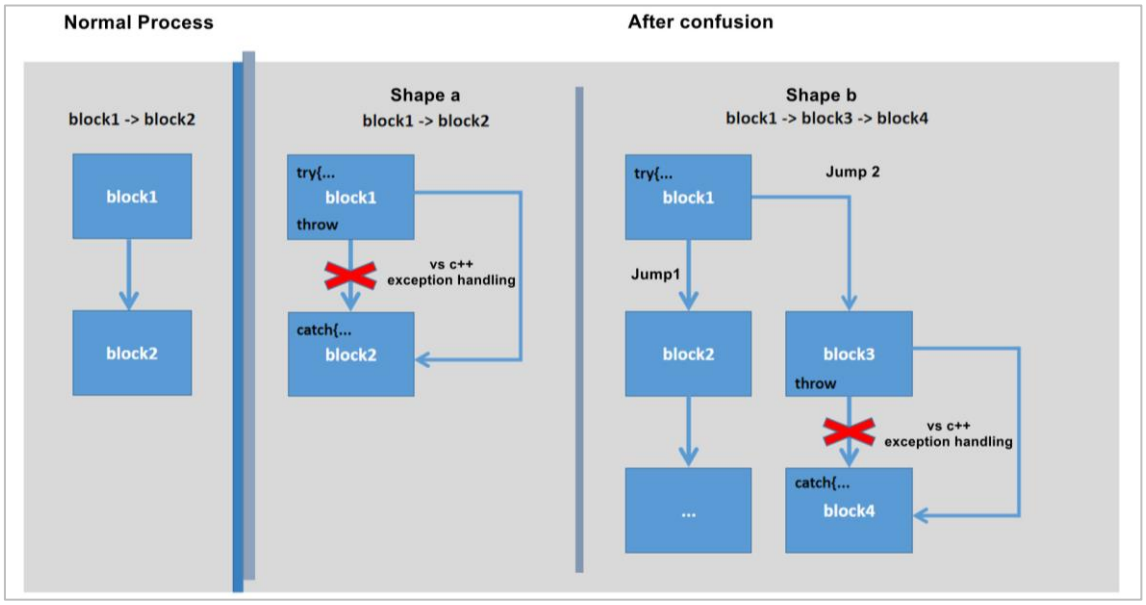


Figure 3.10 A new type of obfuscation used by Confucius during the year

3.5.2.3 TransparentTribe

Pakistan's APT group, TransparentTribe, continued its last year's activity, launching cyberattacks against a wide range of targeted groups. This year, TransparentTribe continues to use two iconic attack components, CrimsonRAT and ObliqueRAT, to carry out its attacks, and its phishing bait genres are very extensive, including military presentations, survey forms, photos and other documents that can be easily mishandled by victims. In terms of targets, the main goal of this year's TransparentTribe is to gather intelligence information from key Indian groups, even though the target group is widely distributed across a wide range of industries.

3.5.3 Korean Peninsula

This year, due to the economic downturn and the uneased inter-Korean relations, the DPRK has once again increased the frequency of its APT operations, which are mainly aimed at the South Korean government and the cryptocurrency industry.

Such high-frequency activity exposes more details about the APT on the North Korean side. The study found that the lines between North Korea's major APT groups are blurring, and multiple groups are sharing attack resources and targets. Following the 2019 correlation (https://blog.alyac.co.kr/2347) between Reaper, two of North Korea's oldest groups, Kimsuky's discovery of a direct attack on cryptocurrencies has led to an intersection with Lazarus, another well-known North Korean APT group, in terms of motivations. This phenomenon also shows that the APT groups on the North Korean side are paying more attention to the offensive in cryptocurrency, and they are pinning their hopes on providing more funds to higher authorities through cyber-attacks while the cryptocurrency channel still has high profitability.

3.5.3.1 Kimsuky

This year, the Kimsuky group remained extremely active, carrying out frequent attacks on the South Korean government and other forces that could pose a threat to the North Korean side.

The activities of Kimsuky observed by NSFOCUS this year mainly include two attack processes. One process center on the malicious macro file and BabyShark Trojan commonly used by the group, while the other process incorporates legitimate cloud storage addresses and a Trojan program marked as KimAPosT by NSFOCUS.

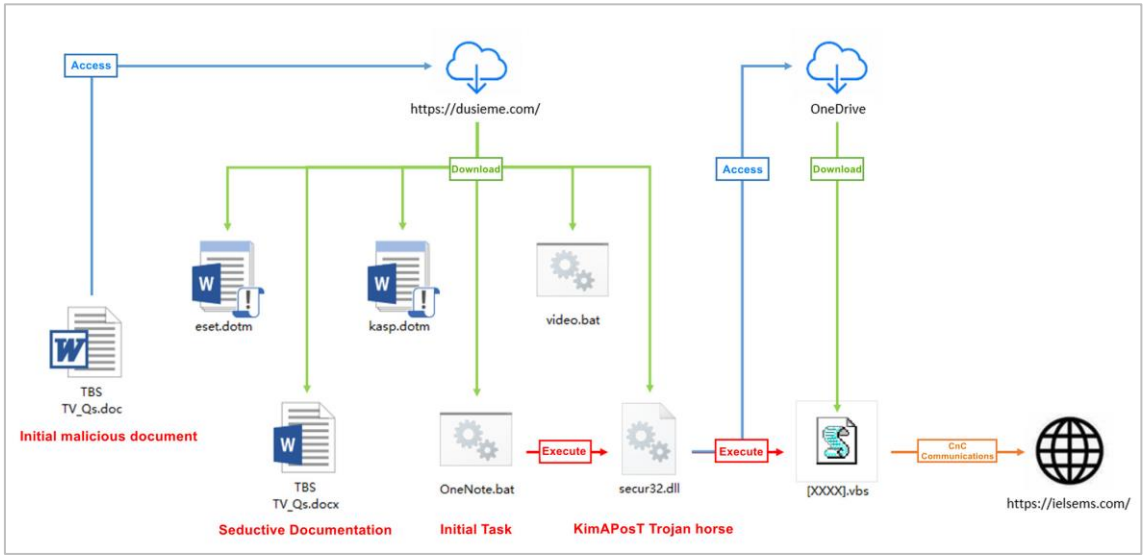


Figure 3.11 This year's Kimsuky is based on KimAPosT' s representative process

In 2021, the Kimsuky group began testing and using this KimAPosT-based attack process, and in this year's attack campaign, it has perfected the bypass strategy and added some anti-analysis methods. Compared to other known Kimsuky attack processes, this process provides more flexibility in terms of final attack code delivery.

3.5.3.2 Lazarus

During the year, the Lazarus group continued to expand its attack vectors and targets.

Most of the Lazarus attacks this year have targeted the cryptocurrency industry, and related companies, exchanges, and users have all endured frequent attacks by the group. Associated incidents show that Lazarus has internally divided the work for this round of attacks, with one or more teams frequently using existing attack tools to maintain a high frequency of phishing attacks, while another team is actively developing new attack methods to try to expand the impact area.

This year, Lazarus' development team began to develop a Mach-O executable Trojan attack process based on the M1 architecture, so that the group can attack cryptocurrency users on multiple platforms at the same time. The process includes a dropper Trojan capable of compiling into multiple platform versions, a phishing pdf file made based on the target, a subsequent loader Trojan, and a downloader Trojan, which can target victims using Windows, M1 Mac, or Intel Macs at the same time.

3.5.4 Middle East

This year, APT attacks in the Middle East continued to focus on the Mediterranean coast and around the Mesopotamian plain, with victims including Turkey, Cyprus, Iran, Israel and other countries.

NSFOCUS found that Turkey and Iran were both the initiators and victims of APT attacks this year. StrongPity, an APT group with a suspected Turkish background, began to be active again in late '21, orchestrating multiple puddle phishing attacks against neighboring countries such as Palestine, while MurenShark, a threat actor of unknown origin, launched a well-planned phishing attack against the Turkish Navy this year; APT groups such as Charming Kitten and AridViper, suspected of having Iranian backgrounds, continued to attack neighboring countries such as Jordan this year, and the country also suffered one of the worst industrial cyberattacks of the year, resulting in the production line of the Khuzestan steel plant in southwestern Iran being damaged and halted down.

The activities of the commercial-oriented APT have also disrupted several countries in the Middle East. In the APT operation called DarkCasino, which was discovered by NSFOCUS, the attackers targeted the online cash flow of countries bordering the Mediterranean, including online trading platforms and online entertainment platforms in Turkey, Israel and other countries. NSFOCUS also observed an attacker of unknown origin, marked as Actor220923, who launched a phishing campaign targeting users of the Cyprus Stock Exchange in Q3.

3.5.4.1 Charming Kitten

This year, the Middle East APT group Charming Kitten (APT35) has been particularly active, and its activities continue to focus on obtaining information on hostile forces through large-scale cyber theft. Charming Kitten's main attack vector is spearing phishing, but unlike other APT groups, after Charming Kitten obtains initial access to the victim's host this year, it usually logs in to the victim's Gmail, Outlook and other mailboxes through the collected credentials, obtains the emails in them, and then filters high-value information from them.

Charming Kitten's attacks this year continue to focus on credential theft and information theft, and the group used a new backdoor Trojan called PowerLess in its campaign late last year and early this year, along with some credential theft tools downloaded by the Trojan to complete the theft attack.

Charming Kitten also actively tries to use the N-day vulnerability to strengthen its attack capabilities. Charming Kitten was one of the first APT groups to attempt a large-scale scan using the Log4Shell vulnerability, started scanning and exploiting vulnerability in January '22.

3.6 Brief Summary

Geopolitical conflicts are always the fundamental driving force of national APT groups. The large number of APT incidents driven by geopolitical conflicts this year proves that the activities of national APT groups have become an important means for corresponding countries to sniff out changes in the situation and cope with the escalation of geopolitical conflicts. The facts of the cyber war between Russia and Ukraine also tell us that when the deterioration of geopolitical relations leads to the outbreak of physical conflicts, APT cyber-attack forces will play a role in supporting and covering the conflict and even become an important combat force.

In the face of the fact that APT attacks are integrated into cyber warfare, defenders need to change their thinking about APT attacks, explore and pay attention to the ‘signal’ attributes of APT attacks, and establish a sound monitoring and statistics system to perceive the tendency and trend of APT attacks, speculate the intentions behind APT attacks, and make correct responses.

4. Ransomware Threats

4.1 Overview of Ransomware Attacks in 2022

According to NSFOCUS's long-term observations, most of the active ransomware attacks in 2022 came from large ransomware groups such as LockBit, Conti, BlackByte, Hive, and BlackCat, and the other came from dozens of small and medium-sized ransomware gangs that have emerged in recent years.

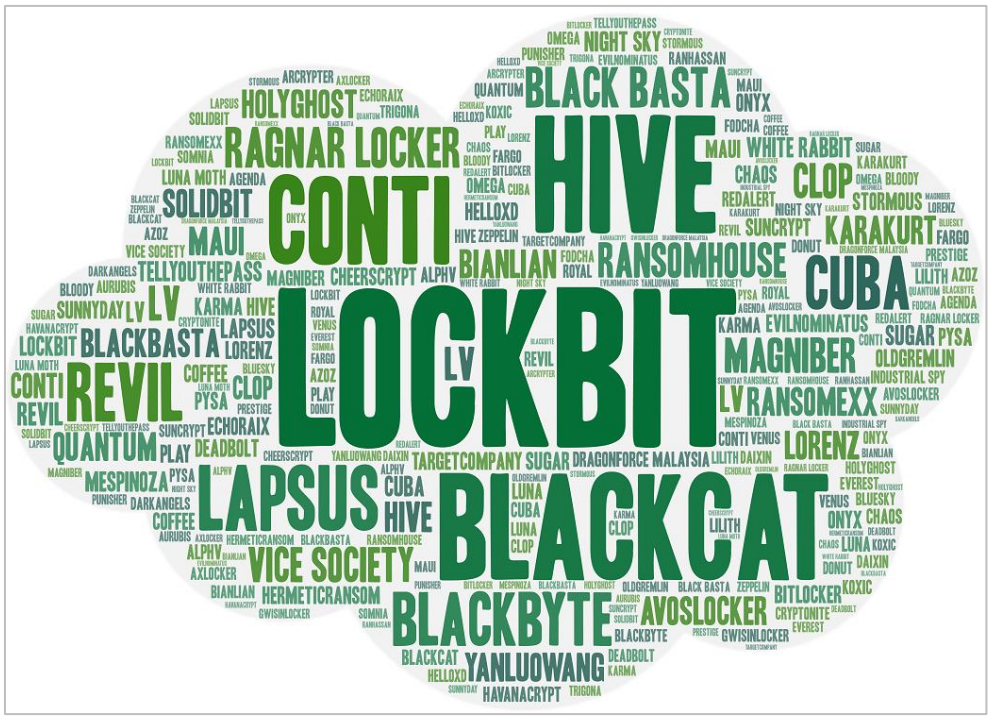


Figure 4.1 Active ransomware word cloud in 2022

NSFOCUS Fuying Lab counted the number of active ransomware Trojans this year and found that most of these Trojans appeared in the second half of the year, with more than 25% of them appearing in November.

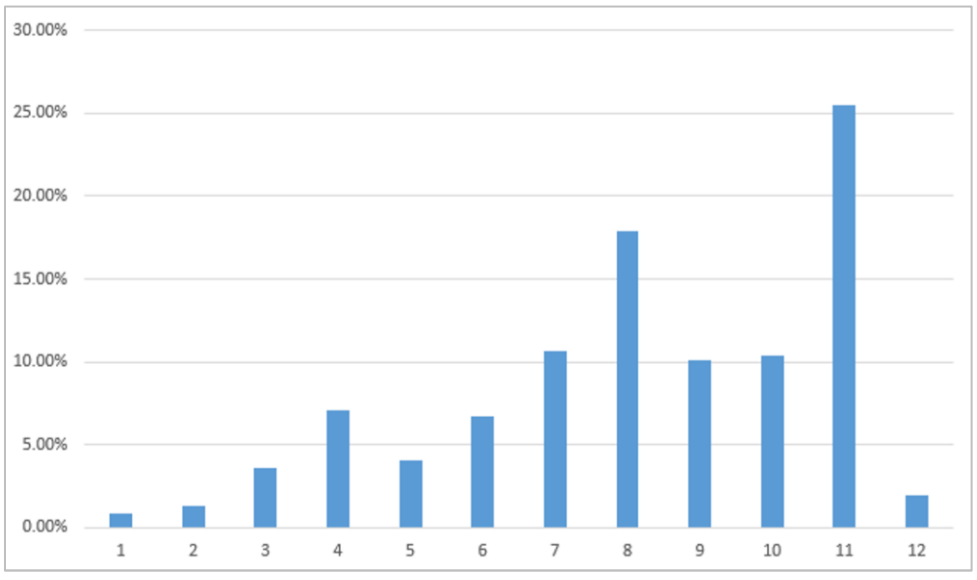


Figure 4.2 Monthly active distribution of ransomware

In terms of the distribution of victim countries, it can be seen that European and American countries are the hardest hit areas of ransomware, of which the United States accounts for 36%.

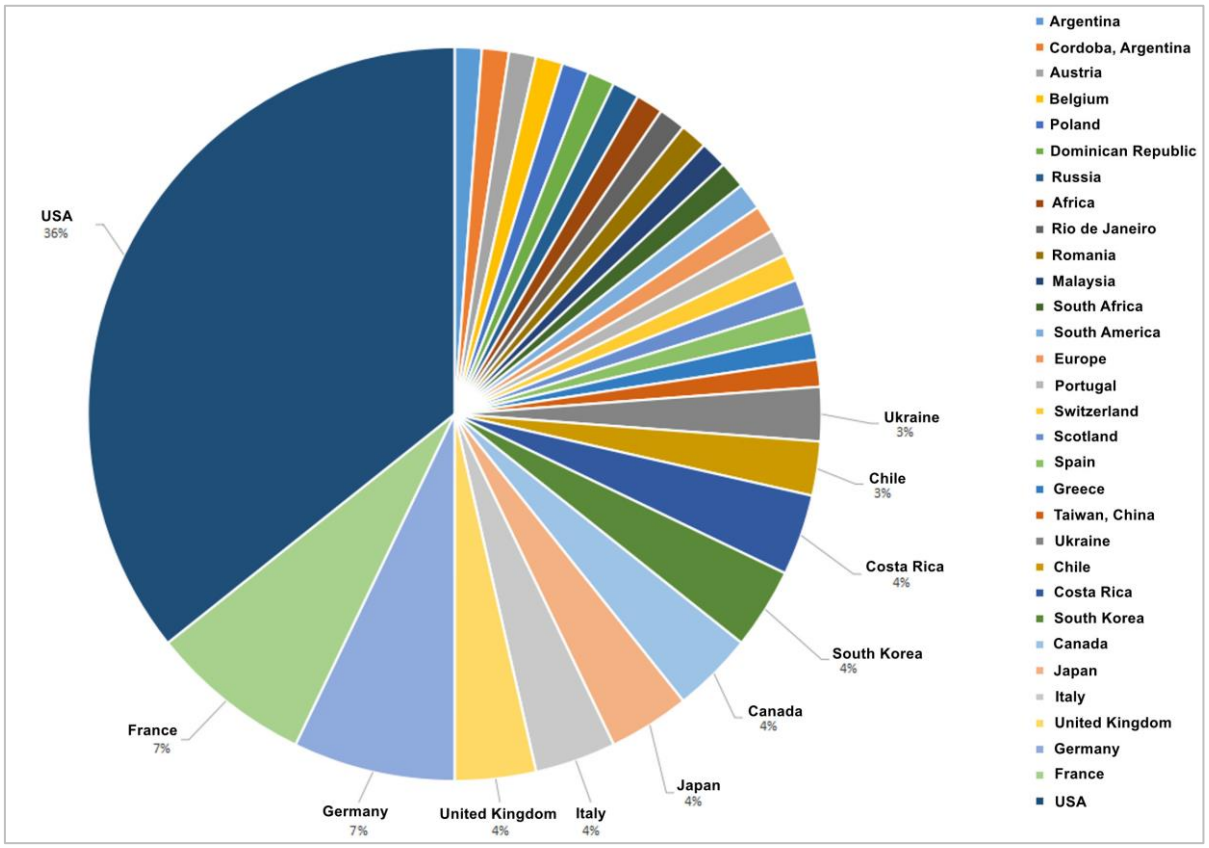


Figure 4.3 Distribution of extortion incidents by country

In terms of the distribution of ransomware victim industries, the government and enterprise, healthcare, energy, transportation, and education industries account for the top 50%, with the government and enterprise industry as the biggest target.

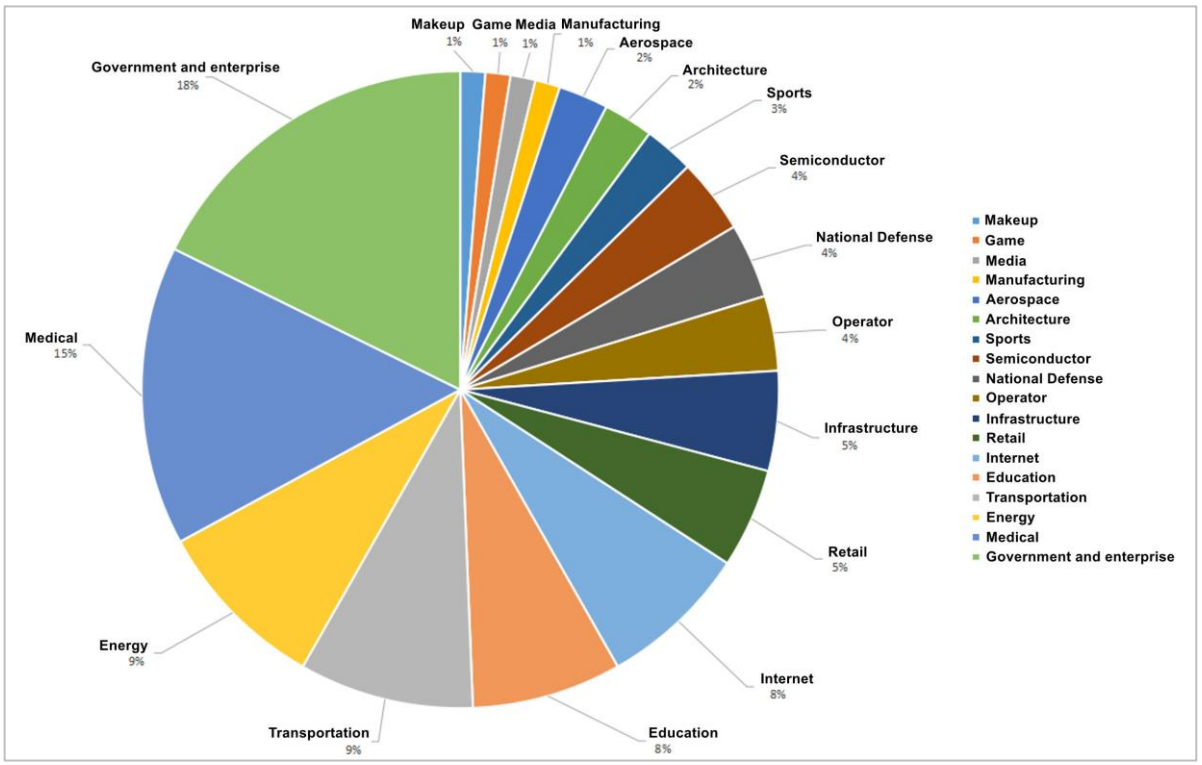


Figure 4.4 Ransomware victim Industry distribution

4.2 Representative Ransomware Families of 2022

4.2.1 Lapsus$

Lapsus$ is a hacking group that buys 0-day vulnerabilities and bribes insiders to gain access to the target company's systems and then steals the sensitive data of the target company for economic gain. Because members of the Lapsus$ group often announce their targets and attacks in Portuguese and English in the Telegram channels created by the group, there is reason to suspect that members of the group may be from the aforementioned regions or native speakers of these languages.

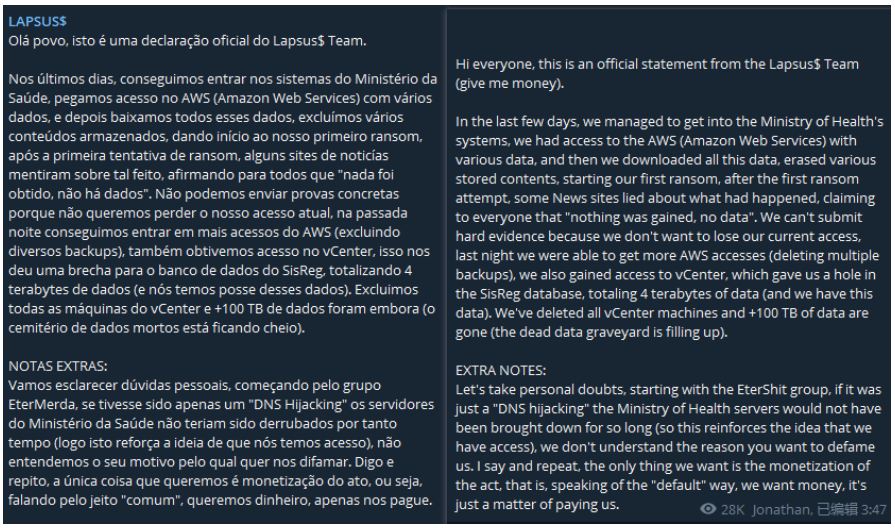


Figure 4.5 Lapsus$ releases information in two Languages

Lapsus$ groups primarily use social engineering techniques to collect information about the business operations of the target group, using various methods to obtain initial access to the target group, such as deploying password stealers, buying login credentials from illegal forums, buying off staff within the target group, and searching for public credentials in public code repositories.

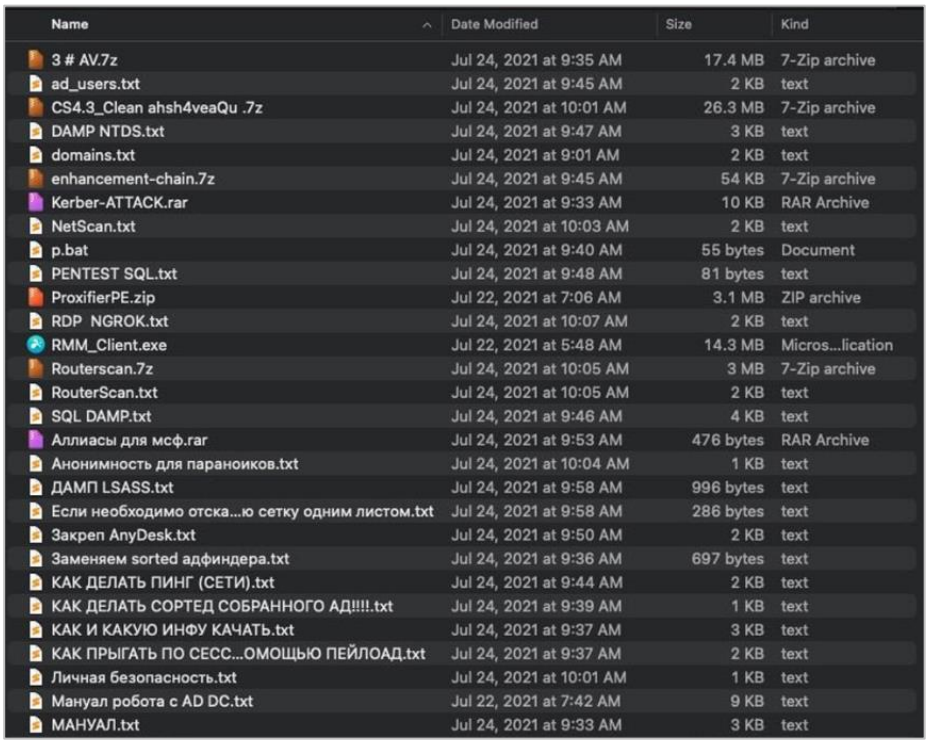
The Lapsus$ group employs a variety of strategies to discover other credentials or intrusion points to expand its access rights, such as exploiting unpatched vulnerabilities on internal accessible servers (including JIRA, Gitlab, and Confluence), searching code repositories and collaboration platforms to obtain public credentials and secrets, etc. Elevate privileges by using the Mimikatz tool or vulnerabilities in Confluence, JIRA, and GitLab.

Lapsus$ groups also utilize dedicated IT infrastructure to remotely download sensitive data from targeted groups for future extortion for economic benefit or public release to increase the group's visibility.

4.2.2 Conti

Conti is a Russian ransomware gang that began its extortion campaign in the summer of 2020 as Ryuk's successor. The Conti gang has carried out a number of attacks, such as compromising and encrypting important data from chip manufacturer Advantech and demanding a ransom of 750 BTC (about $14 million), compromising the U.S. Tulsa municipal network and publishing about 18,000 municipal documents, forcing the city to shut down its network and shut down its online bill payment system, utility bills, and email services. The city's website, council, police force, and more were all affected. However, the most egregious attack by the Conti gang was the attack on the Irish Department of Health's HSE, which encrypted 80% of its healthcare system, severely disrupted healthcare services, and leaked about 700 gigabytes of data containing a large number of Irish identities.

In March 2022, security researchers revealed the source code of the Conti ransomware. By deciphering the leaked files, it was possible to identify the files that the group used to scan and infiltrate the user manuals of different services such as SQL, RDP, Kerberos, and domain controllers.



Name	Date Modified	Size	Kind
3 # AV.7z	Jul 24, 2021 at 9:35 AM	17.4 MB	7-Zip archive
ad_users.txt	Jul 24, 2021 at 9:45 AM	2 KB	text
CS4.3_Clean ahsh4veaQu .7z	Jul 24, 2021 at 10:01 AM	26.3 MB	7-Zip archive
DAMP NTDS.txt	Jul 24, 2021 at 9:47 AM	3 KB	text
domains.txt	Jul 24, 2021 at 9:01 AM	2 KB	text
enhancement-chain.7z	Jul 24, 2021 at 9:45 AM	54 KB	7-Zip archive
Kerber-ATTACK.rar	Jul 24, 2021 at 9:33 AM	10 KB	RAR Archive
NetScan.txt	Jul 24, 2021 at 10:03 AM	2 KB	text
p.bat	Jul 24, 2021 at 9:40 AM	55 bytes	Document
PENTEST SQL.txt	Jul 24, 2021 at 9:48 AM	81 bytes	text
ProxifierPE.zip	Jul 22, 2021 at 7:06 AM	3.1 MB	ZIP archive
RDP NGROK.txt	Jul 24, 2021 at 10:07 AM	2 KB	text
RMM_Client.exe	Jul 22, 2021 at 5:48 AM	14.3 MB	Micros...lication
Routerscan.7z	Jul 24, 2021 at 10:05 AM	3 MB	7-Zip archive
RouterScan.txt	Jul 24, 2021 at 10:05 AM	2 KB	text
SQL DAMP.txt	Jul 24, 2021 at 9:46 AM	4 KB	text
Аллиасы для мсф.rar	Jul 24, 2021 at 9:53 AM	476 bytes	RAR Archive
Анонимность для параноиков.txt	Jul 24, 2021 at 10:04 AM	1 KB	text
ДАМП LSASS.txt	Jul 24, 2021 at 9:58 AM	996 bytes	text
Если необходимо отска...ю сетку одним листом.txt	Jul 24, 2021 at 9:58 AM	286 bytes	text
Закреп AnyDesk.txt	Jul 24, 2021 at 9:50 AM	2 KB	text
Заменяем sorted адфиндера.txt	Jul 24, 2021 at 9:36 AM	697 bytes	text
КАК ДЕЛАТЬ ПИНГ (СЕТИ).txt	Jul 24, 2021 at 9:44 AM	2 KB	text
КАК ДЕЛАТЬ СОРТЕД СОБРАННОГО АД!!!!.txt	Jul 24, 2021 at 9:39 AM	1 KB	text
КАК И КАКУЮ ИНФУ КАЧАТЬ.txt	Jul 24, 2021 at 9:37 AM	3 KB	text
КАК ПРЫГАТЬ ПО СЕСС...ОМОЩЬЮ ПЕЙЛОАД.txt	Jul 24, 2021 at 9:37 AM	2 KB	text
Личная безопасность.txt	Jul 24, 2021 at 10:01 AM	1 KB	text
Мануал робота с AD DC.txt	Jul 22, 2021 at 7:42 AM	9 KB	text
МАНУАЛ.txt	Jul 24, 2021 at 9:33 AM	3 KB	text

Figure 4.6 A list of leaked files from a portion of the Conti group

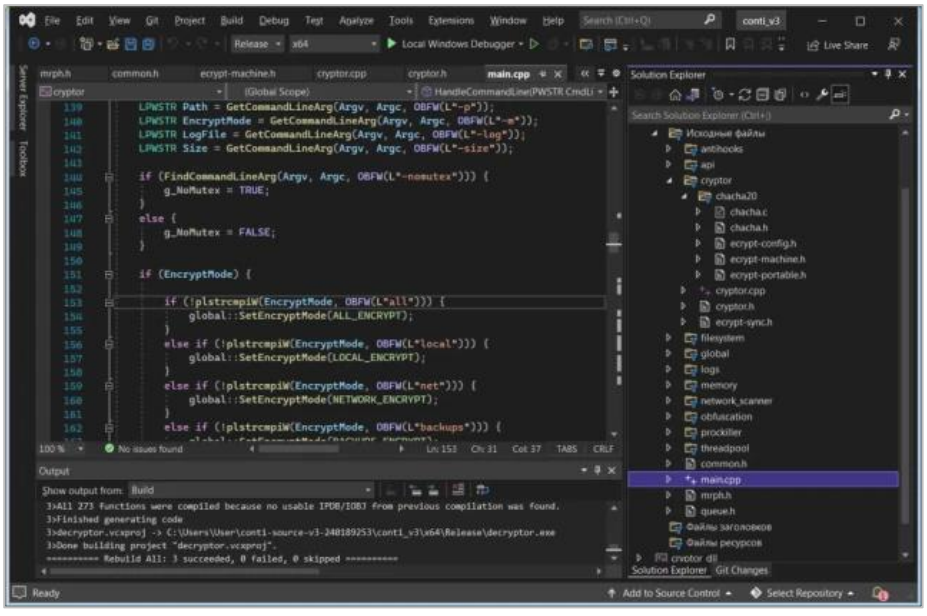
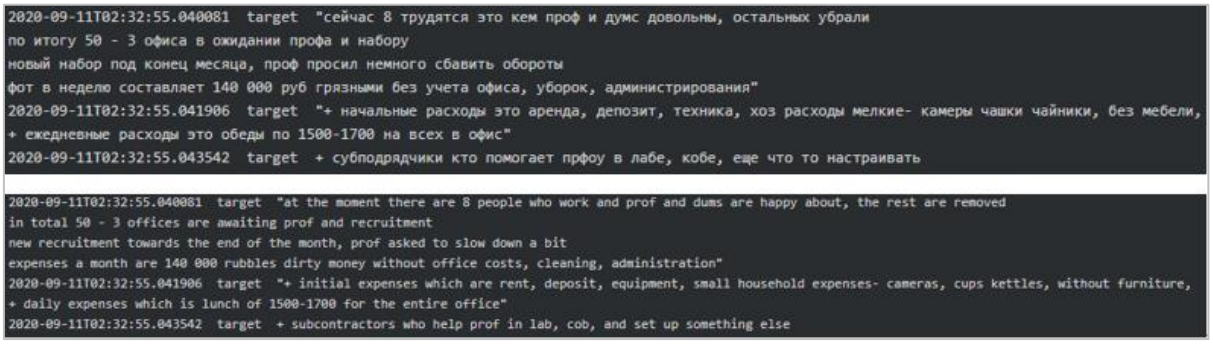


Figure 4.7 Leaked source code for a portion of the Conti group

Analyzing the leaks, it was found that Conti's organizational structure was no different from that of a normal software company, with a training team, coding engineers, reverse engineers, test engineers, etc. And employees have a stable salary and payday.



```
2020-09-11T02:32:55.040081  target  "сейчас 8 трудятся это кем проф и думс довольны, остальных убрали
по итогу 50 - 3 офиса в ожидании профа и набору
новый набор под конец месяца, проф просил немного сбавить обороты
фот в неделю составляет 140 000 руб грязными без учета офиса, уборок, администрирования"
2020-09-11T02:32:55.041906  target  "+ начальные расходы это аренда, депозит, техника, хоз расходы мелкие- камеры чашки чайники, без мебели,
+ ежедневные расходы это обеды по 1500-1700 на всех в офис"
2020-09-11T02:32:55.043542  target  + субподрядчики кто помогает прфоу в лабе, кобе, еще что то настраивать

2020-09-11T02:32:55.040081  target  "at the moment there are 8 people who work and prof and dums are happy about, the rest are removed
in total 50 - 3 offices are awaiting prof and recruitment
new recruitment towards the end of the month, prof asked to slow down a bit
expenses a month are 140 000 rubbles dirty money without office costs, cleaning, administration"
2020-09-11T02:32:55.041906  target  "+ initial expenses which are rent, deposit, equipment, small household expenses- cameras, cups kettles, without furniture,
+ daily expenses which is lunch of 1500-1700 for the entire office"
2020-09-11T02:32:55.043542  target  + subcontractors who help prof in lab, cob, and set up something else
```

Figure 4.8 Leaked chat logs from the Conti group

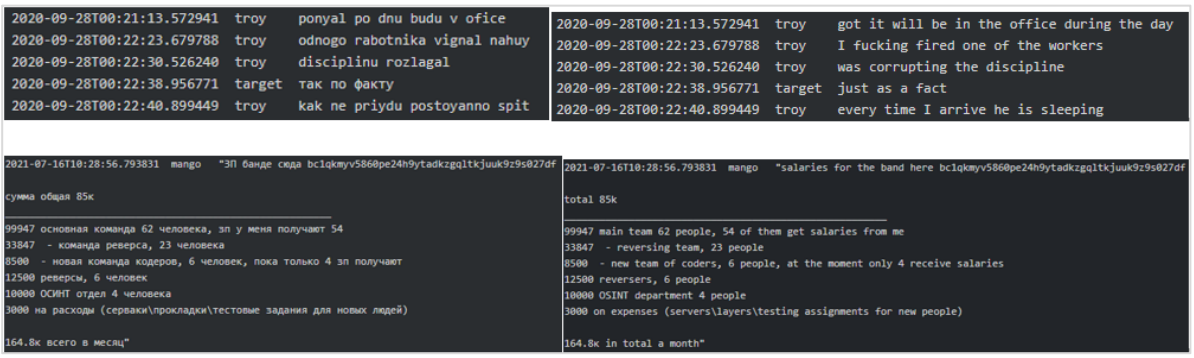


Figure 4.9 Conti organizes chats that are relevant to office and operations

On February 25, 2022, the Conti ransomware gang made a standby publishing a blog post announcing that they would fully support the Russian government's attack on Ukraine. They also warned that if someone organized a cyberattack against Russia, the Conti gang would fight back around critical infrastructure.

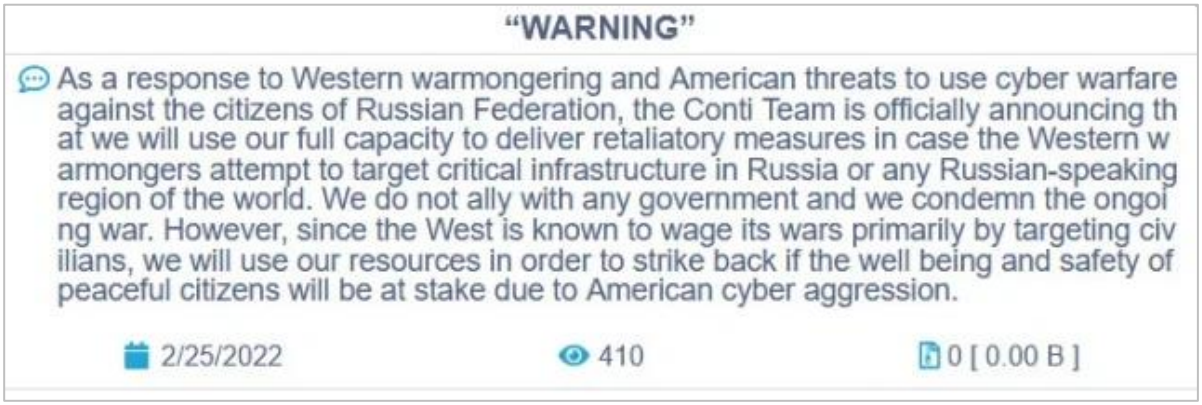


Figure 4.10 Warning message issued by the Conti group

4.2.2 LockBit

LockBit Ransomware was first observed in September 2019. After iterative development, LockBit 2.0 appeared in 2021, and LockBit 3.0 came out in June 2022.

LockBit establishes its initial access through purchased access credentials, unpatched vulnerabilities, insider infiltration, and 0-day exploits to establish control over the victim's host, collect network topology, and achieve its main goals of stealing and encrypting data.

LockBit uses a double-extortion model to get victims to recover their encrypted files by demanding a ransom and then making them pay again on the condition that the leaked data be published. When LockBit operates under a (RaaS) model, the Initial Access Broker (IAB) deploys first-stage malware or otherwise gains access within the targeted group's infrastructure. They then sell that access to multiple LockBit operators for secondary development.

With the advent of LockBit 3.0, its operators launched the first bug bounty program offered by ransomware gangs, where security researchers were rewarded with $1,000 to $1 million for submitting vulnerability reports of severity. This is also an important sign of the commercial operation of ransomware. In addition to bug bounty programs, LockBit operators also offer bounties for ideas or ideas that can improve ransomware. At present, LockBit' s bounty categories cover various platform vulnerabilities, its own software bugs, gang operation suggestions, doxing and other categories.

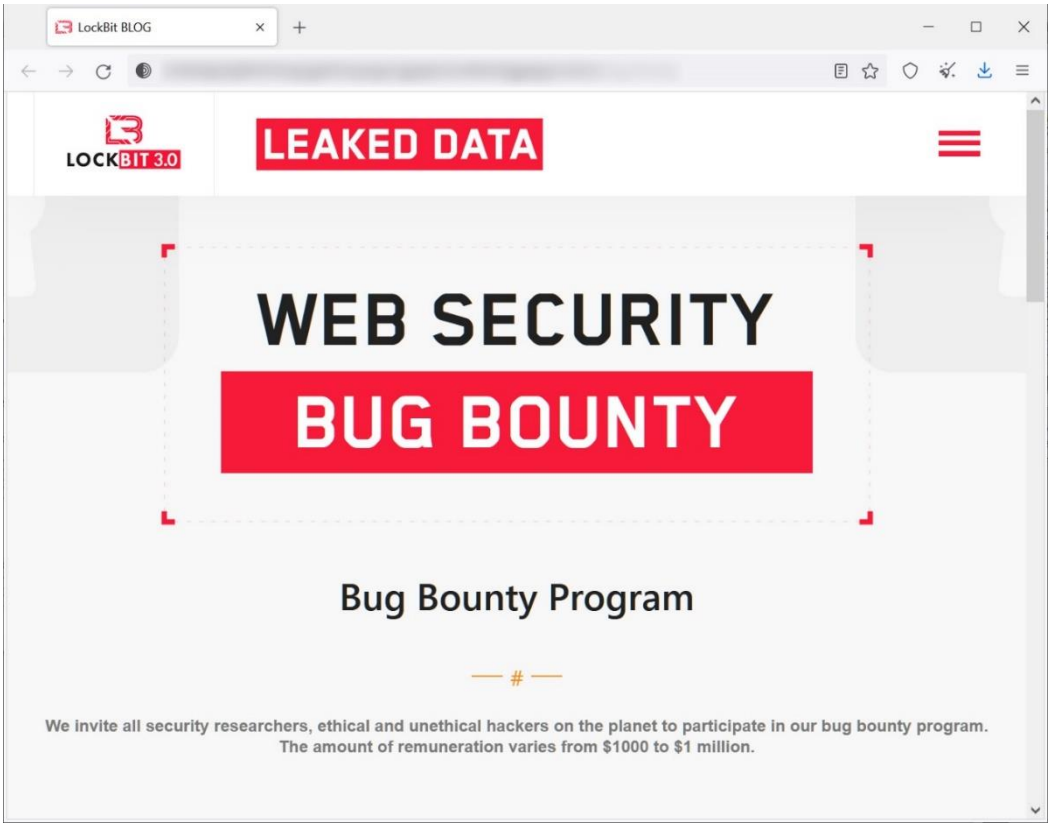


Figure 4.11 Bounty program page organized by LockBit

4.2.3 Hive

The Hive Ransomware was first spotted in June 2021. According to the report, it has grown to become one of the most prevalent ransomwares in the ransomware-as-a-service (RaaS) ecosystem. Hive ransomware-related attacks target a wide range of industries and critical infrastructure sectors, such as government, communications, and information technology, with a focus on healthcare and public health entities.

This year, the version of Hive developed by GoLang has been gradually switched to Rust, which has greatly improved the software functionality, operational efficiency, and confrontation ability of Hive. In the Rust version of the Hive software program, the developers modified the self-made encryption logic to avoid the encryption algorithm vulnerabilities in the previous version and added adaptation code to cover platforms such as VMWare ESXi. This switch has greatly enhanced the attack capability of the Hive ransomware gang, and NSFOCUS has observed a number of Hive attacks on virtualization platforms this year.

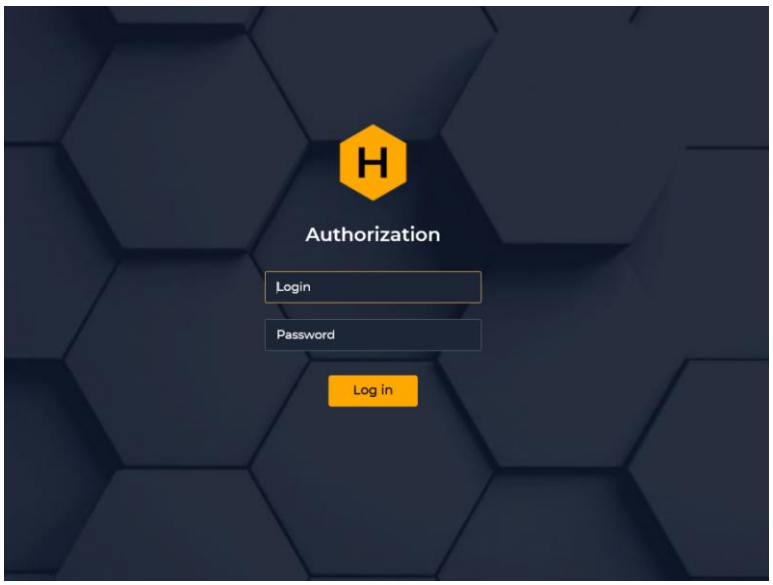


Figure 4.12 Hive personal login page on the dark web

4.3 Development of RaaS Models

The RaaS (Ransomware-as-a-Service) model in the ransomware space is a model of operating ransomware through a cooperative share of the economy, which can be traced back to GandCrab ransomware.

In the early days, the RaaS model was mainly achieved by selling ransomware usage rights and hiring communicators, and the relationship between ransomware operators and users was close to a transaction or employment relationship. The RaaS model of this period also integrated data theft and disclosure deterrence into the attack process, developing a 'double extortion' model: in addition to asking the victim to pay to unlock the data, they also disclosed some of the key data obtained during the attack on their own website, and threatened the victim to pay a large ransom or the full data content would be exposed.

In recent years, the RaaS model has evolved into a more mature partnership model and has become the standard industry model for ransomware groups. On the basis of 'double extortion', ransomware operators no longer sell software usage rights, but completely separate themselves from specific attack businesses, and recruit infiltration attackers to join the ransomware attack activities in the form of cooperative sharing. These infiltrators can use their own means and resources to compromise high-value targets and drop ransomware created by ransomware operators on the targeted devices to complete the attack. The ransom generated by a successful ransom campaign will be split between the ransomware operator and the attacker in a proportional manner.

This year, NSFOCUS Fuying Lab observed further changes in the RaaS model in terms of technology, mode, and system.

4.3.1 The Ransomware Operating Model is More Commercial

Ransomware operations have gradually evolved from simple gangs to corporations, and it is not difficult to find in Conti's leaked data that its organizational structure is no different from that of ordinary software companies, with training teams, coding engineers, reverse engineers, test engineers, etc. Employees also have stable wages and paydays, financial mobility needs and manpower management strategies.

With the advent of LockBit 3.0, its operators launched the first bug bounty program offered by ransomware gangs, where security researchers were rewarded with $1,000 to $1 million for submitting vulnerability reports of severity. This is also an important sign of the commercial operation of ransomware.

Ransomware gangs are also seeking change in ransom payments. The current payment method of choice for ransomware gangs is still cryptocurrency, but payment cryptocurrency tracking companies and relevant law enforcement agencies say that Bitcoin is traceable, and although Monero is a privacy coin, the vast majority of cryptocurrency exchanges in the United States do not sell it. As a result, ransomware gangs are starting to choose Zcash as an additional payment option, which is equivalent to adding a layer of financial security. Zcash is a privacy coin with hard-to-trace properties, and it is currently still being sold on Coinbase, the most popular cryptocurrency exchange in the United States, making it easier for victims to buy it for ransom payments. Ransomware gangs are expected to add more means of payment in the future.

4.3.2 Ransomware Countermeasures are More 'Advanced'

Since 2022, ransomware exploits have become more common. For example, the BlackByte ransomware gang uses techniques utilized by White Drive to assist in the spread. A CVE-2019-16098 vulnerability exists in one version of the MSI Afterburner RTCore64.sys driver, and the BlackByte ransomware gang exploited the vulnerability to disable thousands of security software drivers in order to bypass security software protections.

Vulnerabilities such as Office CVE-2022-30190, Exchange CVE-2021-26855, and Log4Shell CVE-2021-44228 were also widely used by ransomware attackers in 2022.

With the emergence of the 'bug bounty' program represented by LockBit, ransomware attackers will increase their ability to exploit all kinds of known vulnerabilities and even zero-day vulnerabilities in the future.

4.3.3 Ransomware Extortion Models are More 'Diverse'

This year, some ransomware groups have also upgraded their extortion models, from the previous dual extortion model of file encryption + data leakage to a triple extortion model, that is, three threat modes of file encryption, data leakage, and DDoS attacks are used to extort targets at the same time.

In June 2022, after the LockBit ransomware attacked digital security giant Entrust, the LockBit group exposed the stolen data on the website due to Entrust' s refusal to pay the ransom, which was subsequently hit by a DDoS attack. Inspired by this incident, the LockBit group claims to recruit members who are well-versed in DDoS attacks, adding the threat of DDoS attacks to the existing model, further pressuring victims to pay the ransom.

4.3.4 The Ransomware Ecosystem is More 'Industrialized'

Since 2022, as ransomware has become more and more RaaS (ransomware-as-a-service) of ransomware, some leading ransomware gangs have begun to use some development ideas that are close to the software industry to iterate and maintain their own software, resources, and services.

Ransomware gangs have even begun to tap into the power of the online community to help iterate on the software. For example, ransomware gangs openly solicit suggestions for software bugs and development in order to improve their attack tools and even use bonuses as bait.

To make ransomware attacks and data theft more efficient, ransomware groups are constantly developing new tools. For example, the LockBit group used publicly available tools such as FileZilla in its early attack campaigns, but later dissatisfied with the inefficiency of existing tools, developed a more efficient tool, StealBIT, to replace FileZilla.

The ransomware groups are also constantly strengthening their infrastructure construction. Take the LockBit group as an example. Currently, the group has 9 blog websites and their mirrors, 24 file websites and their mirrors that display evidence of intrusion, as well as 9 chat websites and their mirrors for communicating with victims, to cope with the rapidly expanding scale of its ransomware attacks.

This more 'industrialized' trend suggests that the number of ransomware attacks will continue to increase in the coming period, and the severity of ransomware attacks will further increase.

4.4 Insights

The threat of ransomware is long-standing. However, there is often a misconception that ransomware incidents tend to erupt suddenly and end just as abruptly, making them seem like a cyclical type of cyber threat. In reality, the sudden 'outbreaks' of ransomware are usually triggered by the disclosure of particularly severe cases—those that impact national interests or public welfare. Beneath these high-profile incidents lies the tip of the iceberg: a vast number of unreported ransomware attacks targeting various industries. With the explosive growth of the ransomware ecosystem, countless attackers have formed a persistent and dynamic network, exposing victims to the risk of secondary or even multiple rounds of extortion.

Ransomware threats have become a collection of security issues. Today, when attack chain components have been gradually modularized, there are various tools or means that are quite mature and highly replaceable in terms of intrusion, residence, propagation, and functional implementation. Ransomware groups only need to focus on operating a RaaS model to form their own attack system, combining ransomware attacks with credential compromises, exploits, and even botnets, DDoS attacks, and other threats form into more dangerous and complex cyber threats.

The business model of ransomware is evolving. The traditional model of ransomware only obtains ransom by encrypting data, but the proportion of ransom paid is not high. The aggrieved party often avoids paying sky-high ransom by backing up and restoring or by choosing to lose data. This has caused the long-term efforts of the ransomware gang, from intrusion, residence, dissemination to the completion of extortion, to fall short of success. On this basis, various ransomware gangs have gradually evolved a dual ransomware model, that is, stealing data before encrypting it. Even if there is a refusal to pay, hackers can still leak sensitive data as leverage for secondary threats. At the same time, this approach has also broadened the scope of the ransomware business.

At present, the defense against ransomware still needs to focus on anti-penetration. Blackmail, as a purposeful means, often has a very weak ability to spread on its own, which requires the assistance of other tools. Therefore, the fundamental goal of preventing and controlling ransomware is not to stop its operation, but to focus on how to prevent penetration and block the establishment of persistent collection capabilities, and to establish intrusion prevention and horizontal interception mechanisms.

5. APT Trend Prediction

This year, the drastic changes in the global political and economic situation have brought the number of advanced threat attacks to a record high, which also makes macro-observation and prediction of advanced threats particularly important.

NSFOCUS Fuying Lab predicts that advanced threat activities caused by geopolitical conflicts will continue to increase in the future. With the inevitable arrival of economic downturn and recession caused by the global interest rate hike turmoil, the probability of regional conflicts similar to this year will greatly increase, and the number of advanced threat activities such as cyber warfare and APT attacks will also increase with the increase of friction between countries and even become an important bellwether of regional conflict situations.

There will also be an increase in APT activity with cryptocurrencies as the target or means in the coming period. Due to the continued contraction of the cryptocurrency market due to the general tightening policy, APT groups targeting or monetizing through cryptocurrencies will intensify their attacks and exploits on the cryptocurrency industry in the coming period in order to squeeze the most out of the current period when the market remains relatively stable.

Some APT groups will strengthen their capabilities in cyber warfare. Affected by possible cyber warfare in the future, APT groups will continue to expand their capabilities in reconnaissance, surveillance, and sabotage, and improve their capabilities in new cyber warfare such as cognitive warfare and public opinion warfare, so as to enhance the value of their weapons in cyber warfare.

There will be an increase in APT attacks that disguise or hide identities. As the confrontation between attack and defense in the APT field becomes increasingly fierce, well-known APT groups may more widely use the camouflage tactics that emerged in the Russia-Ukraine cyber war and participate in some highly sensitive cyber-attack operations as unknown attackers with no characteristics.

There is a trend of APT groups modifying and using ransomware to carry out devastating cyberattacks. Because ransomware is often highly destructive and highly destructive, APT groups use this method to significantly reduce the risk of being attributed to the source while completing the intended paralysis operation. In the context of intensifying geopolitical conflicts, the combination of APT groups and ransomware may become more obvious in the future.

As an important economy and regional power, China will face more APT attacks in the future. Defenders at all levels need to build a more three-dimensional advanced threat defense system and focus on strengthening the new APT attack forms that have emerged recently, so as to ensure overall awareness and rapid response in the face of a possible APT overall offensive in China.

Appendix A About NSFOCUS

NSFOCUS, Inc., a pioneering leader in cybersecurity, is dedicated to safeguarding telecommunications, Internet service providers, hosting providers, and enterprises from sophisticated cyberattacks.

Founded in 2000, NSFOCUS operates globally with over 3000 employees at two headquarters in Beijing, China, and Santa Clara, CA, USA, and over 50 offices worldwide. It has a proven track record of protecting over 25% of the Fortune Global 500 companies, including four of the five largest banks and six of the world's top ten telecommunications companies.

Leveraging technical prowess and innovation, NSFOCUS delivers a comprehensive suite of security solutions, including the Intelligent Security Operations Platform (ISOP) for modern SOC, Volumetric DDoS Protection, Continuous Threat Exposure Service (CTEM) and Web Application and API Protection (WAAP). All the solutions and services are augmented by the Security Large Language Model (SecLLM) and other cutting-edge research achievements developed by NSFOCUS.

Appendix B About Fuying Lab

It focuses on research of security threat monitoring and countermeasure technologies, covering emerging fields such as APT advanced threats, Botnet, DDoS countermeasures, popular service vulnerability exploitation, black-gray industry chain threats and digital assets.

The research goal is to master the existing network threats, identify and track new threats, accurately trace and counter threats, reduce the impact of risks, and provide strong decision support for threat confrontation.

Adopting the research mode of combining cutting-edge technology exploration with actual combat confrontation, it has assisted national institutions in cracking several APT attack cases, taken the lead in discovering 8 new APT attack groups in the world and handled more than 40 APT attack incidents involving China, making outstanding contributions to major national cybersecurity.