Recorded Future®

By Insikt Group®

Current Trends in the Turkish-Language Dark Web

CTA-2023-0112

We analyzed advertisements, posts, and interactions within Turkish-language hacking and cybercrime forums to explore the capabilities, culture, and organization of these communities. This report is a follow-up to our previous reporting on the state of the Turkish-language dark web as part of a series analyzing cybercriminal communities in Brazil, Russia and China, Japan, and Iran. It will be of greatest interest to organizations and geopolitical analysts seeking to understand the cybercriminal underground in order to better monitor security-related threats, as well as to those researching the Turkish-language underground.

Executive Summary

Turkey's increasingly unstable financial situation, with record inflation rates and a plummeting Turkish lira, has created conditions for disenfranchised young people to join underground communities and engage further in cybercriminal activities. We found that Turkish patriotic hacking collectives are continuing their defacement operations and at least 1 threat group is working to engage in more sophisticated hacking activities. Turkish-language cybercriminals are active on English- and Russian-language forums where they share and sell compromised data from Turkish entities. In our research, we identified at least 3 Turkish-language ransomware groups and we developed a YARA rule to detect TurkStatik Ransomware.

With the prevalence of ransomware-as-a-service (RaaS) models and the resulting decrease in barriers for entry to the ransomware space, we expect an increase in the number of Turkish-language ransomware groups. As a cornerstone of the Turkish underground community, we expect patriotic hacking collectives to continue their operations.

Key Judgments

- Turkish patriotic hackers continue their defacement operations targeting countries they perceive to be "enemies" of Turkey, and in some cases aim to ramp up the sophistication of their activities including leaking confidential data and building a hacktivist botnet.
- Turkish-language, financially motivated threat actors advertise their services, methods, and stolen data on popular global forums to avoid Turkish law enforcement attention and appeal to a larger audience.
  We identified at least 3 Turkish-language ransomware variants being used by threat groups including TurkStatik, SifreCikis, and DeadLocker. At the time of this report, we do not know the number of victims in Turkey affected by these ransomware variants as the operators of said ransomware do not operate extortion websites.

Background

As outlined in our previous reporting, Turkish-speaking dark web communities primarily focus on 2 functional areas: patriotic hacking (hacktivism) and financially motivated cybercrime. Patriotic hacking communities frequently respond to geopolitical events around the world, especially those relating to

Turkey, and show support for the government agenda by targeting countries perceived to be "enemies" of Turkey. Financially motivated communities focus on a variety of fraud-related activities such as payment card fraud, data breaches, and social engineering. Due to pressure from law enforcement, Turkish-language forums do not host content, data, or methods targeting Turkish organizations. A majority of the compromised data and attack methods targeting Turkish organizations are found on English- or Russian-language forums like BreachForums, XSS, and Exploit.

Increased political and financial instability in Turkey are likely contributing factors to the popularity of dark web forums and financially motivated cybercrime. Researchers have argued for a correlation between financial instability (particularly youth unemployment) and cybercrime rates, using the case study of Nigeria as an example. On October 3, 2022, data from the Turkish Statistical Institute (TUIK) showed that inflation levels hit a 24-year high with 83.45% inflation, while independent experts at the Inflation Research Group (a private research group in Turkey) estimate the annual rate to be much higher at approximately 186.27%. Despite high inflation rates, the Central Bank of the Republic of Turkey has been pursuing an unorthodox easing cycle approach by lowering interest rates. As a result, the Turkish lira lost 44% of its value against the dollar in 2021, and the lira hit an all-time low in September 2022 with a further 100-point reduction in interest rates. The rising cost of living combined with the volatile financial situation continues to impoverish Turkey's youth.

Threat Analysis

Patriotic Hacking and Hacktivism

Some Turkish-language underground forums focus on patriotic, vigilante hacking activity such as defacement operations against foreign entities at times of international political disputes. While individual patriotic hacktivism exists, multiple forums host hacking collectives commonly referred to as "tim" (in English, "team"), including Anka Red Team on Turk Hack Team Forum, and Ayyıldız Tim on Ayyıldız Forum. These forums have sections dedicated to sharing news and evidence of operations. Patriotic hacking activities include defacing websites with ideological messages or imagery, rendering websites or services unavailable by distributed denial-of-service (DDoS) attacks, and compromising internal data. Forum members provide evidence of websites they defaced by providing links to the mirrors of defaced websites via defacement archives such as Zone H.

***Figure 1**: Ayyıldız Forum's homepage proclaiming Ayyıldız Team to be "Turk's Cyber Army", with subheading "Beyond this it's either freedom or death" (Source: Ayyıldız Forum)*

Turkish-language hackers do not express concern for government action if they get caught breaching the infrastructure or websites of foreign organizations. Underground discussions indicate that members of the Turkish-language forums assume the Turkish government will show leniency toward their patriotic hacking activities as long as they are not directed at domestic entities. Occasionally, however, we have seen targeting of domestic entities and individuals who have expressed views in opposition to official state positions.

As detailed in our previous reporting on the Turkish dark web, common targets for patriotic hacking activity include websites from countries that are perceived to be "enemy" states due to historical conflicts, such as Greece and Armenia, as well as websites and services from countries such as Germany and France, which the Turkish government has had turbulent ties with due to contemporary political events.

We observed an increase in the number of Russian websites targeted by patriotic hacktivist groups in the last 10 months since the beginning of Russia's invasion of Ukraine, including Anka Red Team allegedly compromising data from multiple Russian organizations on May 19, 2022. The organizations affected by the so-called "special operation" include the Ministry of Economy of Russia, the Federal Security Service of the Russian Federation, the Federal Council of the Russian Federation, the Federal Assembly of the Russian Federation, and Russian business professionals. The targeting of Russian entities reflects Turkey's unique position in the Russo-Ukrainian conflict and its complex relationship with both countries. Despite Turkey's military and political ties to Russia, Turkish defense firm Baykar has been a provider of Bayraktar drones to the Ukrainian military, with Ukrainian President Volodymyr Zelenskyy announcing on September 12, 2022 that Baykar is planning to build a factory in Ukraine. Turkey also hosted 4-way talks in Istanbul between officials from Turkey, Russia, Ukraine, and the

United Nations (UN) to discuss the safe export of Ukrainian grain in July 2022. Likely as a result of Turkey's official stance as a neutral country and the global support for the Ukrainian cause, Turkish patriotic hackers have ignored President Erdogan's close ties with Russian President Vladimir Putin.

Anka Red Team

***Figure 2**: "Cyber coat of arms" for Anka Red Team (Source: Turk Hack Team Forum)*

Anka Red Team, sometimes referred to as Turk Hack Team (THT), is a patriotic hacking threat group operating primarily out of the Turk Hack Team Forum. Similar to other Turkish-language patriotic hacking groups, Anka Red Team uses nationalistic imagery and rhetoric. Their hacktivist activity primarily includes defacement operations and occasional leaks of compromised data. Anka Red Team records their defacement operations on Zone H under the username "ZoRRoKiN", and other defacement archives under the username "TurkHackTeam". Anka Red Team uses the forum's "Gövde Gösterisi" ("Show of Force") section to announce new victims. Active members of Anka Red Team include "P4$A", "OBT is HeRYerDe", and "Safak-Bey".

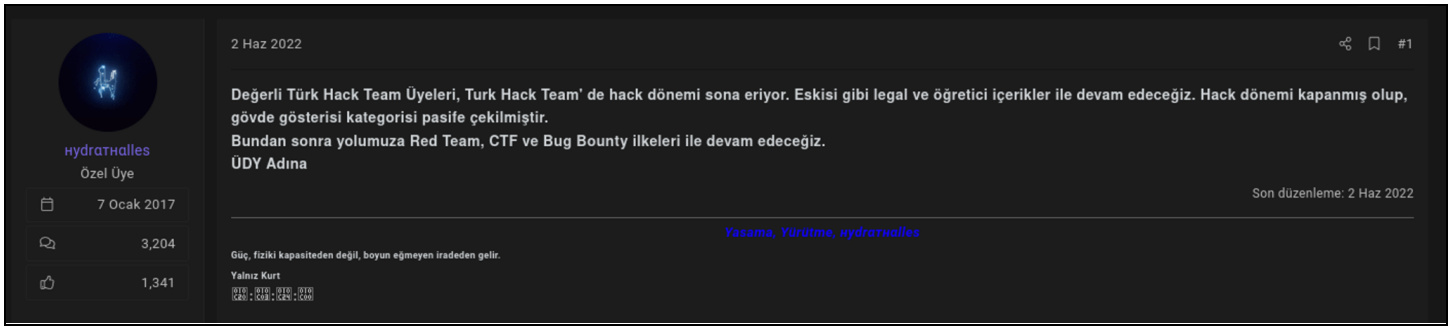

***Figure 3**: Turk Hack Team announces that they are stopping hacking and defacement activities (Source: Turk Hack Team Forum)*

On June 2, 2022, "Hydrathalles", a member of Turk Hack Team Forum, announced that Anka Red Team would not be engaging in any further "hacking" activities, including defacements, and that the Show of Force section of the forum would no longer be active. The user stated that Turk Hack Team Forum would continue to share "legal and educational" content. On October 15, 2022, "Bermuda", an administrator of the forum, created a new thread where they proclaimed that Anka Red Team would recommence its hacking activities due to "the current situation". While the threat actor did not specify what the current situation is, this phrase might refer to Turkey's involvement in multiple geopolitical conflicts including the Russo-Ukrainian War and Turkey's increased tensions with Greece. The threat actor explained that while it appeared that Anka Red Team was not active, they were working in the background to overcome "legal issues", and that after installing stricter rules for the Show of Force section, the team could safely continue their operations. In the same thread, Bermuda emphasized the need for more sophisticated attack vectors including obtaining and leaking source codes and databases from victim websites, DDoS attacks, infecting devices with malware, and adding infected devices to the "THT Botnet Network". The new rules for the Show of Force section state that team members who are able to maintain persistence via backdoors on infected devices will be added to a "special operations team". Defacing or otherwise harming Turkish websites and carding activity is expressly prohibited by the administrators.

The period immediately before and after Hydrathalles's statement that Anka Red Team would stop hacktivist operations was marked with a decrease in defacement activity by Anka Red Team (see Figure 4). Coinciding with Bermuda's announcement, we observed a sharp spike in the number of defacement victims posted by Anka Red Team on Zone H, primarily relying on SQL injection attacks.

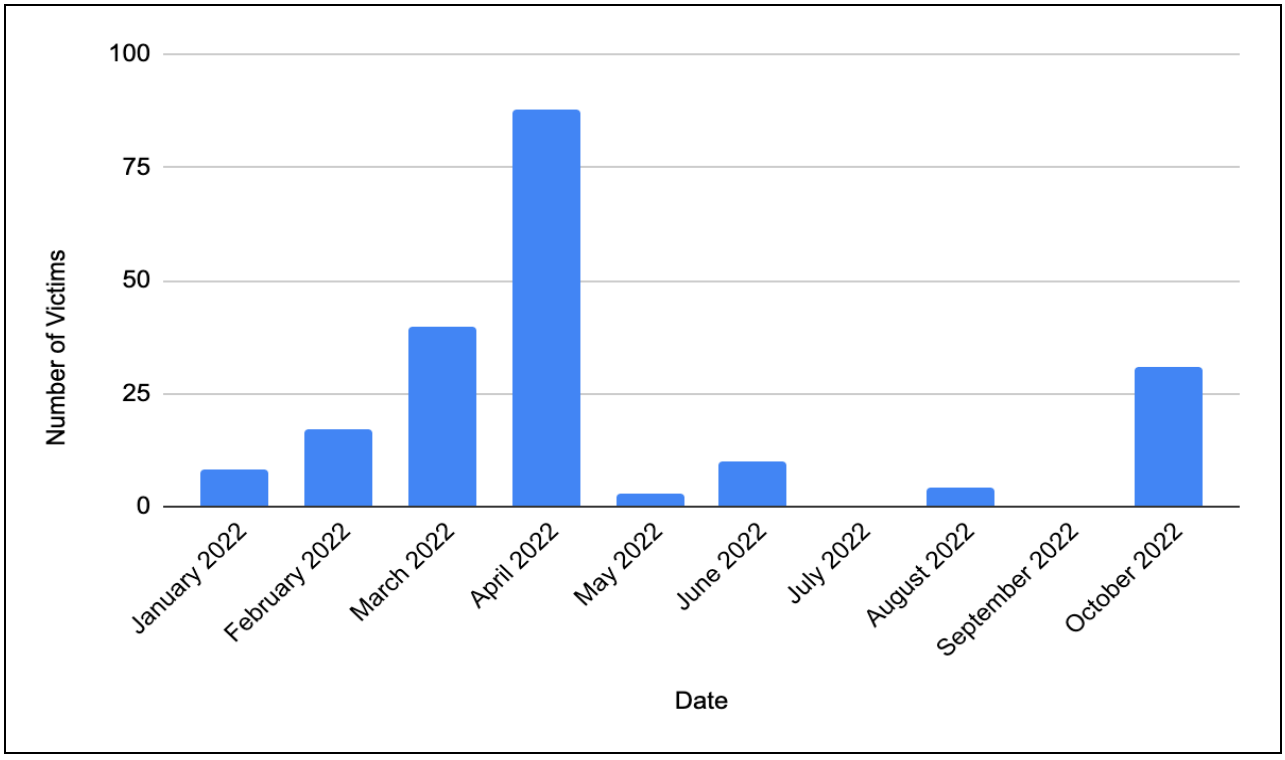

***Figure 4**: Overview of Anka Red Team's defacement victims between January and October 2022 (Source: Zone H)*

Ayyıldız Team

***Figure 5**: "Cyber coat of arms" for Ayyıldız Team (Source: Ayyıldız Forum)*

Ayyıldız Team is a patriotic hacking threat group primarily operating out of Ayyıldız Team Forum. In addition to nationalistic imagery, Ayyıldız Team uses military terms to refer to its operations (such as "Offensive Teams" or "Special Operations") and military ranks to organize its members. The threat group is primarily focused on defacement operations. Active members of Ayyıldız Team include "Orion-Pax", "AYDOĞAN", and "Toyonzade".

Cybercrime and Fraud Trends

We find that the trend of Turkish-language threat actors targeting international entities more than domestic entities persists. All Turkish-language forums we investigated have forum rules that prohibit targeting Turkish entities or releasing documents that will negatively affect the Turkish government's reputation or national interests. We did discover Turkish-speaking threat actors selling databases or initial access to Turkish organizations on popular, non-Turkish sources including the forums Exploit, XSS, and BreachForums.

Initial Access Sales to Turkish Organizations

Threat actors require remote access to compromised networks to conduct successful attacks such as data exfiltration attacks or espionage campaigns. Initial access brokers (IABs) are threat actors who specialize in selling compromised access methods on dark web and special-access forums. As detailed in our previous reporting, IABs are crucial elements in successful ransomware attacks. Top-tier forums XSS and Exploit are the primary sources where IABs advertise access methods and provide access to compromised corporate virtual private networks (VPNs), Citrix gateways, remote desktop protocol (RDP) services, corporate webmail servers, and content management systems (CMSs).

Most initial-access method advertisements do not mention the victim company or organization by name to avoid detection and attribution by law enforcement. Instead, threat actors provide details on the following parameters: “victim country”, “annual revenue”, “industry”, “type of access”, “rights”, “data to be exfiltrated”, and “devices on local network”.

According to our research, threat actors found to be selling initial access to entities in Turkey include the following 3 monikers on Exploit Forum: “zirochka”, “shear”, and “SubComandanteVPN”. These threat actors are prolific initial access sellers and target organizations across multiple geographies and industries. Appendix A of this report includes a detailed table (Table 2) of initial access sales from organizations in Turkey that we have observed in the last 6 months.

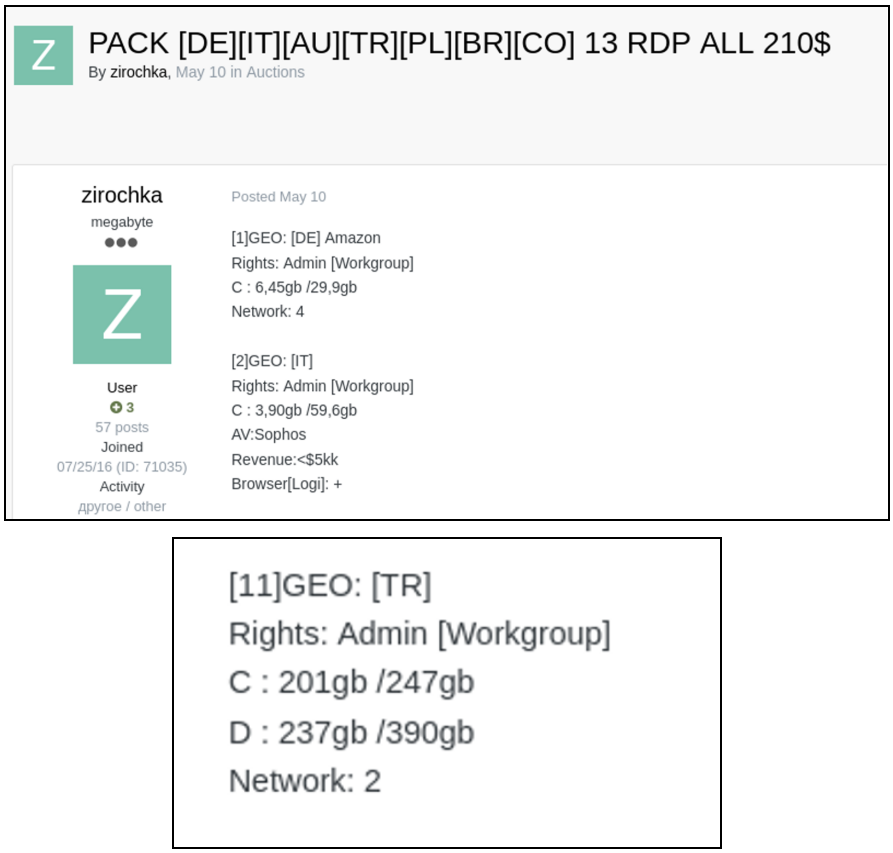

Figure 6: *Threat actor zirochka advertising initial access to organizations in 13 countries, including an organization in Turkey (Source: Exploit Forum)*

Compromised Data Sales

Threat actors are able to obtain confidential data from Turkish organizations and companies through a variety of attack vectors, including exploiting vulnerabilities in web applications to access data by means such as SQL injection, network intrusions, and phishing attacks. Data obtained via these attack vectors are shared or sold on dark web and special-access sources and can be used for fraud or other financially motivated attack vectors such as credential stuffing.

We found that threat actors targeting Turkish organizations did not advertise stolen data on Turkish-language forums. Instead, they shared or sold compromised Turkish data primarily on English- or Russian-language forums, thereby avoiding scrutiny from Turkish domestic law enforcement and reaching a larger audience. These dark web and special-access sources include top-tier forums XSS and Exploit, mid-tier BreachForums, and various public and private Telegram channels. Appendix B of this report includes a detailed table (Table 3) of compromised data sales from organizations in Turkey that we have observed in the last 6 months.

Opportunistic threat actors that frequently target Turkish entities include those who are active on the Telegram channel "數據洩露 | Leak Data | Data Leak Breach" and the associated Telegram user "MooT" (@MooTnew). Since June 2022, there have been approximately 20 listings shared in this Telegram group advertising compromised data from Turkish companies. While this is a significant number of victims from Turkey, the Telegram group shares dozens of other listings every week and members do not appear to be targeting particular geographies. As such, we do not believe the threat actor or group running the Telegram account is targeting Turkey in particular. However, we suggest monitoring the "Messaging Platforms — Cyber" source type for mentions of brands of interest in order to be notified of any victims shared on Telegram channels such as this one.

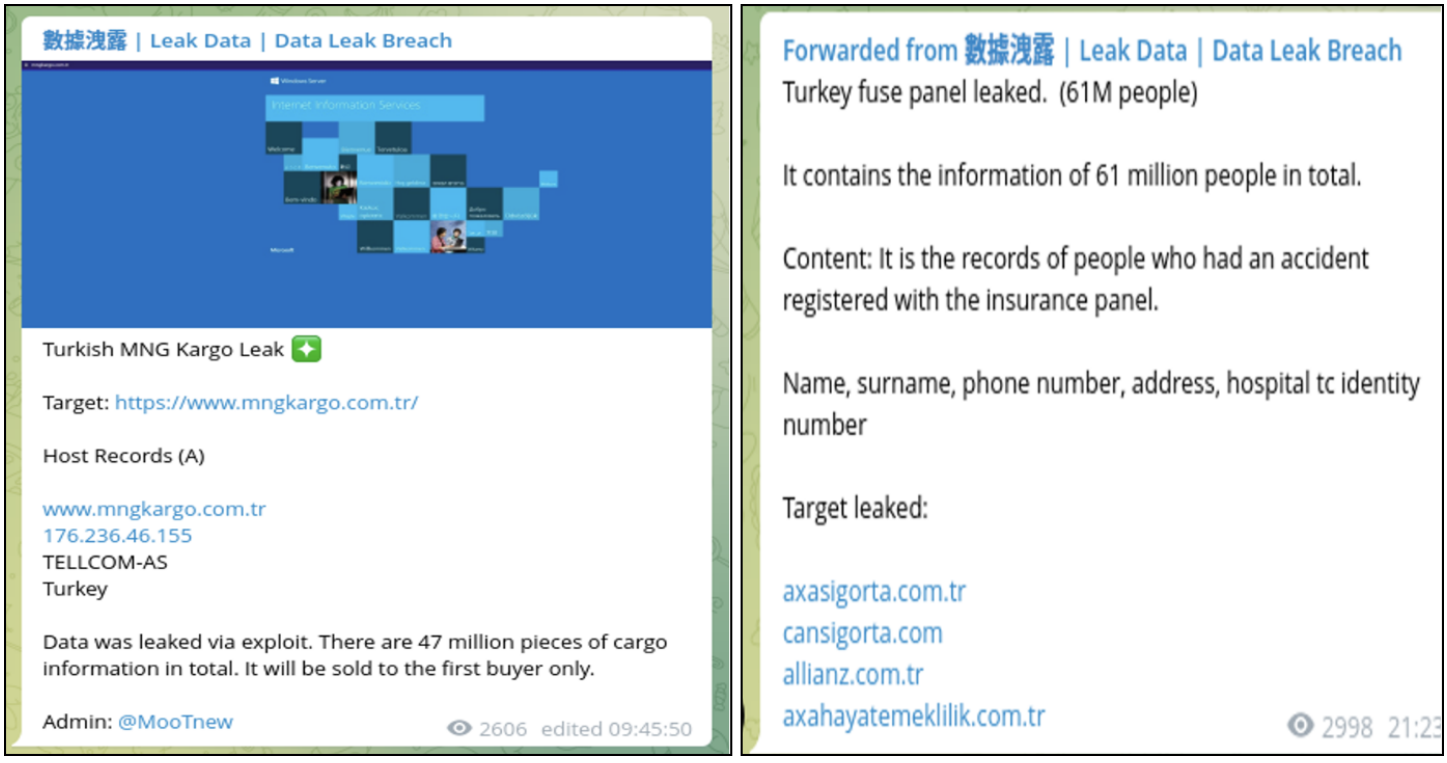

Figure 7: *Compromised data from Turkish companies being advertised on the Telegram channel "data_leak_breach" (Source: 數據洩露 | Leak Data | Data Leak Breach)*

Other threat actors that target Turkish organizations include "saderror" on BreachForums as well as "xssisownz" (also known as "Str0ng3r" on BreachForums), who is active on the forums BreachForums and XSS. The threat actor saderror has shared multiple databases from Turkish organizations including:

- A 17.3 GB database from Turkey's Police Organization (Emniyet Genel Müdürlüğü)
- A database containing employee data from Vestel (vestel[.]com[.]tr), a home appliances manufacturer headquartered in Turkey
- A database from Eysis (eysis[.]io), a Turkish learning management website
- A log file from albumdunyasi[.]org, a Turkish website for sharing music
- Records of personal information for Turkish political leaders, including Turkey's President Recep Tayyip Erdoğan, such as national identity numbers, physical addresses, and identity registration cities

The threat actor xssisownz was selling the following databases from Turkish organizations and websites on BreachForums and XSS:

- A 76,000-record database related to Risale-i Nur Forum (risaleforum[.]net), a Turkish-language religious and Islamic lifestyle forum, for $250
- A database for the Turkey-based fitness and wellness shop Bigjoy Sports (bigjoy[.]com[.]tr) for $100
- A 15 GB, 120 million-record database related to Sinoz Kozmetik (sinoz[.]com[.]tr), a Turkish cosmetics brand, for $500

Ransomware

According to open-source intelligence and Recorded Future's ransomware victim data, Turkey is a prominent target for ransomware attacks. Sophos's report, The State of Ransomware 2022, notes that approximately 60% of the survey respondents in Turkey were targeted by ransomware in the past year and that the average cost of rectifying the attack was $370,000 USD. According to CheckPoint, in 2020 Turkey was the 5th-most targeted country in ransomware attacks, behind Russia, Sri Lanka, India, and the US.

Recorded Future data shows that as of October 2022, 9 organizations from Turkey had their names published and/or data leaked on ransomware extortion websites in 2022 (Figure 8). LockBit Gang was the primary threat group responsible for attacks against Turkish organizations; however, ransomware attacks are opportunistic in nature and ransomware groups target victims primarily based on profitability. Therefore, we do not believe that any of these groups, including LockBit Gang, were targeting Turkish organizations in particular.

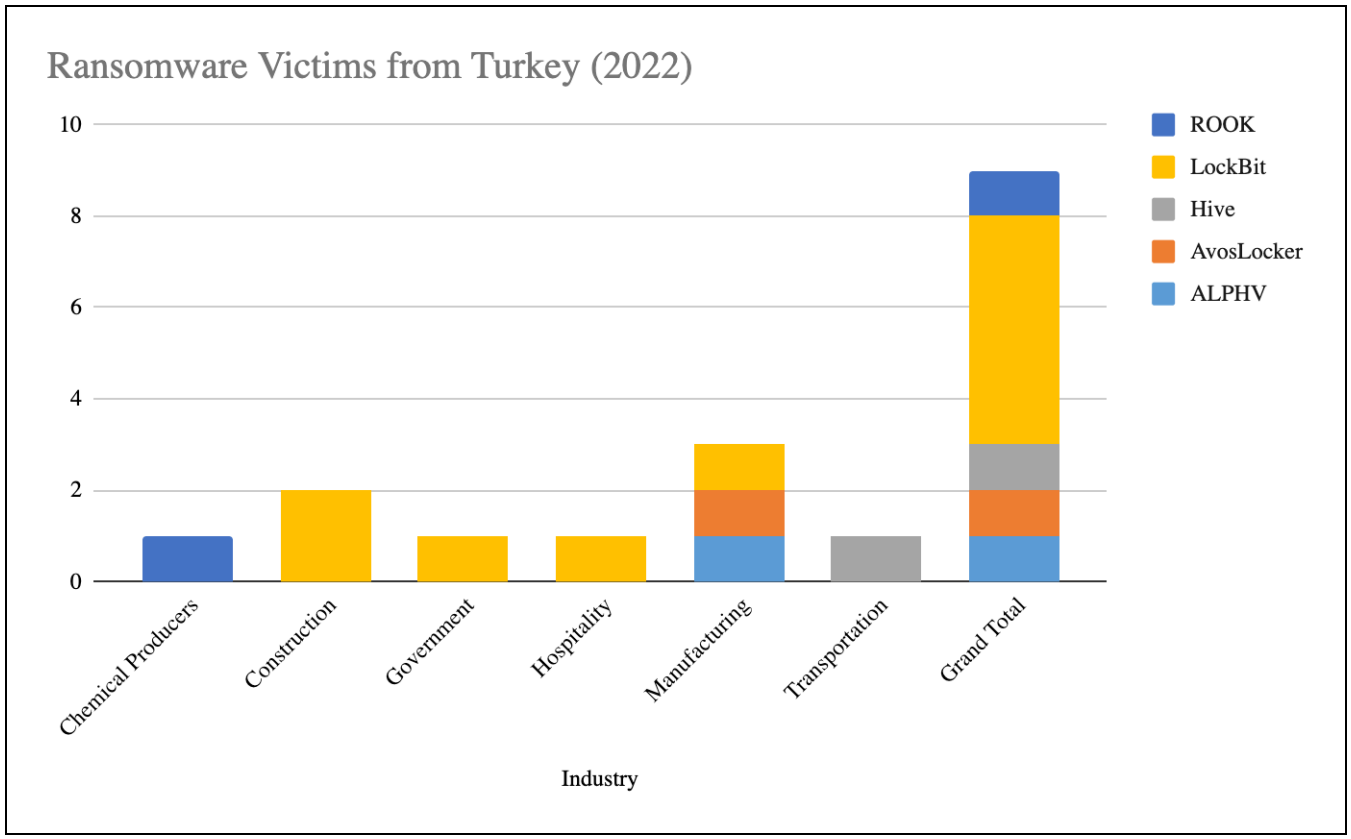

Figure 8: *Overview of Turkish organizations whose data was leaked on ransomware extortion websites in 2022 (Source: Recorded Future)*

We found multiple Turkish-language ransomware strains and threat groups as part of our research, including TurkStatik ransomware, SifreCikis ransomware, and DeadLocker ransomware. According to the ransom notes and infected files we found, these ransomware strains have infected victims in Turkey in the past 6 months; however, the victims were not listed publicly since these ransomware groups do not have ransomware extortion blogs.

TurkStatik Ransomware

TurkStatik ransomware was first referenced on November 22, 2019, when a security researcher, @malwareforme (Jack), reported about its capabilities to encrypt victims' files, appending them with the ".ciphered" extension. TurkStatik is Turkey-specific ransomware designed to target Turkish-speaking victims. It encrypts victims' files using the Rijndael 256 algorithm and drops a Turkish-language ransom note titled "README_DONT_DELETE.txt" onto the victim's system. The ransom note states that all of the victim's data has been encrypted and claims that the only way to recover the files is to pay the ransomware operators behind the infection. The ransomware operators include the email addresses decservice@mail[.]ru and recoverydbservice@protonmail[.]com as points of contact. Emsisoft created a decryption tool for TurkStatik ransomware.

SifreCikis Ransomware

SifreCikis is another ransomware that targets Turkish-language victims. First observed on November 10, 2020, it encrypts victim data by appending files with a random pattern extension. The Turkish-language ransom note instructs victims to contact the SifreCikis operators via the email nitas811@protonmail[.]com to pay a $500 ransom, and also references the currently defunct TOR website address sifrecikx7s62cjv[.]onion. SifreCikis ransomware was reportedly spread via spam campaigns and malware infections.

DeadLocker Ransomware

As reported by MalwareHunterTeam on April 21, 2022, DeadLocker is a ransomware that encrypts victims' files by appending the file extension type to ".deadlocked". The malware prompts the victim device to display a pop-up that contains the ransom note, written in Turkish, which instructs the victim to contact a Discord account (ParadoX#8495) to obtain payment details (Figure 9). The requested ransom amount varies from $300 to $650 in Discord Nitro, which is the credit system used in the Discord application to purchase a premium membership or other add-ons. It is important to note that "BattleLocker" ransom notes with the same visual style and formatting have also been discovered. This indicates that DeadLocker and BattleLocker are different names given to the same off-the-shelf ransomware strain used by less technically proficient actors. Additionally, the fact that the primary method of communication is a Discord account and the payment is requested in Discord currency indicates that the threat actors operating the malware are likely less sophisticated and young individuals focused on improving their financial status within the Discord application.

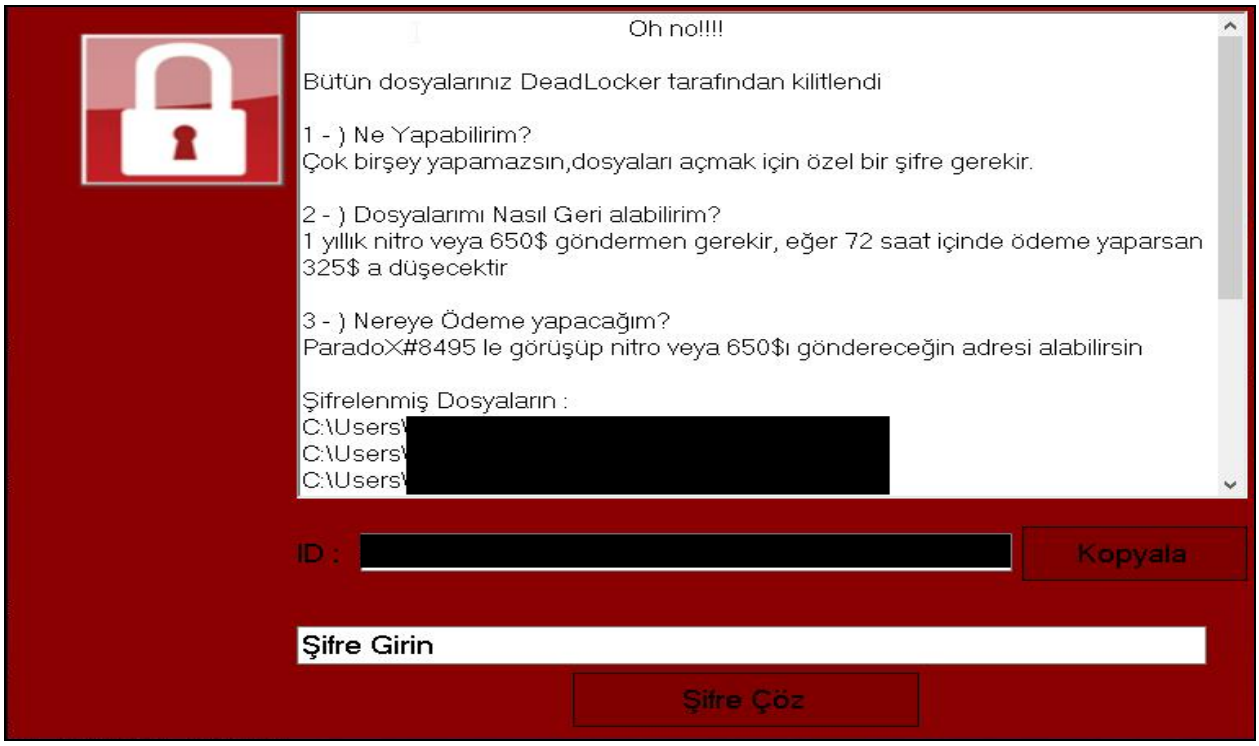

***Figure 9**: A ransom note written in Turkish from "DeadLocker" ransomware (Source: MalwareHunterTeam)*

In addition to the ransomware strains mentioned above, we discovered a victim page from an unnamed ransomware group with a ransom note (Table 1) written in Turkish. The ransom note instructs the victim to log on to a victim payment dashboard (Figure 10) using a custom identification number. The payment dashboard contains payment details including the recipient's Bitcoin (BTC) address and guidance on how to obtain cryptocurrency in Turkey. The ransom price is $250 USD. The language proficiency and Turkey-specific URLs embedded in both the ransom note and the payment dashboard indicate that the operators of the ransomware are native Turkish speakers.

Ransom Note in Turkish	Translation
DOSYALARINIZ SIFRELENDI..! 250 $ KARSILIGINDA DOSYALARINIZIN SIFRESINI COZECEK DCRYPTER YAZILIMINI ALABILIRSINIZ. ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ ~~~~~~~~~~~~~~~ PC ID : [REDACTED] 'NIZ ILE SITEMIZDEN BIZE ULASABILIRSINIZ... SITEMIZ : [REDACTED] ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ ~~~~~~~~~~~~~~~ SITEMIZ SADECE TOR BROWSER ILE ACILMAKTADIR. TOR BROWSER INDIRME ADRESI : https://www.torproject.org/tr/download ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ ~~~~~~~~~~~~~~~ DATA KURTARMA SERVISLERI YADA PROGRAMLARI KULLANMAK ISTERSENIZ LUTFEN DOSYALARINIZIN YEDEGINI ALINIZ.. ALDIGINIZ BU YEDEKLER UZERINDE ISLEM YAPINIZ VEYA YAPTIRINIZ.. DOSYALARINIZI SILMEYINIZ VE ISIMLERINI DEGISTIRMEYINIZ. ASIL DOSYALARINIZIN BOZULMASI.. VERILERINIZIN KURTARILAMAYACAK SEKILDE ZARAR GORMESINE NEDEN OLACAKDIR. ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ ~~~~~~~~~~~~~~~ SITEMIZE ERISEMEMENIZ DURUMUNDA LUTFEN BELIRLI ARALIKLARLA TEKRAR TEKRAR KONTROL EDIN.	Your files have been encrypted..! You can buy the dcrypter software that will unlock your files for $250. PC ID: You can contact us using your id [REDACTED] on our site. Our Site: [REDACTED] Our website is only accessible via Tor browser. You can download Tor at this address: https://www.torproject.org/tr/download If you want to use data recovery services or programs please make a backup of your files. Use data recovery on these backups. Do not delete or change the names of your files. This will cause your original files to be corrupted and your data to be harmed in an unsalvageable way. If you can't access our website please keep checking in intervals.

***Table 1**: Turkish ransom note left on victim's device after it was infected by an unidentified encrypter malware (Source: Recorded Future)*

***Figure 10**: The victim dashboard from an unidentified Turkish-language encrypter malware or ransomware (Source: Recorded Future)*

Outlook

We expect patriotic hacking groups to continue to target state and private entities whose political agenda diverges from the official Turkish state course. These threat actors will continue to deface websites, breach servers, and steal or leak databases of countries that oppose the Turkish state in the international arena. We will continue to monitor patriotic hacking communities for any escalations in attack vectors.

Ransomware-as-a-service (RaaS) models decrease the barriers for entry to the lucrative ransomware space, which is likely an alluring prospect for unemployed or low-earning Turkish nationals looking to engage in cybercriminal activity. As such, there will likely be an increase in Turkish-language ransomware groups of varying technical sophistication, from young gamers looking to earn pocket change to more operationally secure ransomware operators targeting small to medium-sized businesses. We recommend that organizations take necessary mitigation measures against ransomware attacks including implementing YARA rules to identify malware via signature-based detection.

Sources for this report include the Recorded Future® Platform and open-web and dark web research.

Appendix A: Initial Access Sales

Threat Actor	Intelligence
"sganarelle2"	On October 13, 2022, sganarelle2, a member of the top-tier forum Exploit, was auctioning Kerio Control access with administrator privileges to an unspecified Turkish company with over $50 million in annual revenue and 250 employees. Kerio Control is a unified threat management firewall. According to the threat actor, they obtained access to a 1.79 TB database with documents in the corporate cloud as well as some other internal system data and functionality: • Interfaces • Traffic rules • Intrusion prevention • Security settings • Bandwidth management • Content filter • Proxy server (reverse proxy) • Antivirus rules (http scanning, FTP scanning, email scanning) • DHCP Server (enable, disable) • DNS (enable, disable DNS forwarding) • Accounting and monitoring • Remote services (SMTP relay, dynamic DNS, remote backup) • List users (enable, disable, edit, grant or revoke admin rights) • List groups (enable, disable, edit, grant or revoke admin rights) • SSL certificates (add, remove, distrust, import, export) • IP address groups (organize, add, edit, remove) • Services (add, edit, remove) • Check logs The starting price is $300 or it can be purchased immediately for $2,000. The credibility of sganarelle2 is high: the operator has authored 485 threads and posts since registering their account in March 2011. The account has received 49 endorsements and has many indicated sales on the forum.
"K_E_N_Z_O"	On September 11, 2022, K_E_N_Z_O, a member of the top-tier forum Exploit, was auctioning access with local administrator privileges to the network of an unspecified Turkish travel agency headquartered in Istanbul with $18 million in annual revenue. The travel agency is described as operating in 145 countries and 4,000 offices. Based on the details provided by the threat actor on the forum, OSINT indicates that the victim organization is likely Vista Tourism & Travel A.S. (vistatourism[.]com). The starting price is $800 or it can be purchased immediately for $1,500. The credibility of K_E_N_Z_O is low: the operator has authored 9 threads and posts since registering their account in August 2022. The account has not received any feedback on the forum.
"shear"	On August 30, 2022, shear, a member of the top-tier forum Exploit, was auctioning access to an unnamed Turkish online retailer that sells automotive parts and processes in approximately 15 transactions per month. The starting price is $100 or it can be purchased immediately for

Threat Actor	Intelligence
	$500. The credibility of shear is high: the operator has authored 75 threads and posts since registering their account in March 2015. The account has received 1 endorsement and has many indicated sales on the forum.
“19cm”	On August 19, 2022, 19cm, a member of the top-tier forum Exploit, was auctioning RDP access with workgroup administrator privileges to the network of 4 international organizations, one of which is headquartered in Turkey: • An unspecified Turkish company with $5 million in annual revenue. According to the threat actor, the networks of 2 organizations are secured with Quick Heal antivirus software and they obtained access to the data stored in local networks. The starting price is $600 or all 4 networks can be purchased immediately for $1,000. The credibility of 19cm is low: the operator has authored 4 threads and posts since registering their account in August 2022. The account has received no endorsements on the forum.
“zirochka”	On August 11, 2022, zirochka, a member of the top-tier forum Exploit, was selling RDP access with local administrator and domain user privileges to the network of an unspecified luxury beach hotel in Turkey with $5 million in annual revenue. According to the threat actor, the compromised network is secured with ESET NOD32 antivirus software. The starting price was $50 or it could be purchased immediately for $70. The credibility of zirochka is high: the operator has authored 57 threads and posts since registering their account in July 2016. The account has received 4 endorsements on the forum and has many indicated sales.
“orangecake”	On June 18, 2022, orangecake, a member of the top-tier forum Exploit, was selling shell access to multiple networks of international organizations, including a company in Turkey: • Access with domain admin privileges to an unspecified company in Turkey with $84 million in annual revenue that specializes in business service. The compromised network is secured with Trend Micro antivirus software. The threat actor requested $800 for the access. The credibility of orangecake is high: the operator has authored 21 threads and posts since registering their account in September 2021. The account has received 10 endorsements from high-profile threat actors on the forum and has several indicated sales.
zirochka	On May 13, 2022, zirochka was auctioning RDP access to 13 entities for $210, one of which is a Turkish organization with the following description: • Amazon Athena Workgroup access to an unspecified Turkish company with approximately 450 GB of data to be exfiltrated and 2 devices on its local network.

Threat Actor	Intelligence
	The credibility of zirochka is high: the operator has authored 56 threads and posts since registering their account in July 2016. The account has received 4 positive endorsements on the forum and has many indicated sales.
"Nei"	On May 12, 2022, Nei, a member of the top-tier forum Exploit, was auctioning VPN and RDP access with administrator privileges to an unnamed Turkish chemical company with approximately $20 million in annual revenue. The starting price is $600 or it can be purchased immediately for $1,200. The credibility of Nei is high: the operator has authored 40 threads and posts since registering their account in March 2021. The account has received 10 positive endorsements on the forum and has several indicated sales.
"shelltrades"	On May 3, 2022, shelltrades, a member of the top-tier forum Exploit, was auctioning access to an unspecified Turkish online retailer that processes approximately 13 transactions per day and has 9,000 lifetime orders. According to the threat actor, there are approximately 10,000 users in the database. The starting price is $1,200 or it can be purchased immediately for $1,600. The credibility of shelltrades is unknown: this is the only thread the operator has authored since registering their account in June 2021. The account has not received any feedback on the forum.
"nopiro"	On April 28, 2022, nopiro, a member of the top-tier forum Exploit, was selling unspecified access with domain administrator privileges to the networks of a Turkish company that specializes in steel and energy distribution as well as logistics services with approximately $4 billion in annual revenue. According to the threat actor, they compromised approximately 15,000 hosts in the network. nopiro did not specify the prices openly and requested that potential buyers reach out to them via TOX ID 04586CFD37076013CBE95853BE62E5A6499DFC718DB30CF9B9D9CADD4873D902991C5018E818. The credibility of nopiro is low: the user registered their account in April 2022 and has authored 4 threads and posts on the forum.
"wiseguy01"	On April 24, 2022, wiseguy01, a member of the top-tier forum XSS, was selling VPN access to the network of an unspecified Turkish university for $2,000. According to the threat actor, the compromised network contains 2,046 devices and 4 open ports: 3389, 80, 443, and 8080. The credibility of wiseguy01 is low: the user registered their account in April 2021 and has authored 29 threads and posts, with primarily negative feedback on the forum.
"69.pdf"	On April 7, 2022, 69.pdf, a member of the top-tier forum Exploit, was

Threat Actor	Intelligence
	auctioning RDP access with domain administrator privileges to a Turkish biotechnology and pharmaceutical company with more than $1 billion in annual revenue. The threat actor also gained access to the administrator's folder called "Network", IP addresses, device information, and more. The starting price for the access was $15,000 or it could be purchased immediately for $25,000. The credibility of 69.pdf is low: the user registered their account in January 2022 and has not received any feedback on the forum.
"Neophyte"	On March 21, 2022, Neophyte, a member of the top-tier forum Exploit, was auctioning PulseSecure VPN access to an unnamed Turkish furniture accessories manufacturing company with a 40-year history, $217 million in annual revenue, and 800 employees. The starting price is $1,000 or it can be purchased immediately for $2,000. Based on the threat actor details, OSINT indicates that the victim organization is likely Samet S.R.L (samet.com[.]tr). The credibility of Neophyte is low: the operator has authored 21 threads and posts since registering their account in February 2021, but has few indicated sales.
shear	On March 8, 2022, shear, a member of the top-tier forum Exploit, was auctioning domain access to the website of a highly-rated Turkish mobile application that allows users to send and receive money. According to the threat actor, the application is available on Google Play and has over 100,000 lifetime installations. According to the threat actor, the access does not include access to the website or application databases. The starting price is $100. As of this writing, there has been at least 1 bid on the auction, raising the price to $150.

Table 2: *An overview of initial access brokers' advertisements targeting organizations in Turkey in the last 6 months (Source: Recorded Future)*

Appendix B: Compromised Data Sales

Threat Actor	Intelligence
"saderror"	On October 19, 2022, saderror, a member of mid-tier BreachForums, was sharing (8 forum credits to access) a database from Vestel (vestel[.]com[.]tr), a home appliances manufacturer headquartered in Turkey. The database contains approximately 10,000 records and includes Vestel employees' names, phone numbers, job titles, and location data. The threat actor claims they obtained the data in 2022. The credibility of saderror is moderate: the operator has authored 37 threads and 106 posts since registering their account in September 2022. The account maintains a positive reputation score of 23.
"Paulsan"	On October 7, 2022, Paulsan, a member of mid-tier BreachForums, was sharing a database from Netas (netas[.]com[.]tr), a telecommunications technology company headquartered in Turkey. The database is shared in 3 parts and contains internal documents and a database that contains the following: employee names, phone numbers, identification (ID) numbers, and names of Netas clients. The threat actor has shared other "data packs" that were obtained from the victim data posted previously on BianLian Ransomware Group's extortion website. The credibility of Paulsan is low: the operator has authored 6 threads and posts since registering their account in October 2022. The account has not received any feedback on the forum.
"ML_GROUP"	On September 14, 2022, ML_GROUP, a member of the mid-tier BreachForum, was selling documents from Turkish ASB Group, a group of energy and petrochemical companies. The threat actor claims to be in possession of 70 GB of documents in various formats. The documents contain archives of mail messages, plans and projects, transactions, non-disclosure agreement (NDA) and maintenance data, and various documents including contracts in relation to Uganda, Iran, South Africa, Libya, and Russia. The price for the database is $850; the threat actor is accepting Monero (XMR) or BTC as payment. The credibility of ML_GROUP is low: the operator has authored 2 threads and 2 posts since registering their account in September 2022 and has received 30 endorsements on the forum.
"xainn"	On September 16, 2022, xainn, a member of the mid-tier BreachForums, was selling a 126 million-line database containing data related to Turkish citizens and their family members. The database contains personally identifiable information (PII) including full names, names of family members, places of birth, dates of birth, marital statuses, and other information. The threat actor claims to be in possession of 452 GB of documents in JSON format. The credibility of xainn is low: the operator has authored 1 thread and 1 post since registering their account in June 2022. The account has not received any feedback on the forum.
"data_leak_breach"	On August 31, 2022, a database from Yildiz Entegre (yildizentegre[.]com), a flooring manufacturer, was shared on the

	Telegram channel data_leak_breach. The download link for the database redirects to the forum Club Hydra Market. The credibility of the Telegram group data_leak_breach is moderate: the user is the administrator of the Telegram group "data_leak_breach" and its backup channels, which have more than 6000 subscribers. The channels are used to share or advertise compromised databases and access to organizations.
"MooTnew"	On August 22, 2022, a database containing customer data from MNG Kargo (mngkargo[.]com.tr), a shipping company, was shared on the Telegram channel "data_leak_breach" and interested buyers were asked to contact Telegram user "MooTnew". The post states that the data was leaked via exploiting a vulnerability in the company's systems and contains information on 47 millions pieces of cargo. The data was sold to a single buyer. The credibility of the user "MooTnew" is moderate: the user is the administrator of the Telegram group "data_leak_breach" and its backup channels, which have more than 6,000 subscribers. The channels are used to share or advertise compromised databases and access to organizations.
MooTnew	On August 11, 2022, a database containing customer data from multiple Turkish insurance companies was shared on the Telegram channel data_leak_breach and interested buyers were asked to contact Telegram user MooTnew. The post states that the database contains records for 61 million people who had an accident and were registered with one of the affected insurance companies. The affected companies are Axa Sigorta (axasigorta[.]com), Can Sigorta (cansigorta[.]com), Allianz (allianz[.]com[.]tr), and Axa Hayat Emeklilik (axahayatemeklilik[.]com[.]tr). The credibility of the user MooTnew is moderate: the user is the administrator of the Telegram group data_leak_breach and its backup channels, which have more than 6,000 subscribers. The channels are used to share or advertise compromised databases and access to organizations.
"0x_dump"	On July 4, 2022, a database from Tuttur (tuttur[.]com), a Turkish gambling website, was shared on the Telegram channel 0x_dump. The file has 500,000 rows and includes customer data including names and phone numbers. The credibility of the Telegram group "0x_dump" is moderate: the group has 488 subscribers and is used to share compromised databases from data breaches.
"Str0ng3r**"** (also known as xssisownz)	On May 3, 2022, Str0ng3r, a member of the mid-tier BreachForums, was selling a 76,000-record database related to Risale-i Nur Forum (risaleforum[.]net), a Turkish-language religious and Islamic lifestyle forum, for $250. Based on sample data and threat actor indications, the database includes emails and MD5-hashed passwords. The threat

	actor uses Telegram (@Tokugaw4) as their main point of contact. The credibility of Str0ng3r is moderate: the operator has authored 8 threads and 41 posts since registering their account in March 2022. The account has a positive reputation score of 10. The threat actor is a frequent contributor to a number of cybercriminal forums using the monikers “Tokugaw4”, “FuckerZ”, and xssisownz, among others.
“GokhanR00T”	On May 2, 2022, GokhanR00T, a member of mid-tier BreachForums, was sharing a database with 9 million records from Avea and Turk Telekom (turktelekom[.]com[.]tr), 2 telecommunications providers headquartered in Turkey. The leaked database includes users’ Turkish identity numbers and phone numbers. The threat actor uses the Telegram account @GokhanCarderSwats and the Discord account “Gokhan CarderSwats#8887” as primary methods of communication. The credibility of the threat actor is low: the operator has authored 54 threads since registering their BreachForums account in April 2022.
xssisownz	On April 18, 2022, xssisownz, a member of the top-tier forum XSS, was selling a database for the Turkey-based fitness and wellness shop Bigjoy Sports (bigjoy[.]com[.]tr). The exposed database includes data from over 55,000 customers. The threat actor did provide a sample of data from the database within this listing. The price listed for this database is $100 USD, and xssisownz is requesting that potential buyers message them directly via their Telegram username @Tokugaw4. The credibility of xssisownz is moderate: the operator has authored 28 threads and posts since registering their account in December 2019. The account has received 12 positive endorsements but has no indicated sales. xssisownz also maintained reputable accounts on the low-tier, now-defunct Raid Forums (FuckerZ and Tokugawa).
“ZouZic”	On July 25, 2022, ZouZic, a member of the top-tier forum Exploit, was leaking a 2020 database related to Fenerium (fenerium[.]com), the online shop of Fenerbahçe S.K., a professional soccer team from Turkey. The threat actor did not provide any further details about the nature of the compromised database. The credibility of ZouZic is high: the operator has authored 62 threads and posts since registering their account in December 2020. The account has received 1 endorsement and has several indicated sales on the forum.
“lyoxa”	On August 14, 2022, lyoxa, a member of the top-tier forum Exploit, was auctioning a bundle of valid payment cards: • Approximately 2,700 payment cards affecting the residents of Turkey. The threat actor indicated that the bundle is approximately 70% to 80% valid and that the information was harvested from an unspecified compromised online retailer on July 7, 2022. Additional compromised information includes physical and email addresses, telephone numbers, and more. The starting price is $13,500 or it can be purchased

	immediately for $20,000. The credibility of lyoxa is high: the operator has authored 66 threads and posts since registering their account in March 2015. The account has received 2 endorsements and has several indicated sales on the forum.
"copy"	On May 1, 2022, copy, a member of the low-tier BreachForums, was selling a 63,000-record database related to Tofisa (tofisa[.]com), a Turkish online retailer of Islamic women's clothing, including hijabs, dresses, and traditional clothing, for 8 BreachForums credits. Based on sample data and threat actor indications, compromised information includes user identification numbers (UIDs), email addresses, passwords, shipping addresses, and more. The credibility of copy is high: the operator has authored 71 threads and 81 posts since registering their account in April 2022. The account maintains a positive reputation score of 238.
xssisownz	On March 10, 2022, xssisownz, a member of the top-tier forum XSS, was selling a 15 GB, 120 million-record database related to Sinoz Kozmetik (sinoz[.]com[.]tr), a Turkish cosmetics brand, for $500. In addition to the database, the threat actor is also selling a 10 GB database related to the Sinoz Kozmetik subdomain for an additional unspecified fee. The threat actor indicated that of the 120 million records, 260,644 contain personally identifiable information (PII) and plaintext passwords related to Sinoz Kozmetik customers. The threat actor uses Telegram (@Tokugaw4) as their main point of contact. Based on the advertisement and the Telegram handle, we believe that it is likely that the operator of xssisownz is related to the threat actor or threat actor organization that operated the account "Tokugawa" ("FuckerZ") on the now-defunct Raid Forums. We have identified previous instances of this threat actor attempting to sell the Sinoz Kozmetik database but have seen no indication that any sale was made. In several instances, the threat actor re-posted the advertisement and replied to their own threads ("bumping") in order to draw attention to the advertisement, but has never received a public offer. The credibility of xssisownz is low: the operator has authored 3 threads and posts since registering their account December 2019. The account has not received any feedback on the forum.

***Table 3**: An overview of threat actors selling compromised databases from organizations in Turkey in the last 6 months (Source: Recorded Future)*

About Recorded Future

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.