Advances in Web Development Journal

vol. 1 no. 1, pp. 1–12

doi: X

Submitted: 2023-10-11 | Revised: 2023-10-11 | Accepted: 2023-10-11

Keywords: identity theft, phishing, cybercrime, cybersecurity

Przemysław *SZMYD* [1], Dominik *MATEJKOWSKI* [2]

ONLINE IDENTITY THEFT DETECTION AND PREVENTION METHODS

Abstract

Today, a significant amount of work is performed on computers. Because of the prevalence of technology, a lot of data can be obtained by gaining unauthorized access to important network machines, such as servers. Cyberciminals may also target individual Internet users, trying to acquire their personal information by the use of various methods. The gathered information can be used for identity theft, causing direct harm to the victim or an organization, with which they are associated. In this article we explain the nature of identity theft, examine different approaches used by cybercriminals and review a range of strategies for detecting and preventing this phenomenon. Additionally, we provide examples of two attacks: a phishing attack and an intrusion targeting an unsecured server within an organization's network. We conclude that the risk of data theft is often downplayed. An effective way of mitigating this threat is increasing the employees' knowledge about cyber security and using appropriate software and hardware measures.

1.INTRODUCTION

The progressive computerization of society and the ever-increasing reliance on technology is causing an exponential increase in the number of online crimes of various types. Nowadays, in addition to various types of malware, there is an increasing number of fraud and social engineering attacks targeting web users. Cybercriminals are also just as eager to use data from various types of data leaks or disclosures. This article will focus on identity theft methods, their detection and prevention. The aim of this paper is to show the dangers of data through which a person's identity can be stolen and how to detect and prevent them. The article will also present attacks related to the theft of sensitive data and methods to defend against them.

[1] University of Information Technology and Management, Poland

[2] Rzeszow University of Technology, Department of Complex Systems, Poland

2.NATURE OF STOLEN DATA

At the outset, it is worth mentioning in what form the data stolen by cybercriminals can be. In addition to typical data in the form of login, password or phone number, there is also theft of sensitive data. This is a distinct category of personal data that must be especially protected, as the context in which it is processed can cause serious risks to fundamental rights and freedoms. During identity theft, this type of data will allow an almost "perfect" impersonation of a person [1][2]. According to The General Data Protection Regulation (GDPR), sensitive data are the special categories of personal data listed in Słupczewski B. article [9]:

- Data revealing racial or ethnic origin,
- Data revealing political views,
- Data revealing religious or philosophical beliefs,
- Data revealing trade union membership,
- Genetic data,
- Biometric data (used to uniquely identify an individual),
- Health data,
- Data concerning sexuality or sexual orientation.

Sensitive personal data should not be confused with personal information, which includes, among other things, name, home address, telephone number, or PESEL (Polish: Powszechny Elektroniczny System Ewidencji Ludności; Universal Electronic System for Registration of the Population).

3. DATA THREATS

We often hear about the theft of sensitive data (e.g., for the purpose of identity theft) in the context of hacking attacks on large institutions and businesses. These are usually dangerous incidents in which huge amounts of data are leaked through the actions of cyber criminals. As a result, entire databases, containing not only people's names or addresses, but also medical data, phone numbers or passwords, are accessed or sold.

While large companies typically have a wide range of procedures in place to prevent unauthorized access to critical points in their IT infrastructure, this may not be the case in small companies. So all it takes is one employee with bad intentions for customer data, financial data, collaboration data and much more to fall into the wrong hands.

Many times, on a company's servers we can find a lot of information about the firm's employees, the operation of the enterprise, its organization, and even the company's deals with suppliers. Such information can be extremely tempting for someone who wants to steal data or share information with competitors, for example [3].

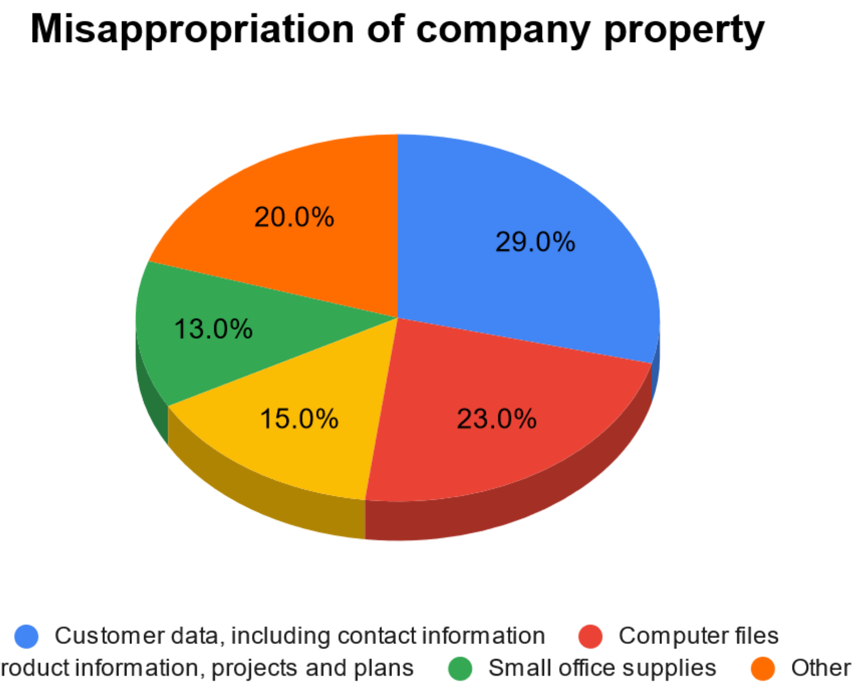


Fig. 1. Misappropriation of company property. Adapted from Help Net Security (2010) "Employees admit they would steal data when leaving a job"

The vast majority of security reports and industry portals indicate that humans remain the weakest link in cyber security systems. Research conducted by Forbes Insights on behalf of VMware shows that only 18 percent of European, including only 10 percent of Polish organizations, believe their employees have the right skills to counter cyber attacks [4]. This kind of mistake is usually made in good faith or unknowingly, and it doesn't have to be the employee's fault alone. It could be due to insufficient training, the development of bad habits or a lack of proper regulation.

Very often, data leaks through the action of malware in the form of computer worms, Trojan horses or spyware. The purpose of spyware is to collect information about the user and send data and information of the user or about the user without the user's knowledge to the author of the program or another person. Spyware programs include keyloggers, which record all the user's keyboard entries, browser hijacker software, which allows a website to be taken over and its settings changed, causing the user to be, for example, redirected to other sites, and password sniffers, which capture the initial data sequence of each session, containing the IDs and passwords of users of a given network [5].

There are also spoofing and phishing attacks. Phishing is distinguished from spoofing by one significant feature. While in spoofing the victim is persuaded to click on a malicious link in order to infect the device, in phishing the goal is to steal access passwords or other sensitive information [6].

According to the annual report prepared by CERT Polska, 10420 security incidents were registered in 2020. Compared to 2019, an upward trend of 60.7 percent can be observed. Phishing attacks ranked first and accounted for 73 percent of all incidents. The most popular phishing attack scenarios were attempts to obtain Facebook account login credentials and online banking login credentials [7].

In 2021, NASK CSIRT's analysis of submissions and incidents identified trends in the dominant identity theft threats:

- Repeated campaigns impersonating the OLX classifieds service.
- Incidents involving the theft of Facebook account credentials.
- Phishing campaigns impersonating courier companies and electricity suppliers.
- SMS campaigns that were initiated against the backdrop of the COVID-19 pandemic.

Data threats, while usually online, are not always related to online activities. Classic versions include:

- ID and driver's license theft.
- Loss of mail deliveries.
- Theft of PESEL identification numbers.
- Identity theft of the elderly.
- Failure of employees to follow procedures.

For example, the human resources department of a certain company uses a program to maintain employee records, including personnel files and matters related to the employment relationship. Unfortunately, however, the program has a flaw that prolongs the conduct of a certain activity. One employee found similar, free online software without this flaw and recommended it to other employees. Most of them transferred their documents there and used it exclusively. After some time, without prior warning, the website offering this service stopped working or was disabled. Employees lost access to all documents saved in this service, not knowing whether the service would ever return and whether the documents had been stolen and would be used in any way.

4.METHODS OF DETECTING IDENTITY THEFT

Like any attack, identity theft leaves traces. Law enforcement agencies usually check all activity performed on the computer. The operating memory, running processes, visited websites, connection list with IP addresses and files are secured. Unfortunately, there are ways to mask criminal activity, so evidence will not always point to the perpetrators [8]. There are other methods of detecting this type of fraud that every informed Internet user should use. Among them are:

- Monitoring and checking bank statements to catch suspicious transactions.
- Monitoring credit reports to identify suspicious activity, such as opening new bank accounts without the user's knowledge.
- Identity theft warnings through various types of services.
- Warnings of data breaches, password breaches, or breaches of internet accounts.

5.WAYS OF PREVENTING IDENTITY THEFT

Using networked computer devices, we transfer a large amount of information and documents. Increasingly, confidential data is also stored on hard drives. Their interception or modification can cause great damage, so it is necessary to pay attention to the state of computer security, the quality of the passwords used and an adequate level of education about the threats and their mechanisms. Every computer user, whether a private individual or an employee in a large enterprise, should follow established rules of conduct when using specific network resources and should apply the principle of limited trust, for example, when unsure about an e-mail message received.

The primary and fundamental method for computer protection is through the use of the appropriate antivirus software. There are numerous solutions available, each with varying levels of protection. It is advisable to select a product that offers comprehensive coverage, includes multiple protection modules, and minimally impacts the device's performance

Today's antivirus packages deal well with MITM attacks, detecting and repelling DNS spoofing, content tampering and manipulation, and SSL removal. To reduce the risk of attack, it is also recommended to avoid connecting to unsecured Wi-Fi networks, use VPN solutions, perform regular system and software updates, and use two-step authentication [9].

Unfortunately, 0-day attacks can be effective even when networks and the devices within them are well protected. When dealing with this type of attack, use common sense, don't open suspicious links and attachments, keep your software updated, and use high-end antivirus software [10].

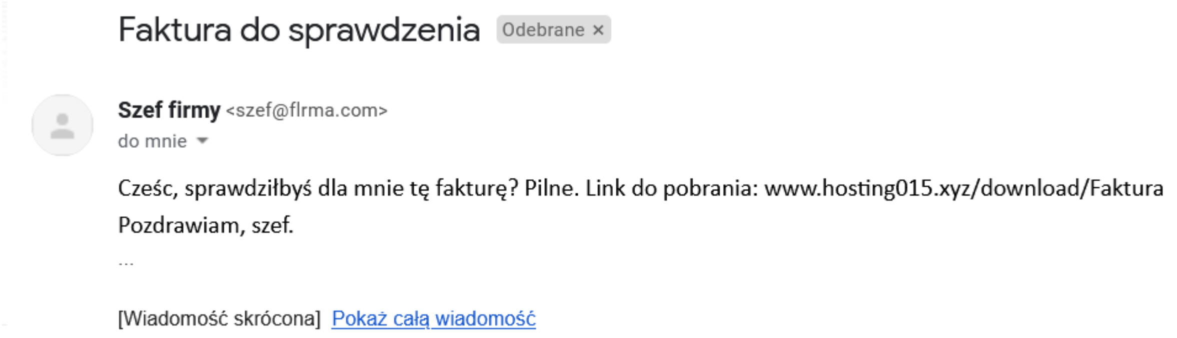
The best way to protect against spoofing is to avoid opening links and attachments from unknown sources. It is also advisable not to answer emails and phone calls from unknown people, use strong passwords, and pay attention to websites for correct placement of elements, spelling or missing content.

To avoid falling victim to a fake site, it is worth paying attention to the correctness and compatibility of the SSL certificate and securing the site via HTTPS (fake sites are often not secured, and their address starts with http). Password managers can also protect against fake websites, if the site is fake, the username and password fields will not be automatically completed.

Protection against phishing attacks is based on applying the principle of limited trust to unknown links and attachments, checking the validity of URLs, having an antivirus protection package and not revealing sensitive data, logins and passwords to others [11][12].

6.EXAMPLES OF ATTACKS THAT ENABLE THE ACQUISITION OF DATA FOR IDENTITY THEFT AND METHODS OF DEFENSE

The first attack we will discuss is a phishing attack. This type of attack involves sending a fake email containing a malicious attachment or a link leading to a fraudulent website. An unsuspecting employee may visit the fake website, which can put them at risk of sharing personal or login information with cybercriminals. This, in turn, could lead to more successful attack attempts or the leakage of company documents from the email service or company servers [13].



Faktura do sprawdzenia

Szef firmy <szef@flrma.com>
do mnie

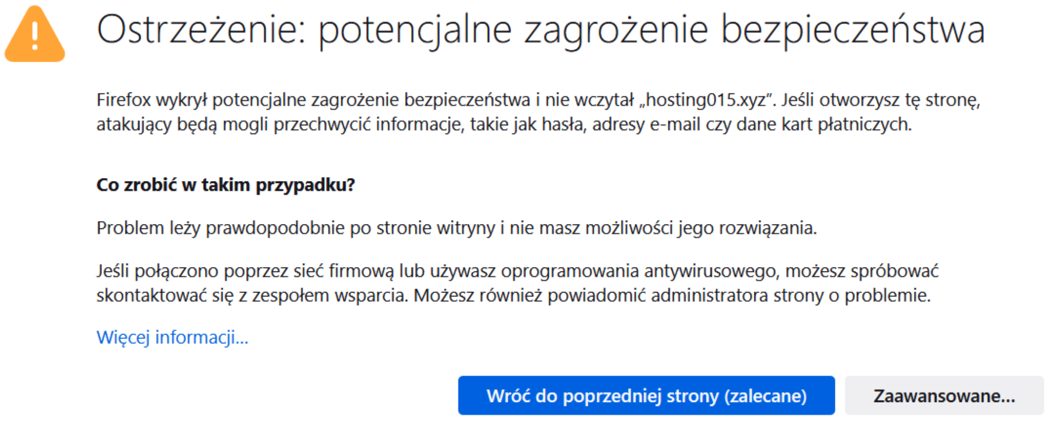
Cześc, sprawdziłbyś dla mnie tę fakturę? Pilne. Link do pobrania: www.hosting015.xyz/download/Faktura
Pozdrawiam, szef.

...

[Wiadomość skrócona] Pokaż całą wiadomość

Fig. 2. A phishing message trying to get a user to follow a link. Source: Author's own work

In this case, when entering a malicious link, we immediately get a message about the danger



Ostrzeżenie: potencjalne zagrożenie bezpieczeństwa

Firefox wykrył potencjalne zagrożenie bezpieczeństwa i nie wczytał „hosting015.xyz". Jeśli otworzysz tę stronę, atakujący będą mogli przechwycić informacje, takie jak hasła, adresy e-mail czy dane kart płatniczych.

Co zrobić w takim przypadku?

Problem leży prawdopodobnie po stronie witryny i nie masz możliwości jego rozwiązania.

Jeśli połączono poprzez sieć firmową lub używasz oprogramowania antywirusowego, możesz spróbować skontaktować się z zespołem wsparcia. Możesz również powiadomić administratora strony o problemie.

Więcej informacji...

Fig. 3. Warning of a potential security risk. Source: Author's own work

If the computer user chooses to add an exception and proceed, they will encounter a phishing page attempting to trick their login credentials.

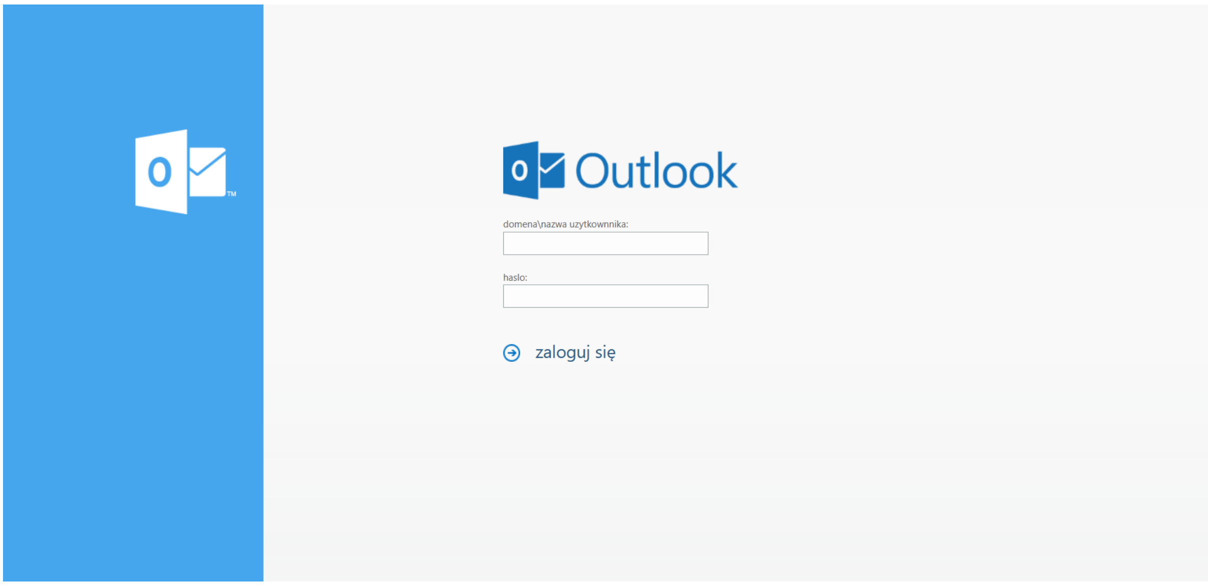


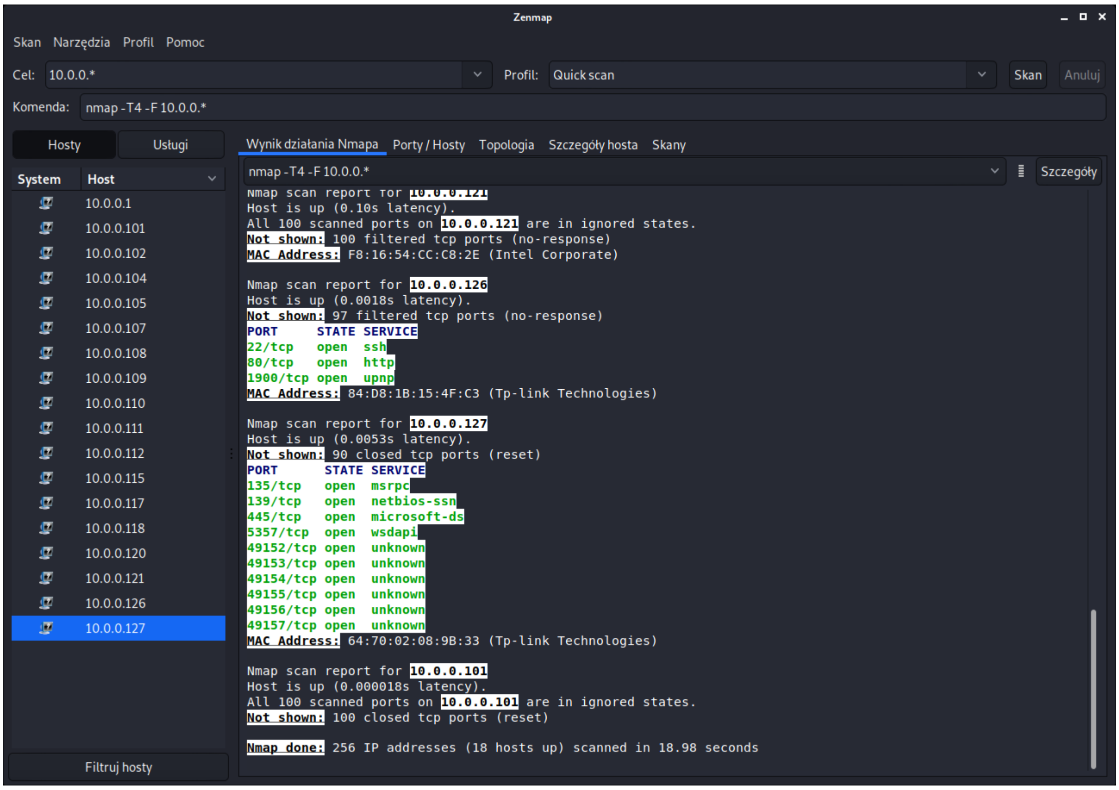
Fig. 4. Phishing site for login details. Source: Author's own work

Very often, these types of sites have grammatical errors and some visual differences that may not be noticeable at first glance. When the user enters login information, the site will send it to cyber criminals. This can lead to the leakage of confidential data, documents and other dangerous consequences.

The most effective defense against phishing attacks involves using common sense and applying a principle of limited trust to messages, attachments, and website links that you receive. Additionally, spam filters can be helpful, although they may not be effective in every case.For example, if a user receives an email, but is unsure of its authenticity, they may pay attention to certain features that phishing messages have in common.

The first such feature is a request to follow a link with a fake URL or download a file from an attachment. The second feature is numerous spelling errors, an unofficial email address of the sender and the use of a generic greeting, with no details of the recipient. Keep in mind that companies don't usually send messages asking for passwords, credit card details, or sending sensitive data. If the recipient still has doubts about the veracity of an email received, they can always seek advice from their company's IT department or inform his or her supervisor, who will implement appropriate procedures or confirm the authenticity of the message [14].

The second attack will be an attempt to gain access to an unsecured computer on the network by exploiting a known vulnerability to steal data used for identity theft. The Nmap scanner was helpful in this attack, along with the official Zenmap GUI, which, in addition to displaying data, allows us to create a graphical representation of the network being scanned. After checking the IP range, we proceeded with the scan, which showed all devices connected to the network. One device, in particular, had the address 10.0.0.127 and an unusually large number of open ports.



Cel: 10.0.0.*

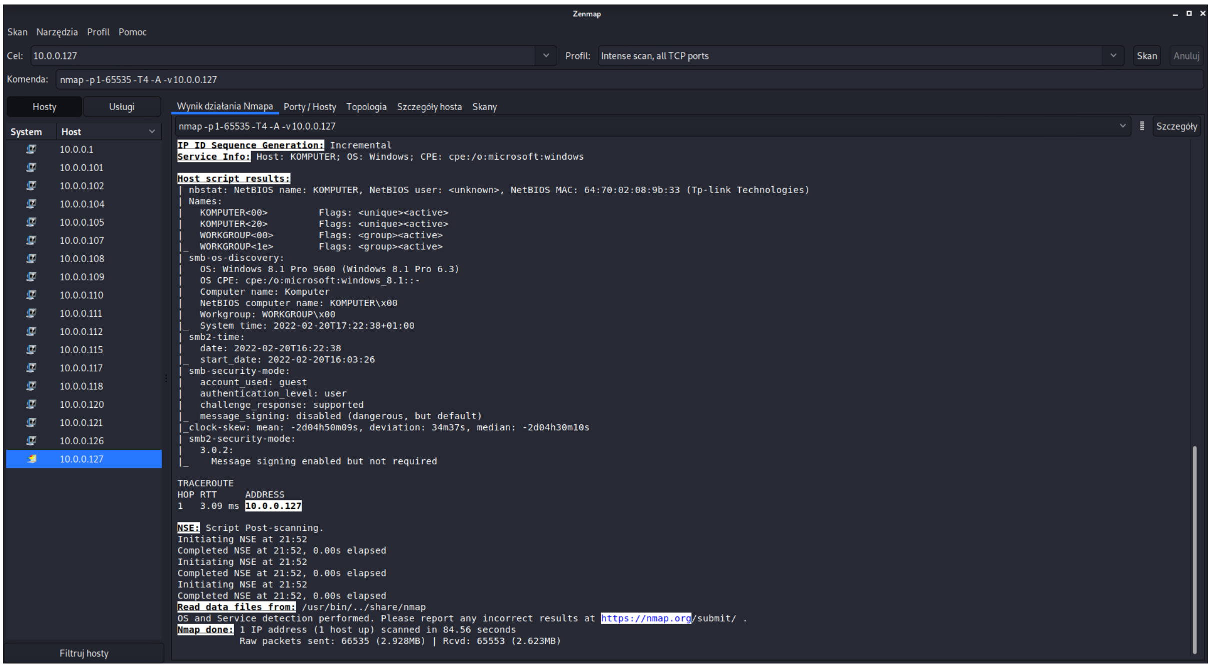
Profil: Quick scan

Komenda: nmap -T4 -F 10.0.0.*

```
nmap -T4 -F 10.0.0.*
Nmap scan report for 10.0.0.121
Host is up (0.10s latency).
All 100 scanned ports on 10.0.0.121 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
MAC Address: F8:16:54:CC:C8:2E (Intel Corporate)

Nmap scan report for 10.0.0.126
Host is up (0.0018s latency).
Not shown: 97 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1900/tcp open  upnp
MAC Address: 84:D8:1B:15:4F:C3 (Tp-link Technologies)

Nmap scan report for 10.0.0.127
Host is up (0.0053s latency).
Not shown: 90 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 64:70:02:08:9B:33 (Tp-link Technologies)

Nmap scan report for 10.0.0.101
Host is up (0.000018s latency).
All 100 scanned ports on 10.0.0.101 are in ignored states.
Not shown: 100 closed tcp ports (reset)

Nmap done: 256 IP addresses (18 hosts up) scanned in 18.98 seconds
```

Fig. 5. Zenmap network scan result. Source: Author's own work

Based on this, it can be estimated that, in all probability, no security suite or firewall is active on this device. A thorough scan of the IP address in question showed more detailed information about the device, including the installed system and its version. Open ports (which were visible) allow an attacker to identify the services running on the vulnerable machine. Similarly, the version of the installed system has its own identified security vulnerabilities that can be exploited.



Cel: 10.0.0.127

Profil: Intense scan, all TCP ports

Komenda: nmap -p1-65535 -T4 -A -v 10.0.0.127

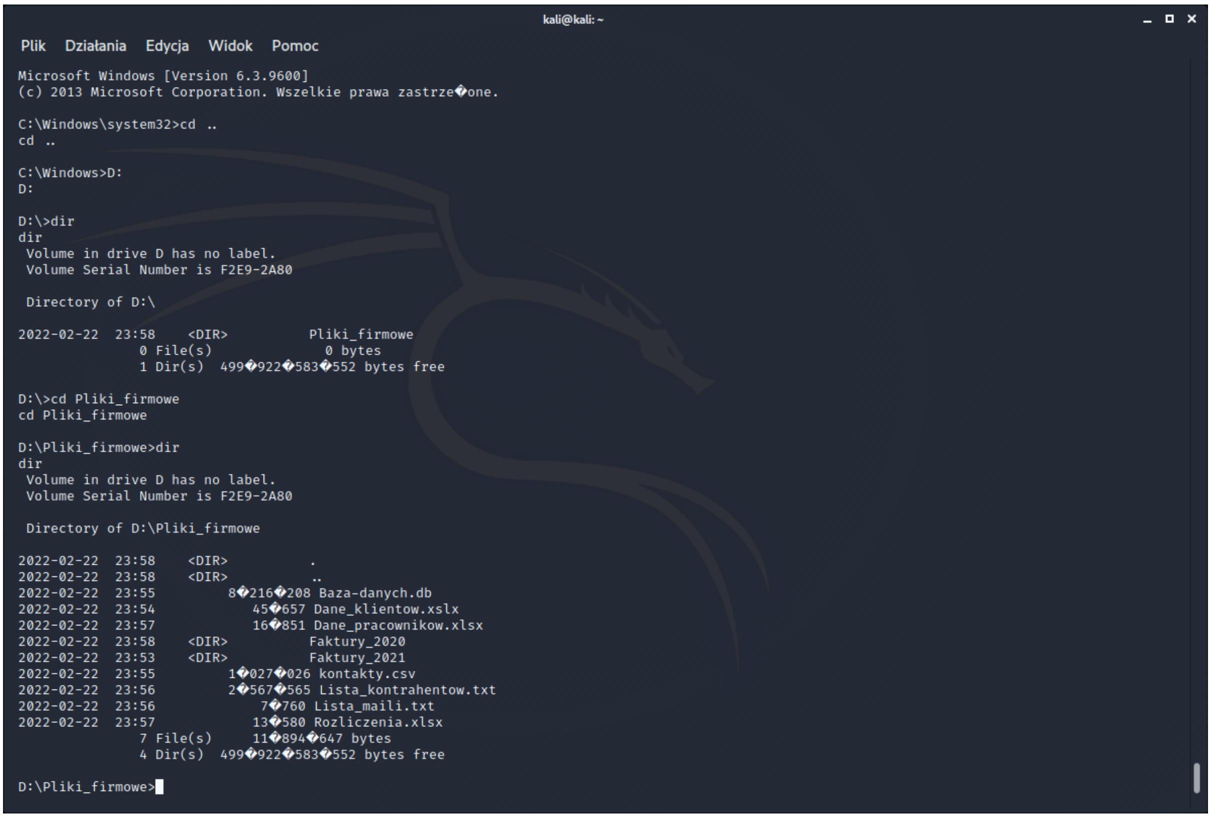
```
nmap -p1-65535 -T4 -A -v 10.0.0.127
IP ID Sequence Generation: Incremental
Service Info: Host: KOMPUTER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: KOMPUTER, NetBIOS user: <unknown>, NetBIOS MAC: 64:70:02:08:9b:33 (Tp-link Technologies)
| Names:
|   KOMPUTER<00>         Flags: <unique><active>
|   KOMPUTER<20>         Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 8.1 Pro 9600 (Windows 8.1 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_8.1::-
|   Computer name: Komputer
|   NetBIOS computer name: KOMPUTER\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-02-20T17:22:38+01:00
| smb2-time:
|   date: 2022-02-20T16:22:38
|_  start_date: 2022-02-20T16:03:26
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -2d04h50m09s, deviation: 34m37s, median: -2d04h30m10s
| smb2-security-mode:
|   3.0.2:
|_    Message signing enabled but not required

TRACEROUTE
HOP RTT     ADDRESS
1   3.09 ms 10.0.0.127

NSE: Script Post-scanning.
Initiating NSE at 21:52
Completed NSE at 21:52, 0.00s elapsed
Initiating NSE at 21:52
Completed NSE at 21:52, 0.00s elapsed
Initiating NSE at 21:52
Completed NSE at 21:52, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 84.56 seconds
           Raw packets sent: 66535 (2.928MB) | Rcvd: 65553 (2.623MB)
```

Fig. 6. Detailed information about the attacked computer. Source: Author's own work

Successful exploitation of vulnerabilities, largely depends on the results achieved in the previous stages. Incompetent selection and exploitation of a vulnerability may simply not work or cause unforeseen consequences, for example, lead to disruption or collapse of the attacked system.

In exploiting the vulnerabilities found on the victim's computer, we used ports related to the SMB protocol, which allows sharing computer resources, including files and printers. To increase the effectiveness of the attack, it is important to check the version of specific services by additionally scanning the ports associated with those services. To exploit the vulnerability, we used the Metasploit tool along with the smb_ms17_010 helper module. Thanks to the said module, vulnerability MS17-010 was detected on the computer. The next part of the attack was to find an exploit that would help directly attack the vulnerable service. An exploit named EternalBlue was used. After setting the appropriate parameters and uploading the payload, we established a connection to the victim's computer.

It allowed the user to run any PowerShell command, view and download files on the victim's disk, eavesdrop on input, view the monitor screen, active processes and much more [15].

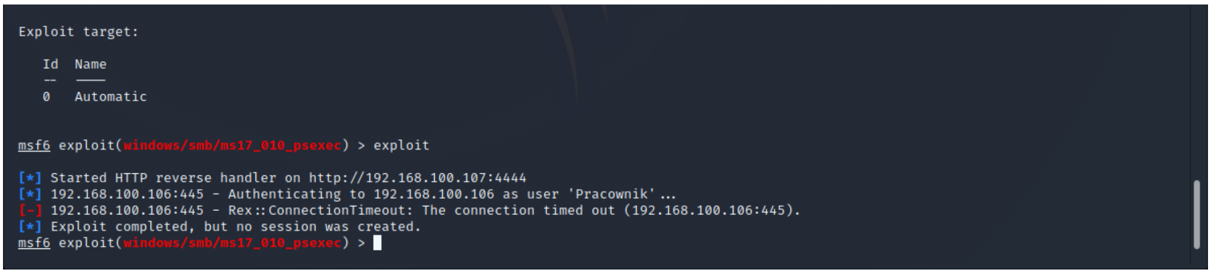


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. Wszelkie prawa zastrze�one.

C:\Windows\system32>cd ..
cd ..

C:\Windows>D:
D:

D:\>dir
dir
 Volume in drive D has no label.
 Volume Serial Number is F2E9-2A80

 Directory of D:\

2022-02-22  23:58    <DIR>          Pliki_firmowe
               0 File(s)              0 bytes
               1 Dir(s)  499�922�583�552 bytes free

D:\>cd Pliki_firmowe
cd Pliki_firmowe

D:\Pliki_firmowe>dir
dir
 Volume in drive D has no label.
 Volume Serial Number is F2E9-2A80

 Directory of D:\Pliki_firmowe

2022-02-22  23:58    <DIR>          .
2022-02-22  23:58    <DIR>          ..
2022-02-22  23:55         8�216�208 Baza-danych.db
2022-02-22  23:54            45�657 Dane_klientow.xslx
2022-02-22  23:57            16�851 Dane_pracownikow.xlsx
2022-02-22  23:58    <DIR>          Faktury_2020
2022-02-22  23:53    <DIR>          Faktury_2021
2022-02-22  23:55         1�027�026 kontakty.csv
2022-02-22  23:56         2�567�565 Lista_kontrahentow.txt
2022-02-22  23:56             7�760 Lista_maili.txt
2022-02-22  23:57            13�580 Rozliczenia.xlsx
               7 File(s)     11�894�647 bytes
               4 Dir(s)  499�922�583�552 bytes free

D:\Pliki_firmowe>
```

Fig. 7. Access to confidential data of the attacked computer. Source: Author's own work

There is no method to completely prevent port scanning on devices, however, there are solutions to limit or block this type of attack. On personal computers, install an antivirus package that includes a firewall, or run and configure a system firewall. It is also worth using IDS (intrusion detection system) solutions, which perform real-time analysis of traffic and detect and block various types of attacks. As an additional safeguard, blocking unused ports will minimize the number of possible attacks.

Since exploits are the result of an error by the manufacturer of the software in question, and it is the manufacturer who is responsible for distributing security updates, there is no good way to protect against this type of attack. First and foremost, install all security patches, have high-end antivirus software and use common sense when using the Internet. Even if security patches are not applied by the software manufacturer on short notice, antiviruses, by receiving updates to detect vulnerabilities, comparing virus signatures and using heuristics, are able to stop the threat even before the software manufacturer applies patches [16].



```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started HTTP reverse handler on http://192.168.100.107:4444
[*] 192.168.100.106:445 - Authenticating to 192.168.100.106 as user 'Pracownik'...
[-] 192.168.100.106:445 - Rex::ConnectionTimeout: The connection timed out (192.168.100.106:445).
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_psexec) > 
```

Fig. 8. Blocked attack using the EternalBlue exploit - view from the attacker's computer. Source: Author's own work

7.CONCLUSION

Recent years have shown how many tasks can be entrusted to electronic devices. Unfortunately, security issues are in many cases downplayed, leading to regular attacks, identity theft and data leaks. The level of awareness of cyber security is steadily increasing, however, there is still a lot of work to be done in this area for everyone. A prime example of the marginal treatment of security issues is the lack of training for employees.

On the one hand, technology makes many tasks easier and faster, but on the other hand, we see situations where data can be compromised. It is not difficult to have a moment of inattention or weakness, which can result in opening a suspicious link or downloading a malicious file. Raising awareness through regular education about threats and solutions to protect against them remains the foundation.

When developing and implementing fully effective procedures and systems, it is important to strive to use not only physical and software protection packages, but also to increase employees' knowledge and awareness of cyber security, as in many cases humans are the weakest link. The use of information on protection methods helps avoid dangerous situations involving the leakage of various types of data, including access or confidential data and also helps protect everyone's identity.

8.OTHER

Author Contributions

All authors declare equal contribution to this research paper.

Conflicts of Interest

☑ *The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.*

☐ *The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:*

…………………………………………………………………………………………

REFERENCES

[1] European Union Agency for Cybersecurity (2020). Kradzież tożsamości Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-identity-theft-ebook-en-pl.pdf

[2] Marshall, A.M., & Tompsett, B.C. (2005). Identity theft in an online world. Computer Law & Security Review, 21(2), 128-137. https://doi.org/10.1016/j.clsr.2005.02.004

[3] PurpleSec. (2022, January 10). Cyber Security Statistics: The Ultimate List Of Stats Data, & Trends For 2022. https://purplesec.us/resources/cyber-security-statistics/

[4] Virtual-IT. (2019, July 19). [Raport VMware] Tylko 10% firm w Polsce ufa pracownikom i cyberzabezpieczeniom. https://www.virtual-it.pl/9649-raport-vmware-tylko-10-firm-w-polsce-ufa-pracownikom-i-cyberzabezpieczeniom.html

[5] Hu, Q., & Dinev, T. (2005). Is spyware an Internet nuisance or public menace?. Communications of the ACM, 48(8), 61-66. https://doi.org/10.1145/1076211.1076241

[6] Najwyższa Izba Kontroli. (2023, March 7). Obywatelu, przed cyberatakiem broń się sam. https://www.nik.gov.pl/aktualnosci/przestepstwa-internetowe-zapobieganie-i-zwalczanie.html

[7] CERT Polska. (2020). Krajobraz bezpieczeństwa polskiego internetu, Raport roczny z działalności CERT Polska, 13.

[8] Rzeczpospolita (2013, October 10). Cyberprzestępstwa: Kradzież danych osobowych w Internecie. https://www.rp.pl/dane-osobowe/art5339031-cyberprzestepstwa-kradziez-danych-osobowych-w-internecie

[9] Słupczewski B.(2022, February 2). Zapobieganie Kradzieży Tożsamości. https://www.wojsko-polskie.pl/woc/articles/publikacje-r/zapobieganie-kradziezy-tozsamosci/

[10] Avast Software (2022, February 19). Co to jest Zero Day Exploit?. https://www.avast.com/pl-pl/c-zero-day

[11] Gupta, B.B., Arachchilage, N.A.G. & Psannis, K.E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommun Syst 67, 247–267. https://doi.org/10.1007/s11235-017-0334-z

[12] Orange. (2019, February 25). Co to jest ransomware i jak się zabezpieczyć przed złośliwym oprogramowaniem?. https://web.archive.org/web/20200409172611/https://www.orange.pl/poradnik/twoj-internet/co-to-jest-ransomware-i-jak-sie-zabezpieczyc-przed-zlosliwym-oprogramowaniem/

[13] ESET (2022, January 5). Eksperci cyberbezpieczeństwa podsumowują 2021 rok. https://www.eset.com/pl/about/newsroom/press-releases/news/eksperci-cyberbezpieczenstwa-podsumowuja-2021-rok/

[14] Jakobsson, M., Tsow, A., Shah, A., Blevis, E., Lim, YK. (2007). What Instills Trust? A Qualitative Study of Phishing. In: Dietrich, S., Dhamija, R. (eds) Financial Cryptography and Data Security. FC 2007. Lecture Notes in Computer Science, 4886. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-77366-5_32

[15] Dimov, R., Nikolov, L., Dimov, D. (2021). Vulnerability Analysis in Server Systems. Security & Future, 5(4), 141-146.

[16] Muniz J., Lakhani A. (2017). Kali Linux. Testy penetracyjne. Helion. 36, 140.