Impact Zones: How cybercrime disrupts and shapes the landscape of data security

Claudia Alecsandra GABRIAN,
Babeş Bolyai University, Doctoral School of International Relations and Security Studies, Cluj-Napoca, Romania
claudia.gabrian@ubbcluj.ro

Abstract

In a highly networked digital world, cybercrime and data breaches are increasing together, putting up a strong front and proving to be a challenge for everyone: individuals, organizations, and governments. Cybercrime is associated with financially motivated attacks and one type of cyberattack that is one of the most prolific is ransomware. Objectives of the study: to analyze the disruption which destabilizes and breaks the system's normal functioning. The overall horizontal objective is to identify the activities that can breach data, cause financial losses, and also can influence the cybersecurity landscape. The paper is important in this topic area because knowing about cybersecurity is the key to knowledge, advancement of research, and practical application of solutions for society. Approach: strategies and regulations are always changing, and have the main role in protecting the data and responding to cyber-attacks; but unfortunately, cyber-attacks are more present and more advanced every day, and this involves different perspectives for this type of cyberattacks, in this paper the main methods are netnography, document analysis and the case study. The results show that a large number of interconnected devices in an Internet of Things landscape enhances vectors for attacking and amplifies the complexity of data security challenges. The following research will demonstrate the fact that ransomware attacks are a part of a huge disrupting type of cyberattack and represent a critical threat to data security and cybercrime has a major role in this topic. Also, an example of data leaks is a specific case study about one of the NSA officers who tried to send classified defense information to Russia, explaining that the Snowden case is not unique in the cybersecurity landscape.

Keywords: cyberattacks, ransomware, data leaks, darknet and social media marketplaces.

1. Introduction

Data security and cybersecurity in a particular way represent a suite of strategies and technologies aimed at protecting data from unauthorized access, in this case, cybercrime has a very important role because involves breaching the systems to access personal and sensitive data. Also, data leaks are closely related to data security because some people want to disclose information by intention. Firstly, cybercrime includes a lot of illicit activities, some of these activities are financially motivated attacks such as ransomware. In order to exploit at least one vulnerability in data security measures, ransomware in 2023 according to the ENISA report, was the first type of cyberattack will the most scale of attacks [1].

The most recent challenge in cybersecurity is to identify what type of cyberattacks increase their sophistication and malicious activity because represent a major challenge to experts, governments, and society. The interconnection between cybercrime and data security can be identified in various contexts, and one of these is the proliferation of interconnected devices using the Internet of Things (IoT) which represents a complexity challenge for cybersecurity. For a collective defense and to prevent these types of cyberattacks that are constantly evolving, is necessary to have a comprehensive approach that integrates technical defense, threat intelligence, and cybersecurity culture among people [2].

Cybersecurity has developed mechanisms to prevent and respond to the attacks. Categories of this have included a systemic procedure, for instance, an application security model to all the systems, whereby all best practices are included. On the other hand, data information and security levels are at stake since many cyberattacks seek to obtain all the data through unauthorized access. Securing data is another area entire of challenges regarding threats; security measures go a long way. Applied to these, data analytics play other roles in learning from existing threats in developing solutions for unknown threats toward these networks, infrastructures, data, and information. It would be collected in massive amounts, leading to the popular term "big data," signifying large datasets not only in size but also generated at a high rate, having heterogeneity, and that first and foremost is, in this complex environment, it will give valid findings or patterns. In each of these systems, is necessary to monitor the infrastructure for accurate functioning and to prevent, detect, and recover from cyber threats. There is a varying degree of supervision and management of such data with the varying degrees of prevention, detection, or recovery expected in the domain. Some domains are very preventive while others are very detective or recovery-based. In both cases, multiple types of datasets can be collected to provide intelligence about the cyber threats and evaluate user behaviors to prevent future threats or even to identify some insider propagating the threats [3].

2. Modern market sales for cybercrime

With Telegram becoming the most critical messaging application for very many people in the world, it is also becoming a hub for several cybercrime activities like sales and leaks of stolen personal or corporate data organization and operation of cybercrime gangs, distribution of hacking tutorials, hacktivism, and more. The Telegram messaging application has gained many users, thus making it a big challenge for security researchers in the war against cybercrime. The features that make Telegram appealing to cybercriminals are its purported built-in encryption and the ability to create channels and huge private groups. Tracing and monitoring criminal activities within the platform, though, becomes a challenging task for any law enforcement or security researcher because of these two characteristics. Furthermore, cybercriminals use coded language and alternative spellings to discuss their activities on the platform, making it quite difficult for security agencies to decipher their conversations. It is also used for the sale of stolen data and illicit goods through the recruitment of new members. The ability to remain anonymous while on Telegram is one of the main features that attract hackers to the platform. Registration of accounts without personal information makes it possible for most users to create multiple identities and easily engage in conversation without using their identity [4].

Many cybercriminals, including Discord, Jabber, Tox, and Wickr use several more chat applications. Each one offers a specific set of features and characteristics, but they all offer some level of furtiveness and protection that cybercriminals find attractive. It is a decentralized, secure application for messaging where one doesn't need to register or provide personal information; data is also encrypted through peer-to-peer technology and the NaCl library, with users identified by a Tox ID. Indeed, the Telegram channel is also the platform of preference for cybercriminals to sell and share just about any PII, from social security numbers, driver's licenses, and passports to dates of birth and physical and email addresses. Cybercriminals can then exploit this information to engage in fraud that leverages stolen identities, including taking up bank loans, for instance, and opening bank accounts. Many of the ransomware and data extortion groups are cybercrime gangs, using their net offense experiences to steal private data from organizations while threatening to publish it in return for ransom money from victims. Ransomware gangs encrypt information using ransomware, while data extortion groups, on the other hand, only steal the data [4]. When the war between Russia and Ukraine started, a lot of telegram groups appeared, one of these groups that posted important data leaks was "Data1eaks" in Russian.

Darknet is another market where data are posted and sold, these data contain full names, birthdates, social security numbers, credit card information, bank account details, email addresses, and passwords. Cybercriminals also trade medical records, driving licenses, and passport details. For example, payment card data costs around $10 and ranks as the most commonly found item on the darknet market. Mobile phone numbers and online accounts cost around the same amount. Cryptocurrency wallets and account login details attract more interest than bank accounts. Passport copies topped the list as the most expensive item, averaging around $600. While the prices for stolen information may seem high, the repercussions for individuals whose data is sold can be higher. People whose data gets sold online may face financial losses, damage to their credit scores, and identity theft [5].

3. Ransomware attacks

Ransomware is an extortion attack in which an attacker deprives a victim of their valuable organizational data until the attacker is paid. The ransomware groups are upping the ante now with an assortment of extortion tactics: posting sensitive information online if not paid. RaaS (Ransomware as a service) provides user-friendly tools for performing this act amateurishly and essentially widens the scope of ransomware for more would-be bad actors [6].

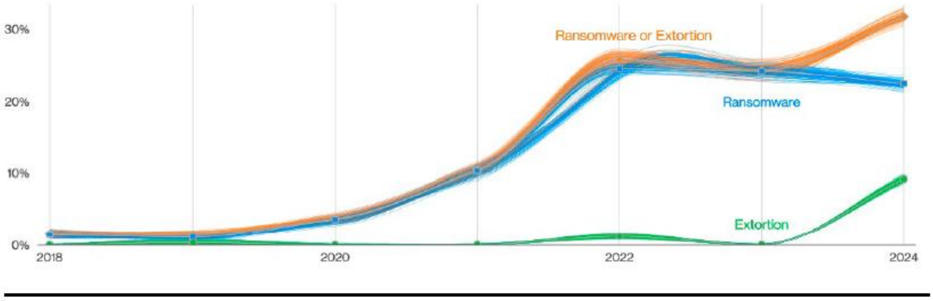


Fig. 1. Ransomware and Extortion breaches over time
Source: Verizon Business, "2024 Data Breach Investigations Report", 2024.

The chart indicates a steep increase in incidents with ransomware, beginning in the middle of 2019, cresting up through 2021, and stabilizing at a high level by the end of 2024. Extortion remained low until mid-2021 before it grew sharply, particularly in 2022. Both concatenated categories, "Ransomware or Extortion", show a similar trend from the Year 2021 and further increase until the Year 2024. This conveys the evolving and changing space of cyber threats: a somewhat scarily high level of ransomware attacks, and a significant rise in extortion instances that call for better security measures.

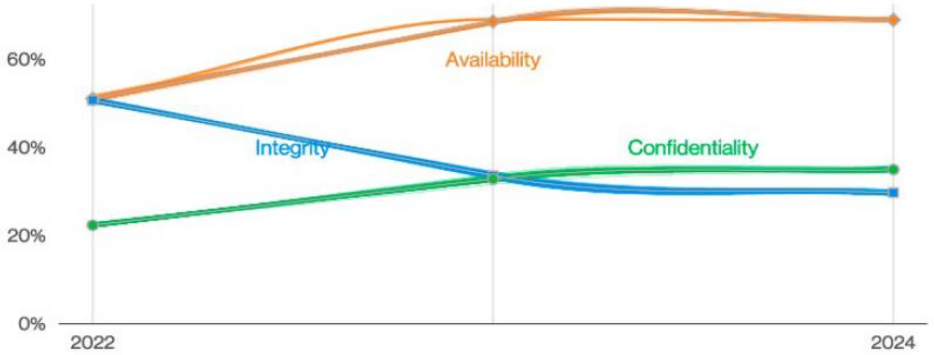
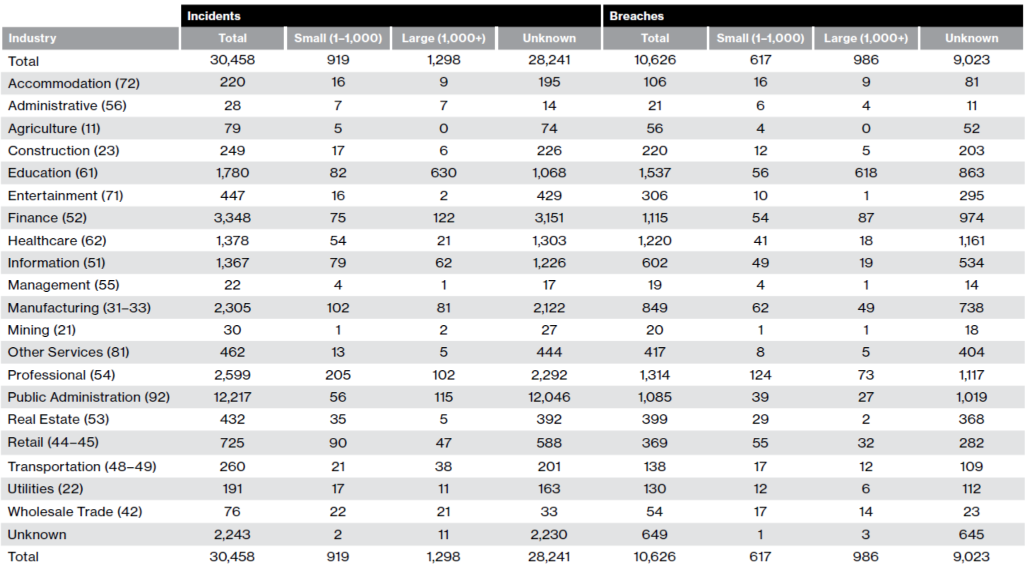


Fig. 2. Attributes over time in incidents
Source: Verizon Business, "2024 Data Breach Investigations Report", 2024.

The graph shows that incidents of availability rise sharply between 2022 and 2024, peaking above 60% by mid-2023 and then declining, while incidents of integrity decrease steadily from close to 40% to around 30%; at the same time, incidents of confidentiality rise from around 20% to 30%, finally overtaking integrity by the middle of 2023. It represents an increase and continued focus on the disruption of service availability, a declining trend of threats to data accuracy, and quite an increase in data privacy risks—reflecting an evolving threat landscape in cybersecurity.



	Incidents				Breaches			
Industry	Total	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	30,458	919	1,298	28,241	10,626	617	986	9,023
Accommodation (72)	220	16	9	195	106	16	9	81
Administrative (56)	28	7	7	14	21	6	4	11
Agriculture (11)	79	5	0	74	56	4	0	52
Construction (23)	249	17	6	226	220	12	5	203
Education (61)	1,780	82	630	1,068	1,537	56	618	863
Entertainment (71)	447	16	2	429	306	10	1	295
Finance (52)	3,348	75	122	3,151	1,115	54	87	974
Healthcare (62)	1,378	54	21	1,303	1,220	41	18	1,161
Information (51)	1,367	79	62	1,226	602	49	19	534
Management (55)	22	4	1	17	19	4	1	14
Manufacturing (31–33)	2,305	102	81	2,122	849	62	49	738
Mining (21)	30	1	2	27	20	1	1	18
Other Services (81)	462	13	5	444	417	8	5	404
Professional (54)	2,599	205	102	2,292	1,314	124	73	1,117
Public Administration (92)	12,217	56	115	12,046	1,085	39	27	1,019
Real Estate (53)	432	35	5	392	399	29	2	368
Retail (44–45)	725	90	47	588	369	55	32	282
Transportation (48–49)	260	21	38	201	138	17	12	109
Utilities (22)	191	17	11	163	130	12	6	112
Wholesale Trade (42)	76	22	21	33	54	17	14	23
Unknown	2,243	2	11	2,230	649	1	3	645
Total	30,458	919	1,298	28,241	10,626	617	986	9,023

Fig. 3. Number of security incidents and breaches by victim industry and organization size
Source: Verizon Business, "2024 Data Breach Investigations Report", 2024.

This table classifies cybersecurity incidents and breaches by differences between industries, total incidents and breaches, and small (1-1,000 employees) and large (1,000+ employees) organizations. The total number of incidents reported is 30,458, with the vast majority falling under unknown size at 28,241, indicating serious under-reporting or a lack of data on the organizational sizes affected. Public Administration (12,217), Finance

(3,348), and Professional Services (2,599) are the first three in line to have major incidents. In terms of breaches, unknown organization sizes account for 10,626 and 9,023 incidents. Here, too, Public Administration with the highest number—1,085—is followed by Finance at 1,115 and Education at 1,537.

Data shows that the Public Administration, Finance, and Education sectors are at higher risk of cyber incidents and breaches, reflecting the great value of sensitive information and essential services within these sectors. More broadly, smaller organizations in all sectors report fewer incidents and breaches. This may reflect lower targeting by cyber threats, or it may also relate to possible under-reporting. Large organizations also reported fewer incidents compared to organizations of unknown size, but they still account for significant numbers of breaches. Notably, in the Education sector, there are 618, and Professional Services account for 124. This shows that while all businesses must take security very seriously, those working at scale need even better cyber protection for the more considerable possible risks.

LockBit was known in the first place as “ABCD” ransomware, and it has evolved into a specific threat over the years. LockBit is another subclass of ransomware; this means that it is a 'crypto virus' for the apparent reason that it has crafted its ransom demands around financial gain from those affected in return for the decryption of the data. It targets mainly enterprises and government organizations rather than individuals [7].

The organizations big and small across the globe were negatively affected by the LockBit RaaS and its affiliates. In 2022 and 2023, LockBit was declared as the most active global ransomware group and RaaS provider, going with the number of victims claimed on their data leak site. A Ransomware as a Service (RaaS) criminal cyber-group operates a particular strain of ransomware and rents that ransomware out to one or more other individuals or groups of actors (commonly referred to as "affiliates"). It helps affiliates distribute their ransomware by charging fees up front, operating subscription services, sharing profits, or some combination of these three remuneration models [8].

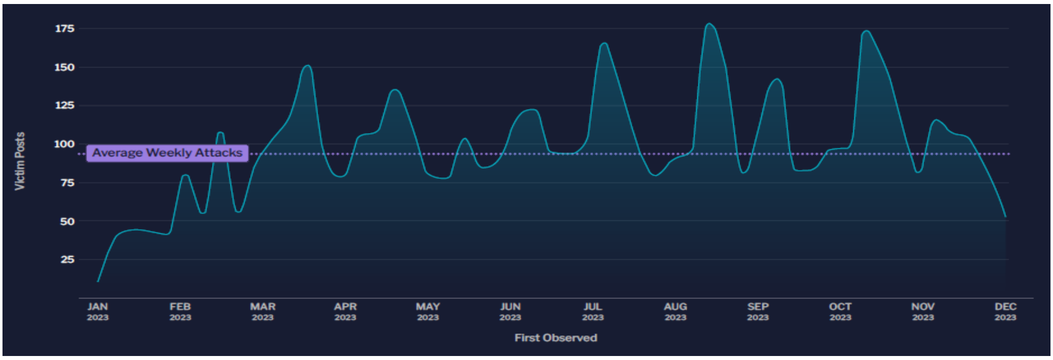


Fig. 4. Public Victim Posts by Week in 2023

Source: Flashpoint, "2024 Global Threat Intelligence Report," 2024.

The ransomware landscape has changed considerably since the apparition of the LockBit group in 2019. After that, since 2022 and continuing in 2023, LockBit remains one of the most prolific ransomware, just with an exception of 3 months when CL0P ransomware targeted a lot of companies with two zero-day campaigns. LockBit is recognized as a more evolved and ruthless version of ransomware and LockBit 3.0 is still active but not sure for how long. The 4.0 variant seemed to be in the making after the operation Cronos when LockBit was taken down in February of 2024. To add to this, it all leaves the victims with yet another aggressive form of negotiation along with a triple-extortion scheme.

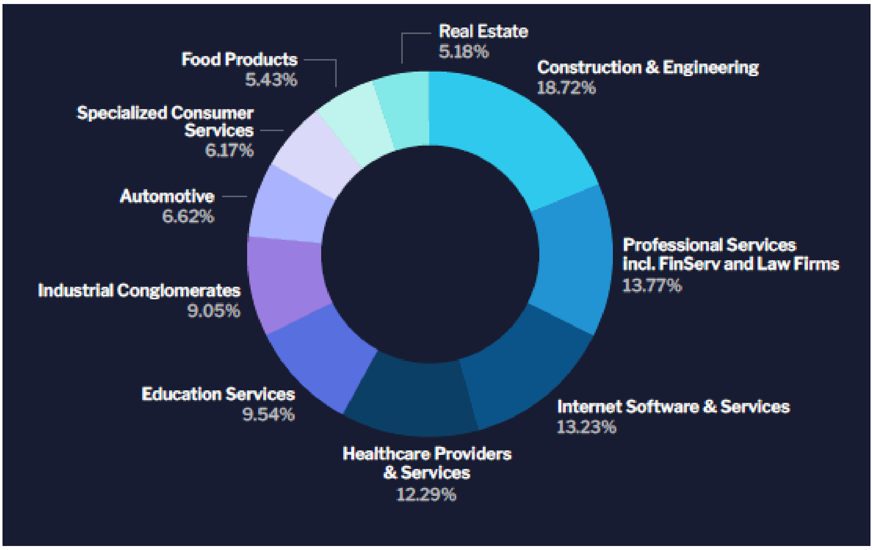


Fig. 5. Top Ten Industries Targeted by Ransomware in 2023
Source: Flashpoint, "2024 Global Threat Intelligence Report," 2024.

The construction and engineering sector was the most targeted in 2023, with 416 publicly reported incidents. Other highly targeted sectors were professional services, internet software and services, and healthcare, reinforcing the cross-industry impacts ransomware can have and the vital need for industry-tailored defense strategies. The most targeted with 57 public attacks is the construction and engineering sector, only in the first two months of 2024. Following behind are the manufacturing and healthcare sectors, with 49 public attacks in the first two months of 2024.

4. Case study about data leaks

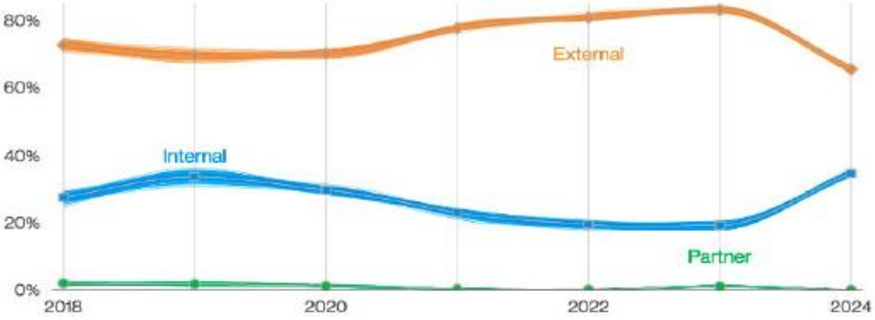


Fig. 6 Threat actors in breaches over time
Source: Verizon Business, "2024 Data Breach Investigations Report", 2024.

In 2022, one of the former employees of the United States National Security Agency was arrested for interfering in the sale of classified information to a spy operating for Russia, who was an operative for the Federal Bureau of Investigations. Jareh Sebastian Dalke, presently 32 years old, had worked at NSA for just under a month from June 6 to July 1, 2022, contracted in Washington D.C. while on a temporary assignment to NSA from his employer. During his employment with the NSA, he emailed three classified documents to a non-government entity on his encrypted email account: one at a secret classification level and two additional documents at the top-secret classification level. He also scheduled the transmission of an extra quantity of National Defense Information subject to his control to be transferred to the undercover FBI agent and scheduled payment for such transmission via cryptocurrency. The proposed payment was for compensation in exchange for transmitting the information. The files also contained a letter from Dalke in which he stated, "Dear friends! I am thrilled to have this opportunity finally to present this information to you. I welcome our friendship and mutual benefit. If there are desired documents that you would like for me to locate, please let me know, and I shall try when returning to the main office." He further indicated that he had attempted to establish contact using a submission to the SVR TOR site. Dalke's arrest followed within days of the Russian government conferring Russian citizenship on former U.S. intelligence contractor Edward Snowden, who is wanted on charges of espionage after leaking tens of thousands of documents listing a plethora of surveillance programs operated by members of the UKUSA community. He also said that his revelations would have meaning for Russia and urged them to keep him in touch, promising to provide more documents later. This man was convicted and sentenced to nearly 22 years in prison for attempting to transfer classified documents to Russia [9].

Jareh Sebastian Dalke's act, therefore, was a significant violation of ethics and general legal and constitutional provisions regarding national security. Jareh's act of trying to dispose of classified data to a foreign body of interest seriously removed the integrity and safety of the United States as a whole; innumerable lives and a slew of strategies of national defense would be set on the line. There is a reason for the classification of documents: they contain sensitive information important to national security, defense, and intelligence activities. Enemies might use the release of such information without due authority for several disastrous consequences – espionage, sabotage, and even terrorism. This is a relevant example that data leaks are no just from external, but also internal, and this example is relevant because when we analyze all the types of data leaks, human error intentional or unintentional is present every day.

Further, when classified information is divulged in the purview of gaining monetary benefit and that, too, in terms of a cryptocurrency, Dalke inflicts a blow on the name and value of the institutions responsible for national security. This erodes the confidence that the public and other nations might have in the United States to guard secrets and maintain global stability. In betraying his country, Dalke did not just place the current operations at risk, but he set an example that would give other people plans on how to exploit their access to sensitive information for personal gain.

The relevance of cases such as Jareh Sebastian Dalke and Edward Snowden contributes significantly, underlining, in one way or another, the risk level that insider threats pose to national security through unauthorized disclosure and data leakage of classified information. Furthermore, while Dalke's failure to sell susceptible data to foreign power put on the table some of the weaknesses in security protocols, Snowden's massive leaks exposed large government surveillance programs, leading to ongoing debates on government surveillance and changes that privacy and intelligence practices and policies will face in the process. They both emphasized the necessity of security measures, legal frameworks, and oversight mechanisms strong enough to guard sensitive information, prevent leaks, maintain trust, and maneuver in international relations and espionage.

5. Conclusions

In the contemporary digital world represents a challenge to face cybercrime, data leaks, and the ransomware ecosystem. Cyberattacks such as ransomware have evolved and at present have turned into a very organized and money-making enterprise. Cybercriminal groups have developed the Ransomware as a Service (RaaS) business model, affiliate networks, and very sophisticated methods to demand ransom from their victims and earn a lot of money. Such attacks against businesses, critical infrastructures, and public entities are seriously increasing around the globe, emphasizing the multi-domain impact of incidents on the global security paradigm.

Having personal data published on Telegram and the Dark Web exposes people to a large of potential threats: from targeted phishing, social engineering, and extortion schemes. Cybercriminals manage to impersonate their victims, take over their accounts, and commit fraud or even blackmail. Moreover, after exposure to these platforms, personal data can quickly multiply and be next to impossible to control or eliminate, raising risks of identity and reputational compromise. The combination of factors under which exponential data growth in digital format, the sophistication of cyber threats, and expanding attack surfaces driven by cloud services, IoT devices, and mobile technology in return actually facilitate data leaking.

Cybercriminals wish to acquire and disclose data for many reasons, whether financial, ideological, or personal vendettas. In the digital age, data is among the most valuable things around, and cybercriminals take advantage of systems and network vulnerabilities to steal sensitive information like intellectual property and other private information—personal and financial data and trade secrets. They might want to commercialize such data by resorting to identity theft, extortion, or even selling the data on underground markets. Further reasons may lie in political motivations, notoriety, or personal beliefs against organizations or individuals. Data are published as a control mechanism for causing damage or for manipulating public opinion; this, indeed, is the multi-motivation behind cyber activities.

The future of LockBit ransomware, especially after Operation Cronos, will be nothing short of uncertain, and indeed, the 4.0 variant that now gets admission to the cyberspace of this underworld will most probably indicate new trends of evolution and adaptation in the ransomware space. It is thus that Operation Cronos managed to prevent the ransomware—at least for now—as police forces from around the world and cyber-researchers worked unceasingly to access the infrastructure belonging to the LockBit syndicate. However, above all, cybercriminals are best known for their stubborn resilience and adaptability. The creation of yet another LockBit 4.0 variant shall only be one more indication in the process of continuous evolution of the ransomware technical capabilities, with new features, encryption methods, and evasion techniques likely to be added that will effectively facilitate targeting new victims.

References

[1] ENISA, "ENISA Threat Landscape Report 2023," European Union Agency for Cybersecurity, 2023.

[2] T. Holt and A. Bossler, "Cybercrime and Digital Forensics," *Routledge,* 2022.

[3] V. P. Janeja, Data Analytics for Cybersecurity, 2022, pp. 8-29.

[4] Kela Cyber, "Telegram: The Cybercriminal's Toolkit," 2023.

[5] V. Lyskoit, "Darknet Markets: The Complete Guide," NordVPN , 2024. [Online]. Available: https://nordvpn.com/blog/darknet-market/. [Accessed 7 May 2024].

[6] Unit42, "Stages of a Ransomware Attack," 2022.

[7] Cybersecurity and Infrastructure Security Agency (CISA), "Cybersecurity Advisory: AA23-165A," CISA, 2023.

[8] Kaspersky, "LockBit Ransomware," [Online]. Available: https://www.kaspersky.com/resource-center/threats/lockbit-ransomware. [Accessed 10 May 2024].

[9] U.S. Department of Justice, "Former NSA Employee Sentenced to Over 21 Years in Prison for Attempted Espionage," 1 February 2024. [Online]. Available: https://www.justice.gov/opa/pr/former-nsa-employee-sentenced-over-21-years-prison-attempted-espionage. [Accessed 10 May 2024].