ALFA BK UNIVERSITY
FACULTY OF INFORMATION TECHNOLOGIES
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
International Scientific Conference

Alfa BK Univerzitet

UDK:711.45:004.78
343.9:004.738.5
DOI: 10.46793/ALFATECHproc25.090V
Rewiev paper

# Malware attacks on public data of smart cities

Čaba VARŠANDAN[1], Milica VARŠANDAN[2]

**Abstract:** Public data in smart cities is frequently targeted by malware. Protecting such data represents a serious threat, as basic security services, individuals, and the functionality of the system itself are at risk. Malware attacks are a growing threat due to the complex technologies used. Open data is utilized to improve the management of urban systems and increase efficiency. With the help of advanced technologies such as artificial intelligence, encryption, blockchain, and security measures, smart cities can enhance system protection and reduce the risk of attacks. This paper analyzes public data in smart cities, the types of attacks on public data, and how malware attacks affect it.

**Keywords:** malicious software, open/public data, attacks, smart cities

## 1. The role of Open Data in Smart Cities

Public or open data is inevitable in the development of smart cities, enabling transparency, improved services, and better interaction between citizens and authorities. Here are some aspects of their role from [1]:

Increasing transparency and accountability: Open data provides citizens with access to information about city governance, thereby increasing the accountability of local authorities. Citizens can monitor decisions related to public spending, projects, infrastructure, and other aspects of life in the city.

Data on energy consumption, transport, pollution, waste and other elements enable city authorities to better manage resources and use them more efficiently.

Open data provides an opportunity for innovation, enabling private companies, start-ups and researchers to develop new applications, services and products that improve the quality of life of citizens. These include applications for monitoring public transport, energy management or optimizing resource consumption.

Data usage for analysis and decision making could lead to better living conditions. For example, air quality data can help predict pollution and implement preventive measures.

Open data on energy, water resources, and pollution can be used to guide environmental initiatives, reduce carbon footprint, optimize consumption, help to understand the warnings and the nature of the appearance and implement sustainable practices in the daily lives of cities.

Open data can improve the interaction between citizens and authorities, allowing citizens to contribute to decision-making. Citizens can use the data to make proposals, report problems (e.g., accidents, infrastructure failures) and actively participate in policy making.

Connectivity and integration of different systems: Public/open data enables the connection and integration of different city systems (e.g., transport, utilities, health, education) into a single ecosystem, which helps better coordination and efficiency in the functioning of the city.

### 1.1 Example of successful implementation of a smart city

Copenhagen is known for its focus on sustanability and smart city initiatives. It can be read in the paper [2] that the city has implemented smart traffic management systems to reduce congestion and improve air quality. Copenhagen also uses a smart grid to optimize energy consumption and support renewable energy sources.

## 2. Types of malwares targeting smart cities

Malware that targets open data has a specific goal – to steal, damage, or manipulate that data. These attacks can have a wide range of negative effects on individuals, organizations, and society as a whole. Below I will describe a few types of malwares. We will focus only on a few of them, so as not to expand the focus of research on them too much or possibly reduce the emphasis from smart cities.

### 2.1 Data manipulation malwares

In smart cities, data manipulation malware can be a serious security risk. These cities rely on internet connected (IoT) technologies and big data to manage infrastructure and services. It follows that protection against such threats is crucial to ensure the security and efficiency of city systems.

The goal of such malware can be to alter or falsify data in order to create confusion or to sabotage various operations. As an example, we can cite a disruption in the functioning of infrastructure, a change in traffic data [3] to cause a traffic jam or divert the flow of vehicles.

### 2.2 Malwares for information stealing

Malware of this type is designed to gain unauthorized access, collect, and steal sensitive data from centralized databases, such as citizen or infrastructure data.

Depending on the type of malware, we can talk about a trojan that is copied everywhere in the system later to exploit the vulnerabilities of the attacked systems, or they can have the general purpose of copying events from the system, perhaps stealing data from the population that can be useful for attackers, as well as to collect confidential data/information. In some cases, they take control of the infrastructure and demand large ransoms. We can also include rootkits, which can camouflage their existence and thus serve as a point of transmission of all types of data.

### 2.3 Data-deleting malwares

This type of malware deletes data from your computer or network. This can cause serious damage, especially if this will no longer give you the ability to recover your data.

As a goal of such data manipulation, we can emphasize the threat to the functioning of a (critical) system/city services. If it deletes key configurations, any type of system could be in malfunctioned state because of it. They spread in many ways, through emails, web pages, USB drives, SD cards, and so on, as the authors of the paper [7] described.

### 2.4 Malwares spreading disinformation

They have been successfully used to spread misinformation and manipulate public opinion, create false reports or statistics. This type of attack may be becoming more and more popular. The list [6] can serve as a good source of information about the attacks. IoT devices, mentioned in articles [1][4], are very prevalent in smart cities, so they can even control traffic, but they have a multitude of purposes.

Various statistics [8] show that as technologies advance, both attacks and types of attacks are becoming more and more frequent and that it is necessary to use and prepare for the same with existing solutions that include artificial intelligence capabilities.

## 3. Impact of the attacks on smart cities

Attacks has always been, and always will be. The implicit aspects are, at the very least, the functionality or safety of urban systems. Smart cities use various technologies such as the Internet of Things (IoT), automation, sensors, and other digital tools to improve the quality of life of their citizens and optimize city services. However, these systems can be vulnerable to malware attacks.

Impacts occur in various forms, such as disruptions in the functioning of services. Changes to weather conditions may affect airports or public transport. Eventually, if it comes to reading temperature data, they can affect the choice of citizens' wardrobe.

Such unrealistic data can lead to a loss of trust in the public data. I'm sure you've all been disappointed at times because of weather forecasts that are inaccurate for some reason. If the data is unreliable or subject to manipulation, citizens can lose trust in the city's smart solutions.

There are also financial losses. The stock market data is also public. What would happen if we got the wrong information about the stock market in a certain time range? There are too many changes happening from second to second, this can obscure the true state of affairs and misguide brokers in the next steps. Compromised data can lead to direct financial losses through ransomware or indirect costs due to service downtime.

In addition to all of the above, it may happen that some data is open but should not or leak due to some attack. Inadequate data protection can lead to legal consequences for the city administration, various companies that have guaranteed the security of the same.

## 4. Attack methods

The types of attacks are most distinguishable from the types of malwares [9]. There are many types identified separately today, and so the ways in which different systems are infected.

A 2023 survey provides the following taxonomy [10] of attack patterns:

Polymorphic and metamorphic attack, ransomware attack, fileless software attack, advanced persistence threat (APT), zero-day attack. This is just one in a series of categorizations of the same, we will stick to this distribution in the continuation of the work.

### 4.1 Polymorphic and metamorphic attack

A polymorphic attack, as the name implies, occurs in a variety of forms. The strategy of the software itself is to constantly change shape and can take the form of trojans, viruses, worms, bots, or keyloggers. For the same reason, it's hard to catch. In this way, the goal of execution remains the same, which is to avoid detection programs [14].

In a metamorphic attack, the malware is more complex, completely altering its code each time it executes and making replicas of itself.

There are several types of families such as Virlock, Cerberus, Crysis, Kelihos Botnet, Beebone, and the like.

### 4.2 Ransomware attack

It targets individuals and organizations to extort ransom money. The method works by encrypting the victim's data. Making them unavailable unless a ransom is paid. They use a variety of phishing campaigns, brute force attacks to gain access to data, and then deploy ransomware to take control of systems. Payment is usually requested in cryptocurrencies [10], which adds even more complexity in finding attackers. As a result of non-payment, users/companies may lose their data.

The most well-known such attacks are WannaCry, NotPetya, Ryuk, CryptoLocker and others.

### 4.3 Fileless software attack

This attack does not use traditional files that could be detected and analyzed by antivirus programs. It uses existing tools, processes, and resources within the infected system to perform its malicious actions. They often rely on legal tools and already present processes in the system.

The attack consists of 5 steps, the initial access is made using an email, a malicious link, or compromised websites. When a user falls on these contents, performs an experiment with them, a script is downloaded.

After downloading the script, use scripts such as PowerShell, VBScript, or JavaScript to perform its actions.

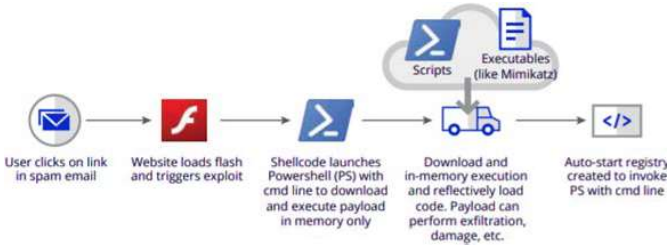


**Figure 1**: Attack without software files [15]

The malware takes advantage of the internal applications of the system, hides deep inside the system, so that it remains active even after a reboot.

Given that internal applications or tools within the operating system are used, they are very well camouflaged and difficult to detect.

### 4.4 Advanced Persistence Threat (APT)

This is a sophisticated form of malware that allows attackers to gain access to systems and remain undetected for an extended period of time.

APT malware is usually made to last a long time, hence the label persistent [10].

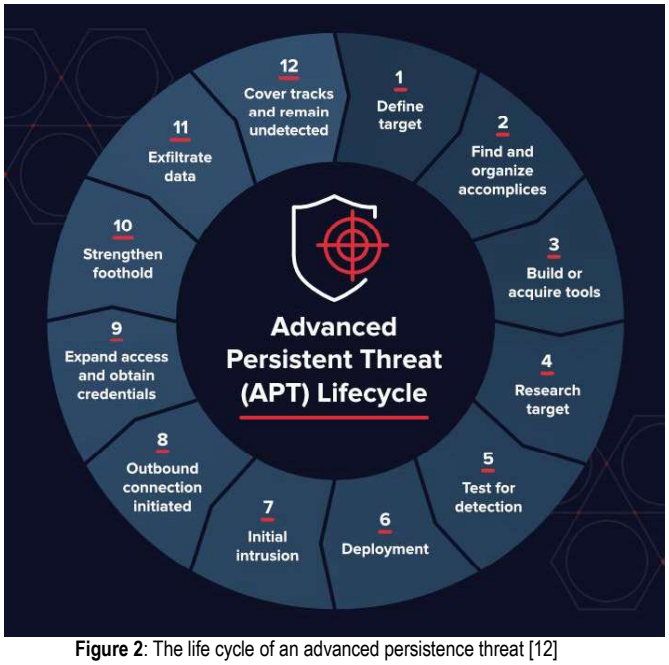


**Figure 2**: The life cycle of an advanced persistence threat [12]

Their potential targets are intellectual property, confidential data, personal information, infrastructure data, access credentials, sensitive or incriminating communications, and to remain in someone's system for as long as possible.

The most well-known attacks of this kind are Stuxnet, Flame, Duqu, and Project Sauron.

### 4.5 0day attack

Zero-day attacks have an element of surprise because they were previously undetected; [16] An attacker embeds a zero-day exploit into their planned list of vulnerabilities that they carefully scoured through lines of code for hours, weeks, or even months to discover these flaws. Once they are found, they integrate the zero-day exploit into their planned vulnerability list. After creating a penetration and planned spectra of the program, they launch their attack, catching their targets off guard.

Cyber attackers use a variety of techniques to carry out zero-day attacks, such as social engineering phishing, spamming and phishing, various messages alluding to unpaid or unsuccessful payments to various services, the technique of embedding exploitation tools in advertisements and malicious websites, and infecting computers, networks, or servers.

## 5. Protection strategy

In the daily pace of growth and the emergence of new technologies, technological advances, there is no universal form of protection of any system.

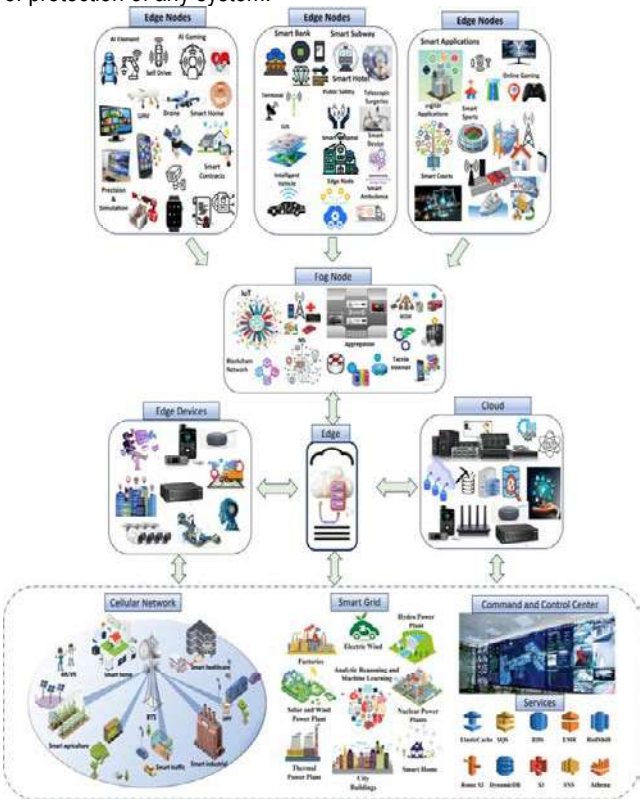


**Figure 3**: Security requirements of computing in smart cities [17]

Malicious groups always find a way to get to protected data, break encryption, but that doesn't mean that at least basic protection should not be established in the system where public data is located.

### 5.1 Tehničke mere

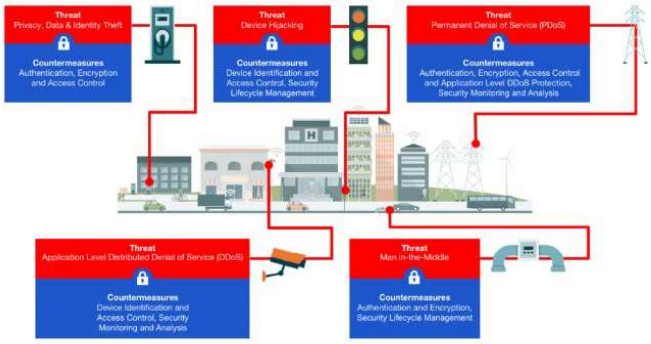


**Figure 4**: Smart cities and countermeasures [17]

#### 5.1.1 Encryption of the data

The privacy and security of data is ensured by encrypting it when it is sent over the network. Encryption is the process of converting data into an unreadable format that can only be restored to its original form using a specific key. Without this kind of encryption, any third party could easily get access to sensitive information. The goal of this technique is to ensure that only those who need access to the content have access. We could extend this topic to different types of encryptions, to encryption algorithms, to the use of data encryption, and so on. These topics are present everywhere in everyday communication.

#### 5.1.2 Network segmentation

By using the exact same network, we can make it easier to attack the internal network. By segmenting the network, we isolate parts of the system and thus increase security. Open data systems should be kept separate from critical parts of the system. This approach reduces the risk of the attack spreading to the entire system, as attackers who compromise one network segmentation will not automatically have access to other segments.

#### 5.1.3 Regular software updates

We are talking about updates that address known vulnerabilities. If there is a known problem/vulnerability in a system, each new update can resolve the vulnerabilities. Delaying it can expose devices to attacks that use the previously mentioned vulnerabilities.

#### 5.1.4 Malware detection tools

Use advanced tools to identify and remove the malwares. In order to successfully examine or catch a threat, it is necessary to use behavioral analysis techniques, heuristic scanning, and so on. Often, the tools are also integrated into other systems, such as attack protection or network monitoring, to ensure a quick response to potential threats.

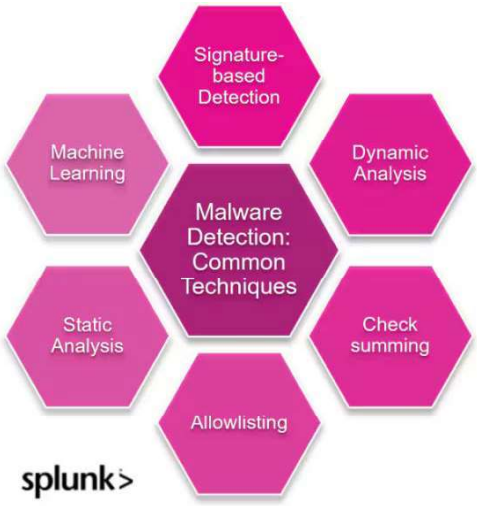


**Figure 5**: Smart cities and countermeasures [18]

There are many solutions, including VirusTotal, Malwarebytes, Windows Defender (Microsoft Defender), antivirus products such as Kaspersky, Sophos Intercept, Eset Nod32, RougeKiller and many others. They are all powerful tools, and it's hard to choose which one would be the most useful. There are also comparisons on the internet of these tools. That might make it a little easier for us to choose. There is no need to underestimate the importance of products that are based on AI or blockchain technology. More and more of them can be found on the market, and with the help of various agents, various automations of the same can be defined.

### 5.2 Forensic analysis

It's a form of computer analysis. It consists of a process of investigation, identifying the mode of attack, the impact of it, and analyzing the evidence. It should be carried out when a security incident has occurred or when there is a suspicion that data has been compromised.

**Access Tracking**: Collect all requests for access to data to detect suspicious activity and identify threats. Access controls are also checked here, and if there are forensic leads. Some of the well-known tools for the same are Splunk or Ossec.

**Attack Reconstruction**: Digital forensics can help identify the source of an attack and the data affected. It needs to be fully clarified how and where the attack began, how it developed, and of course what consequences it caused. Tools for the same are EnCase, FTk, Wireshark, and others. It leaves the reader's curiosity at all times to explore or become interested with any of the tools not mentioned in the work.

**Expert/General Understanding Training**: Developing the capacity to respond quickly to attacks. There is no single way to do it, but the internet has become a good place to find material. Various organizations and individuals offer retraining/upskilling in the cybersecurity field in general. Increasingly, companies or organizations are hiring in-house people to cover security.

### 5.3 Legal and procedural approaches

**Data Management Policies**: Clearly defined policies on the collection, processing, and sharing of data. There are different types of regulations such as GDPR, CCNA, and all of them are very defined and control a specific territory. Nowadays,

there is a lot of emphasis on them and it is necessary to take into account the rules set out in the regulations. More on this in the paper under [20].

**Public Education**: Informing citizens and organizations about the importance of cyber security. Depending on the form of the company and the way of working, internal trainings can also be organized. In this way, people can be prepared for some cybersecurity challenges.

## 6. Case studies

**Attack on San Francisco's public transportation system (2016):** Hackers attacked the San Francisco City Transportation Agency. The ransomware attack has disabled access to timetable data. During the attack, more than 2,000 computers were locked and 100 bitcoins were demanded for ransom. It was worth about $73,086. The transport company did not make a statement as to whether it ultimately paid the ransom or simply allowed their data to be lost [19].

To minimize the impact of the attack, the company has given everyone a free ride.

**A surveillance camera system was infected in China (2021):** They found a database that was exposed to the entire internet, and no password or any additional authentication was required to access it. The same database contains gigabytes of facial recognition data from hundreds of people and the rest of the important information from a couple of months of camera research. It has triggered a negative wave of opinion in general about the use of facial recognition systems.

**Tampa Bay Irrigation System Attack (2021):** Hackers tried to play around with the levels of chemicals in the water. In this case, the attack was quickly detected and they were able to prevent great trouble caused by the presence of various chemicals in drinking and technical water.

Many other examples can be found in the article [21] and in articles on the Internet in general. Probably all possible cases have not yet been identified.

## 7. Conclusion

Malware attacks on smart city open data are a serious threat that requires an integrated approach to protection. Newly-developed solutions using an artificial intelligence model, or a blockchain solution with a high level of security, should not be underestimated. In addition to technological solutions, it is crucial to improve legal frameworks, citizen education and cooperation between the private and public sectors in order to effectively respond to these challenges.

Even the slightest flaw can create an opportunity for attackers to get their hands on important data, or worse, to manipulate a population of people.

## 8. Reference:

[1] Pier Luigi Mazzeo, Paolo Spagnolo (2024) Smart Cities - Foundations and Perspectives. Open access peer-reviewed Edited Volume.
doi: 10.5772/intechopen.114510

[2] Laura Puttkamer (2023) City Portrait: Smart City Copenhagen
https://www.beesmart.city/en/smart-city-blog/copenhagen

[3] Jehad Ali, Sushil Kumar Singh, Weiwei Jiang, Abdulmajeed M. Alenezi, Muhammad Islam, Yousef Ibrahim Daradkeh, Asif Mehmood (2025) A deep dive into cybersecurity solutions for AI-driven IoT-enabled smart cities in advanced communication networks. *Computer Communications, Volume 229*, 1 January 2025.
doi: https://doi.org/10.1016/j.comcom.2024.108000

[4] State of Green partnership authors (2023) 10 examples of smart city solutions.
https://stateofgreen.com/en/news/10-examples-of-smart-city-solutions/

[5] Rambus company members (2023) Smart Cities: Threat and Countermeasures.
https://www.rambus.com/iot/smart-cities/

[6] Microsoft knowledge base (2025) What is malware?
https://www.microsoft.com/en-us/security/business/security-101/what-is-malware

[7] Josh Fruhlinger, John Leyden (2024) 15 infamous malware attacks: The first and the worst
https://www.csoonline.com/article/572911/11-infamous-malware-attacks-the-first-and-the-worst.html

[8] AI Edge Labs (2022) Cybersecurity Best Practices in Smart Cities
https://edgelabs.ai/blog/cybersecurity-in-smart-cities-risks-and-protection-best-practices/

[9] Kurt Baker, Crowdstrike (2023) The 12 most common types of malwares
https://www.crowdstrike.com/en-us/cybersecurity-101/malware/types-of-malware/

[10] Jannatul Ferdous, Rafiqul Islam, Maumita Bhattacharya, Md Zahidul Islam (2023) Malware Resistant Data Protection in Hyper-connected Networks: A survey.
doi: 10.48550/arXiv.2307.13164

[11] Microsoft knowledge base (2025) What is cybersecurity?
https://www.microsoft.com/en/security/business/security-101/what-is-cybersecurity

[12] Michael Buckbee (2023) What is an Advanced Persistent Threat (APT)?
https://www.varonis.com/blog/advanced-persistent-threat

[13] Wiem Tounsi, Helmi Rais (2018) A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security, Volume 72*, Pages 212-233
doi: 10.1016/J.COSE.2017.09.001

[14] James B. Fraley and Marco Figueroa, "Polymorphic malware detection using topological feature extraction with data mining," Conf. Proc. - IEEE SOUTHEASTCON, vol. 2016.
doi: 10.1109/SECON.2016.7506685

[15] Trellix company members, What Is Fileless Malware?
https://www.trellix.com/security-awareness/ransomware/what-is-fileless-malware/

[16] Umesh Kumar Singh, Chanchala Joshi, Dimitris Kanellopoulos (2019) A framework for zero-day vulnerabilities detection and

prioritization. *Journal of Information Security and Applications Volume 46*, Pages 164-172
doi: https://doi.org/10.1016/j.jisa.2019.03.011

[17] Abeer Iftikhar, Kashif Naseer Qureshi, Muhammad Shiraz, Saleh Albahli (2023) Security, trust and privacy risks, responses, and solutions for high-speed smart cities networks: A systematic literature review. *Journal of King Saud University - Computer and Information Sciences, Volume 35, Issue 9*
doi: https://doi.org/10.1016/j.jksuci.2023.101788

[18] Blessing Onyegbula, Muhammad Raza (2024) What is Malware Detection?
https://www.splunk.com/en_us/blog/learn/malware-detection.html

[19] Samuel Gibbs (2016) Ransomware attack on San Francisco public transit gives everyone a free ride
https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware

[20] Daniela Popescul, Laura-Diana Radu (2016) Data Security in Smart Cities: Challenges and Solutions. *Informatica Economică vol. 20, no. 1/2016*
doi: http://dx.doi.org/10.12948/issn14531305/20.1.2016.03

[21] Victor Poitevin (2024) Overview of cyberattacks on connected cities
https://www.stormshield.com/news/overview-of-cyberattacks-on-connected-cities/

**Contact information:**

**Čaba VARŠANDAN1**, Senior Quality Assurance Engineer
(Corresponding author)
HTEC Group,
Bulevar Milutina Milankovića 7Đ, 11070 Belgrade, Serbia
varsandancaba@gmail.com
https://orcid.org/0009-0009-4321-9276

**Milica VARŠANDAN 2** MSc, Teaching Assistant
Dr Lazar Vrkatic Faculty of Law and Business Studies,
Bulevar oslobođenja 76, 21102 Novi Sad, Serbia
milicamarjanovic89@gmail.com
https://orcid.org/0009-0002-6500-2464