DATA MANAGEMENT ON CURRENT DARK WEB ACTIVITY AND CYBERCRIME PREVENTION

Cosmin Sandu Bădele[1]
Dr. Lucian Ivan[2]
Irena (Arădăvoaicei) Apolzan[3]

Abstract:
Cyber attackers are constantly updating their tactics, techniques and procedures used to launch increasingly complex attacks that can cause image, financial or even strategic damage to victims. Communication and interaction between members of the international hacking community allows them to stay abreast of the latest developments in the field and implement their cyber attack plans. Cybercrime forums are the ideal environment for cyber actors, as they can interact anonymously, offer malware applications, tools, discovered vulnerabilities for sale, or recruit other members to organize and run large cyber campaigns.

The marketing of malware applications at the level of cybercrime forums is an advantage for the cyber actors who are part of that community, as it allows them to purchase ready-made applications, saving them the effort of developing others from scratch. At the same time, the constant marketing of some malware applications to cyber actors with advanced capabilities and knowledge also leads to the development of new variants of the same application, more efficient and adapted to the latest security updates.

Keywords: *Cyberspace, Artificial Intelligence (AI), Big Data, Machine Learning – ML.*

JEL classification: *M1, M15, O11*

1. INTRODUCTION

The development of techniques and the use of artificial intelligence opens up a whole universe that offers new opportunities. The technological evolution leads to the emergence of digital products and services that become more and more popular and end up forming an integral part of our everyday life. Every new technological development leads to our dependence, which means that cyber security becomes more and more important. **The more personal data we post online and the more connected we are, the more at risk we are of being victims of various forms of cyber crime or cyber attack**.

With every new device connected online or to other devices, the so-called "attack surface" in cyber security grows. The development of the Internet, cloud technologies, big data systems and the digitization of industry is accompanied by an increase in the exposure of vulnerabilities, allowing malicious actors to target more and more victims. Given the variety of attack types and their increasing sophistication, keeping up with new developments is a real challenge.

2. CYBER SECURITY

The present means that in today's time, many organizations are digital and data-driven. Which makes cyber security very important, but also very difficult.

Organizations face increasingly complex challenges when it comes to cybersecurity

Everything is digital, everything is hyper-connected and cyber is being introduced into all layers of the organization. Thus, the ingredients for cyber attacks are everywhere.

Compliance needs

Strong compliance requirements are no longer limited to healthcare and finance. Every company needs security adapted to strict regulations.

Digital ecosystems

Access to data is becoming increasingly complex and spread across different parts of your organization. Data sharing activities drive the need for robust data security and protection solutions.

[1] Expert within the Ministry of Internal Affairs, Phd Student at the "VALAHIA" University from Târgoviște, e-mail: cosmin.badele.cb@gmail.com.
[2] Expert within the Ministry of Internal Affairs, associate professor at the Bucharest Academy of Economic Studies.
[3] Expert within the Ministry of Internal Affairs, Phd Student at the Bucharest Academy of Economic Studies.

Increasing risk of attack

Organized crime networks are well-financed and increasingly professional. Your security measures must be up to par against the proliferation of cyber attacks.

Cyber security requires a large-scale approach

Being cyber resilient is not just a matter of buying or implementing a solution. Threats are constantly evolving, and so is your cybersecurity strategy.

✓ By introducing a continuous process of security improvement and adaptation, it is possible to constantly assess the situation and act accordingly to protect your business and maintain control.

✓ We manage security solutions from implementation to 24x7 management and monitoring to ensure your security infrastructure stays up to date without increasing your workload.

✓ Cybersecurity ensures focus on what matters most to a business, comprehensive preventative measures, 360° monitoring, detection and response, and rapid recovery should your business be compromised.

3. TEN WAYS YOUR DATA SECURITY IS AT RISK ON THE DARK WEB

Cybercrime is "the biggest threat to every business in the world." Data security is a top priority for organizations to avoid business interruption, reputation damage, and data and financial losses. In fact, the average total cost of a data breach was recently estimated at 3.92 million $.

Ways information can be leaked and how data security solutions can help reduce the risk of an attack.

1. Providing instructions for fraud

Dark web forums contain how-to discussions between people who intend to open fraudulent accounts. Users can also purchase detailed step-by-step guides on dark web marketplaces. These guides are often associated with specific companies or organizations and are updated to avoid any new security strategies they implement.

2. Release of a VIP's personal data

The dark web and open web contain sites where users maliciously exchange or post information (identifying, financial and/or technical) about an individual. Known as "doxing", this process is often motivated by politics, vigilantism or vandalism. Some doxing attacks inaccurately link illegal activities on the dark web to a company or its employees, putting your company's reputation at risk.

The dark web contains anonymous forums and marketplaces where doxing is planned or personal information is sold. Personal data is also published on open websites such as Pastebin (dark web link dumps and other leaked data).

3. Sale of bank account numbers and payment cards

Dark web marketplaces contain thousands of listings for complete bundles of personal information, giving users unauthorized access to bank and other account information. Users can also purchase fraudulent bank cards, from debit cards to platinum or business cards.

4. Submission of fraudulent tax documents

Fraudulent tax documents such as W2s and T4s are often bought and sold on the dark web. This is especially common in the run-up to tax season, when cybercriminals try to submit fraudulent returns before the actual taxpayer. If your company has suffered a data breach, your employees' tax records may have been compromised for this purpose.

5. Compromising national security

If your organization's role is to provide security at the national level (as a defense contractor or airport security strategist, for example), a security breach could have global

consequences. Listings for leaked national security data such as defense strategies, weapons plans or construction plans are present on dark web markets.

6. Leaking source code

If your organization's source code is leaked, hackers can easily determine if there are vulnerabilities present in your operating systems or security software. The source code can also be stolen and used by another organization. Unless you're a big name making headlines, leaked source code can be hard to detect when it's posted on the dark web or unindexed websites like Github and Pastebin.

7. Creating "spoofing" templates.

Cybercriminals on the dark web create and sell "spoofing" templates as part of an identity theft or fraud scheme. Templates allow fraudsters to create fake websites or forms in the name of a financial institution or other organization. This is sent to a real customer who enters their personal information, which the scammer can then exploit by opening accounts or applying for loans.

8. Disclosure of databases

An organization's database contains sensitive information about employee accounts and locations, as well as a company's overall footprint, including partnerships and private contracts. Cybercriminals can use this information to conduct phishing attacks against employees or leak information about private companies on the web.

9. Selling access to private events

It is not unheard of for dark web vendors to sell counterfeit passes or credentials to gain access to private or high-profile events. If your data security has been breached, dark web criminals can determine how and when to pose as compelling journalists or event attendees.

10. Conducting inexperienced searches on the dark web

In an effort to uncover attacks against your organization's data security, an employee or third-party security vendor may attempt to surf the dark web. This could lead to more harm than good if the navigator is inexperienced. For example, repeatedly searching for a specific company or person name in a dark web search engine could expose your efforts and increase security risks.

A dark web search tool is essential for any organization that wants to protect its reputation, employees and assets from information security threats. Because the dark web is difficult and dangerous to navigate, and because many open websites are not indexed by search engines, data security technologies are necessary to protect data that could be compromised in a cyber attack.

Flashpoint allows users to safely browse the dark web without using a Tor browser. Users can narrow their searches with keywords and filters relevant to their organization and its potential threats. A dark search tool helps users:

✓ Discover leaked data and personal information on dark web or unindexed open websites like Pastebin.

✓ Avoid the time, learning curve and risks associated with manual or inexperienced dark web browsing.

✓ Easily get market listings for any of the above transactions related to your organization.

✓ Proactively discover anonymous discussion forums where data security attacks are planned.

✓ Maintain their organization's reputation by finding and addressing data security risks before they get out of hand or reach the media.

4. DEEP WEB AND DARK WEB: KNOWING THE HIDDEN WORLD TO LEARN HOW TO DEFEND YOURSELF AGAINST CYBER THREATS

Not only drug trafficking and illegal services: the Dark Web is now a fundamental tool for the world of cybercrime. Here's how hackers exploit it and why cybersecurity experts consider it a field to guard.

What we are used to calling "the web" is actually only 0.03% of the Internet. The rest of the network is "hidden". The Deep Web is the part of the Internet that is not indexed. These are pages, for example, whose access is subject to the use of specific protocols or credentials (username and password) that limit access. We are talking, in most cases, of absolutely legitimate web pages, such as those dedicated by companies to internal services and resources, which in any case remain hidden from search engines.

A small subset of the Deep Web, on the other hand, hosts illegal content: we normally speak of the Dark Web. In this case, the fact that the pages are not accessible through normal navigation tools is a real strategy to "hide" the illegal content that is hosted within them. "The case study is broad", explains Luca Bonora, Cyberoo's Head of Business Developer Management. "On the Dark Web you can find a little bit of everything: from drug and arms dealers to sellers of hacking tools or data stolen through cyber attacks." From this point of view, in short, the Dark Web is a kind of "bazaar" for computer hackers who, in recent years, have professionalized themselves through an extremely complex structure.

The level of evolution of cybercrime is evident in the new affiliation formulas chosen by cyberhackers, who have now adopted the "as a service" formula borrowed from the commercial world.

In practice, it is a hierarchically organized system in which leaders provide tools and resources to their affiliates to enable them to conduct cyber attacks more effectively than they could independently. The distribution of profits then takes place according to a commission logic expressed in percentage terms, which usually provides for the payment of 30% of the proceeds to the group leaders. "The system is particularly popular when it comes to ransomware attacks," continues Bonora. "Most criminal hacking groups specializing in this extortion technique now use affiliation as a normal modus operandi."

The phenomenon is also amplified by the transversality of ransomware, which now represents a threat that affects all companies, regardless of their size or the sector in which they operate.

The role of the dark web in ransomware campaigns

The use of the Dark Web as the nerve center of cybercriminal activity essentially focuses on the pooling of tools and information that enable hackers to carry out their attacks.

From sharing malware to sharing information about software and application vulnerabilities that can be exploited to breach corporate networks, the markets lurking in the undergrowth of the Internet are a veritable gold mine for criminal hackers. "One of the most worrying phenomena detected on the Dark Web is the buying and selling of personal information," Bonora points out. "Traffic in credentials stolen from corporate users is a valuable tool for cybercriminals looking to target a specific company with a ransomware attack."

A tried and tested scheme that also has even more "revealed" declinations such as that of initial access brokers, topics that animate a market where direct access to previously compromised corporate networks is available and sold to the highest bidder. The "services" associated with affiliate-based ransomware campaigns go much further, however: in most cases, in fact, cybercriminals also provide the platform that allows them to negotiate ransoms with companies and manage online "public relations."

When the Dark Web Isn't So "Hidden"

The ransomware phenomenon underlies one of the less obvious uses of the Dark Web, such as the publication of "proxy sites" of cybercriminal groups. In addition to the fact that it

is difficult to access, in fact, the Dark Web has another characteristic: a high level of anonymity in the management of the contents published within it.

Sites with the ".onion" domain, accessible only by using the TOR network, are not actually registered through control authorities like regular websites, but are managed through private keys. A system that allows site managers to hide their identity even when pages are identified.

In other words, pages on the Dark Web can be used to gain visibility without being tracked. But to what end? "One of the new trends in ransomware attacks is to target a double ransom note," explains Roberto Veca, head of Cyberoo Cyber Security. "In addition to using malware to encrypt data on company systems and block their activity, hackers systematically exfiltrate the information they find on compromised machines and exploit the threat of public disclosure as leverage to demand a second payment ".

5. INFORMATION SECURITY MANAGEMENT

Cybersecurity information management is about managing threats and risks, building capacity and awareness, and coordinating and sharing information in a climate of trust.

Information security management involves the creation of structures and policies to ensure the confidentiality, integrity and availability of data. Information management is much more than a technical matter, requiring effective leadership, sound processes and strategies aligned with organizational goals. A subcategory of this concept is cybersecurity governance, which covers all types of cyber threats, including sophisticated and targeted attacks, security breaches, or incidents that are difficult to detect or manage.

Cyber security models differ from one Member State to another. Furthermore, at the national level, responsibility for cyber security is often divided between several entities. These differences could hinder, at national level, and even more so at EU level, the cooperation needed to respond to large-scale cross-border incidents and share threat intelligence.

6. CONCLUSIONS

The EU is working on several fronts to promote cyber resilience, fight cyber crime and strengthen cyber diplomacy and cyber defence.

Critical sectors such as transportation, energy, healthcare and finance are increasingly dependent on digital technologies to manage their core activities. While digitization brings enormous opportunities and offers solutions to many of the challenges facing Europe, not least during the COVID-19 crisis, it also exposes the economy and society to cyber threats.

Cyberattacks and cybercrime are increasing across Europe, both in quantity and sophistication. A trend that is set to grow in the future as 22.3 billion devices worldwide are expected to be connected to the Internet of Things by 2024.

A stronger cybersecurity response to create an open and secure cyberspace can contribute to greater citizen trust in digital tools and services.

Cyber attacks have experienced an explosive diversification lately, some of which can be classified as global epidemics due to the high speed of their spread in the virtual environment.

Threats specific to information systems are characterized by an accentuated dynamic and a global character, which makes them difficult to identify and counter. Although there are numerous protection methods, increasingly efficient, ensuring the security of information in the cyber environment cannot be achieved exclusively through technical measures, being mainly a human problem.

Many times, security incidents are generated by an inadequate organization of security policies and less due to a deficiency of security mechanisms. In this context, it is necessary to develop cyber security strategies, by defining policies in this regard, and campaigns to prevent and combat the phenomenon of computer crime at the national level. Romania is in a continuous process of strengthening cyber security at the national level, both from a legal, institutional and procedural point of view, with efforts being undertaken, in this sense, supported by the authorities with responsibilities in the field.

SELECTIVE BIBLIOGRAPHY:

1. ENISA evaluation, 2017. In the period 2014-2016, approximately 80% of ENISA's operational budget was used for the purchase of studies.

2. ENISA, Exploring the opportunities and limitations of current Threat Intelligence Platforms, December 2017.

3. ISACA (formerly known as the Information Systems Audit and Control Association), Information Security Governance: Guidance for Boards of Directors and Executive Management, second edition, 2006.

4. EY, Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017, p. 16.

5. McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy and H. Lung), Hit or myth? Understanding the true costs and impact of cybersecurity programs, July 2017.

6. Securities and Exchange Commission, Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures, February 21, 2018.

7. European Securities and Markets Authority, Joint Committee report on risks and vulnerabilities in the EU financial system, April 2018.

8. ENISA, Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs, December 2015.

SOURCES CONSULTED ONLINE

1. https://www.cegeka.com/en/ro/cybersecurity?gclid=Cj0KCQiAyMKbBhD1ARIsANs7rEF3K8Xij5zfEvUjkiL3Or3Cpv4mecuNgtck455brsBLlAKhiV8WyNsaAkJiEALw_wcB;

2. https://flashpoint.io/blog/data-security-dark-web/;

3. https://www.cybersecurity360.it/nuove-minacce/ransomware/deep-web-e-dark-web-conoscere-il-mondo-nascosto-per-imparare-a-difendersi-dalle-cyber-minacce/

4. https://www.consilium.europa.eu/it/policies/cybersecurity/