CYBER ATTACKS ON DOCUMENT CENTRIC SYSTEMS

Prof. Serghei Ohrimenco, DSC[1]
Assoc. Prof. Lucia Gujuman, PhD[2]
Ghenadie Belinschi[3]

Abstract: *This article examines document-centric information systems as its main subject. These systems have the capability to integrate with other business platforms, such as ERP, CRM, and BPM. They include text editors, spreadsheets, document management systems, and email clients used by organizations and individuals to store and exchange confidential information. The article attempts to define the category of „document-centric systems," represented by software platforms that focus on document management throughout their entire life cycle. The information content of these systems is often the target of cyberattacks, which occur at multiple levels to access sensitive information—from individuals to small and medium businesses, large commercial organizations, and government agencies.*

Keywords: *Information Systems, Document-Centric Systems, Cyber Threats, Cyber Risks*

JEL: **C63, D74, D81, F52, K24**

1. Introduction

Information systems (IS) consist of a combination of various embedded subsystems that operate both independently and in interaction with the external environment. These embedded subsystems function under conditions of inherent uncertainty, context dependencies, and potential threats from the external environment (both cyber and physical). Security is one of the key concepts for protecting the IS environment and its embedded devices, aiming to establish a reliable and secure communication platform (Winkler, 2018).

It should be noted that numerous approaches and methods have been proposed and implemented worldwide to ensure the security of information systems. These include areas such as social engineering, security standards, supplier control, and access control, among others. This article focuses on the effectiveness of access control, given the emphasis on research related to the functioning of document-centric systems.

2. Definition of a Document-Centric Information System

A document-centric information system is a software platform designed to manage documents throughout all stages of their life cycle. This type of system

[1] osa@ase.md, Academia of Economic Studies of Moldova, Laboratory of Information Security, Chisinau, Moldova
[2] gujuman.lucia@ase.md, Academia of Economic Studies of Moldova, Department Information Technology and Information Management, Chisinau, Moldova
[3] ghenadie.belinschi@dsd.md, Doc Space Development, Ltd, Chisinau, Moldova

provides centralized storage, protection, and controlled access to documents. It supports document creation, editing, and collaboration functions, while also integrating with other business systems to automate workflows and processes.

Managing the full life cycle of documents means that the system encompasses all stages of document handling, from creation and editing to approval and archiving. Collaborative editing functions enable effective interaction, allowing users to work together seamlessly. This functionality ensures control over changes made to documents and maintains their relevance throughout their entire period of use.

These systems can also integrate with other business platforms, such as ERP, CRM, and BPM. This integration enables the automation of numerous workflows and enhances the overall efficiency of the organization by linking document management with other critical processes (Chapple, 2020), (Chapple M. B., 2013), (Moore, 2005).

Additionally, document-centric systems support the Office Open XML (OOXML) standard, ensuring compatibility with various applications and offering advanced data security features.

3.1 Cyberattacks

Cyberattacks on document-centric systems (DCS) are complex, multi-stage actions carried out by attackers to compromise information systems, steal data, or disrupt their operations. DCS includes text editors, spreadsheets, document management systems, and email clients used by organizations and individuals to store and exchange confidential information. These systems are particularly vulnerable to attack due to the widespread use and distribution of office software suites, which are often linked to cloud services.

In the context of document-centric systems, cyberattacks include phishing, exploitation of software vulnerabilities, ransomware attacks, and the injection of malicious macros or scripts into documents. These methods enable attackers to gain access to not only documents and document management systems but also other critical resources, potentially causing serious consequences for an organization (Sonowal, 2023), (Tally, 2023, April).

Tools such as XML format processors, document rendering processors, document editors, spreadsheets, and presentation software can contain significant amounts of code—often tens of millions of lines—that are susceptible to memory management issues and other errors. Since these processors frequently download content from the Internet, they are particularly vulnerable to attacks (Eltayeb, 2024).

Bookmarks in documents, such as malicious macros, hidden scripts, or exploits, can be just as dangerous as viruses spread through email messages.

3.2 Goals of Cyberattacks

The main targets of cyberattacks encompass nearly all aspects of our surroundings, including small and large businesses, government entities, and the

information activities of individuals. The execution of cyberattacks leads to a significant rise in information leaks and losses, affecting personal data, commercial secrets, and state secrets governed by law. The key targets include the following:

- Individuals: The greatest risk to individuals is the leakage of financial information and personal data, such as medical records. Attackers can use stolen data to commit financial fraud or identity theft.
- Small Businesses: For small businesses, data loss can result in the loss of a competitive advantage. Many small businesses have unique processes and know-how, the leakage of which can compromise their market position and potentially lead to the complete collapse of the business.
- Large Organizations: Large businesses are susceptible to industrial espionage and are vulnerable to leaks of financial statements and production data. Attackers may exploit this information to manipulate stock markets or engage in blackmail.
- Government Agencies: Government entities, including electronic document management systems, are strategic targets for cyberattacks aimed at obtaining critical information that can affect national security and the economic stability of the state.

Another important aspect of assessing the impact of cyberattacks is the resulting damage, which can take various significant forms. Key forms of damage include:

- Financial Losses: Cyberattacks can lead to direct financial losses related to data recovery, system downtime, ransom payments, and regulatory fines. Additionally, organizations may suffer indirect losses, such as loss of customers and reputational harm.
- Data Breach: The exposure of sensitive information, such as financial statements, strategic plans, or personal customer data, can result in serious legal consequences, including lawsuits and penalties from regulatory bodies.
- Disruption of Operational Activities: Attacks can disrupt organizational systems, causing production shutdowns, interruptions in service delivery, and other operational issues.
- Reputational Damage: A loss of trust from customers, partners, and investors can have long-term consequences for a business, reducing its competitiveness and market capitalization.

The main targets of cyberattacks include:

1. Long-Term Monitoring of an Organization’s Activities

Description: Attackers install hidden mechanisms within an organization's systems to covertly monitor internal processes, read business communications, and gather strategic information. This enables them to continuously gain insights into internal plans, decisions, and sensitive data, such as financial reports and customer information.

Methods Used: Embedding malicious macros, bookmarks, or scripts into documents, as well as deploying mechanisms that provide persistent remote access to the organization's systems.

Consequences: Long-term surveillance enables attackers to manipulate an organization's strategic decisions, anticipate its actions, and interfere with its operations. This can result in a loss of competitive advantage, loss of customers and partners, and a decline in financial performance.

2. Causing Significant Financial Damage, up to and Including the Liquidation of the Organization.

Description: Attackers aim to destabilize an organization’s financial position through persistent attacks that cause data leaks, financial losses, and operational disruptions.

Methods: Repeated exploitation of vulnerabilities in document-centric systems to steal data, extort, and blackmail. This can include using malicious documents to encrypt data and demand ransom or manipulating financial reports to damage investor and customer confidence.

Consequences: Ongoing attacks can lead to severe financial losses, loss of trust from customers and partners, declines in stock prices, and other economic impacts. Ultimately, this may result in bankruptcy and the closure of the organization.

3.3 Actors

The constantly evolving cyber threat landscape and the growth of Darknet markets allow both individual hackers and organized cyber groups to use similar tools. This includes techniques for misleading analysts and analytical systems during incident investigations and attack attribution. A key characteristic of targeted attacks (APT) is that attackers focus on a specific company or government organization. This distinguishes these threats from mass hacker attacks, where a large number of targets are attacked simultaneously, and the least protected users are the most likely victims.

These APT groups attempt to obscure their activities by faking compilation times, operating outside of typical working hours, embedding different languages or unique cultural markers into their code, and re-registering domains previously used by other attackers. Additionally, they often use universal software that is highly effective for achieving short-term goals or carrying out narrowly focused tasks. These tactics make it difficult to attribute a cyberattack to either an individual attacker or an APT group.

Let us examine the available statistics characterizing the quantitative structure of APT groups. For this purpose, we will use the archived data preserved on the Thailand Computer Emergency Response Team's website (https://apt.thaicert.or.th/cgi-bin/aptstats.cgi) (Tha24).

The data covers the period from July 19, 2020, to January 21, 2022. The database statistics as of July 17, 2020, are presented in the following table.

Table 1. Encyclopedia of Threats

No.	Indicator	Value
1	Total threat groups	312 (including 239 APTs, 40 others, 33 unknown)
2	Total group aliases	794
3	Total operations	1,239
4	Total counter operations	70
5	Unique source countries	27
6	Unique victim countries	160
7	Unique victim sectors	42
8	Unique tools	1,327
9	Total tool aliases	1,966
10	*Unique external links*	*4,868*

Source: Archived data from the Thailand Computer Emergency Response Team (ThaiCERT) website, https://www.thaicert.or.th.

Among the sources of threats, China is the clear leader, with 106 groups identified. Russia follows in second place with 42 groups, and Iran is third with 31 groups. For the first time, groups from the USA (7 groups) and Israel (1 group) are also named and present.

Data on the most affected sectors of the economy are presented in the following table.

Table 2. The Most Affected Sectors of the Economy

No.	Name of the Victim Sector	Quantity
1	Government	136
2	Defense	85
3	Finance	73
4	Energy	59
5	Telecommunications	55
6	Mass Media	52
7	Education	41
8	Healthcare	37
9	Industry	34
10	High Technologies	31

Source: Archived data from the Thailand Computer Emergency Response Team (ThaiCERT) website, https://www.thaicert.or.th

Experts are expressing serious concerns about the growing number of threats in the healthcare sector, a trend that is observed in nearly all developed countries with advanced information technology infrastructure.

4. Conclusion

Are any measures being taken to improve the security of document-centric systems? In fact, actions are being implemented, but they are insufficient to

provide complete protection. Despite existing security standards, access control methods, and other security practices, attackers continue to discover new vulnerabilities in the software used by such systems (Caltagirone, 2013), (Rid, 2015).

While advancements in cybersecurity have been made, including improved authentication methods and the introduction of new encryption algorithms, these measures are still unable to address all potential threats. The number of successful cyberattacks and data breaches continues to rise. Particularly concerning is the ongoing issue of complex, multi-stage attacks, such as the introduction of malicious macros or the exploitation of vulnerabilities in the processing of XML documents.

Therefore, despite the efforts made, full protection of document-centric systems remains unachieved. This underscores the need for the continuous evolution of cybersecurity approaches and the development of more comprehensive solutions capable of effectively countering emerging threats and ensuring a high level of data and document process protection.

Many information security issues fall outside the scope of this article and will be discussed in future works.

References

Caltagirone, S. P. (2013). The diamond model of intrusion analysis. *Threat Connect*, 1-61.

Chapple, M. (2020). *Access control and identity management.* Jones & Bartlett Learning.

Chapple, M. B. (2013). *Access control, authentication, and public key infrastructure.* Jones and Bartlett Publishers, Inc.

Eltayeb, O. E. (2024). The Crucial Significance of Cyber Threat Intelligence in Mitigating Cyber Attacks. *Journal of Ecohumanism, 3(4)*, 2422-2434.

http://thaicert.or.th/statistics/statistics-en.html. (2024, 10 03). Retrieved from Thailand Computer Emergency Response Team (ThaiCERT): https://www.thaicert.or.th/

Moore, W. (2005). *Managing information access to an enterprise information system using J2EE and services oriented architecture.* Books24x7. com.

Rid, T. &. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies, 38:1-2*, 4-37.

Sonowal, G. (2023). *Social Engineering Attack. Rethinking Responsibilities and Solutions. .* Nova Science Publishers, Inc.

Tally, A. C.-E. (2023, April). Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. *Tips, tricks, and training: Supporting anti-phishing awareness among mid-career office workers based on employees' current practices*, (pp. 1-13).

Winkler, T. H. (2018). *The Dark Side of Globalization. And How to Cope with It.* LIT VERLAG GmbH & Co.