CVE-2025-0411: Ukrainian Organizations Targeted in Zero-Day Campaign and Homoglyph Attacks

By: Peter Girnus February 04, 2025 Read time: 10 min (2645 words)

Summary

In September, 2024 the Trend Zero Day Initiative™ (ZDI) Threat Hunting team identified the exploitation of a 7-Zip zero-day vulnerability used in a SmokeLoader malware campaign targeting Ukrainian entities.

The vulnerability, CVE-2025-0411, was disclosed to 7-Zip creator Igor Pavlov, leading to the release of a patch in version 24.09 on November 30, 2024.

CVE-2025-0411 allows the bypassing of Windows Mark-of-the-Web protections by double archiving files, thus preventing necessary security checks and allowing the execution of malicious content.

The vulnerability was actively exploited by Russian cybercrime groups through spear-phishing campaigns, using homoglyph attacks to spoof document extensions and trick users and the Windows Operating System into executing malicious files.

The vulnerability was likely exploited as a cyberespionage campaign against Ukrainian government and civilian organizations as part of the ongoing Russo-Ukraine conflict.

We provide recommendations for organizations to proactively secure their systems. This includes updating 7-Zip to at least version 24.09, implementing strict email security measures, and conducting employee training on phishing (including homoglyph attacks).

Introduction

On September 25, 2024, the Trend ZDI Threat Hunting team identified a zero-day vulnerability exploited in-the-wild and associated with the deployment of the loader malware known as SmokeLoader. This vulnerability is believed to be used by Russian cybercrime groups to target both governmental and non-governmental organizations in Ukraine, with cyberespionage being the most likely purpose of these attacks as part of the ongoing Russo-Ukrainian conflict. The exploitation involves the use of compromised email accounts and a zero-day vulnerability existing in the archiver tool 7-Zip (CVE-2025-0411), which was manipulated through homoglyph attacks (which we will also define and explain in this blog entry).

Following initial analysis and the development of a proof-of-concept (PoC), we formally disclosed the vulnerability to Igor Pavlov, the creator of 7-Zip, on October 1, 2024. The issue was

subsequently addressed, with 7-Zip releasing a patch as part of version 24.09 on November 30, 2024.

This entry will first examine CVE-2025-0411 in a theoretical context, based on the PoC submitted to 7-Zip. Subsequently, we will analyze the real-world exploitation of this vulnerability as a zero-day in active use.

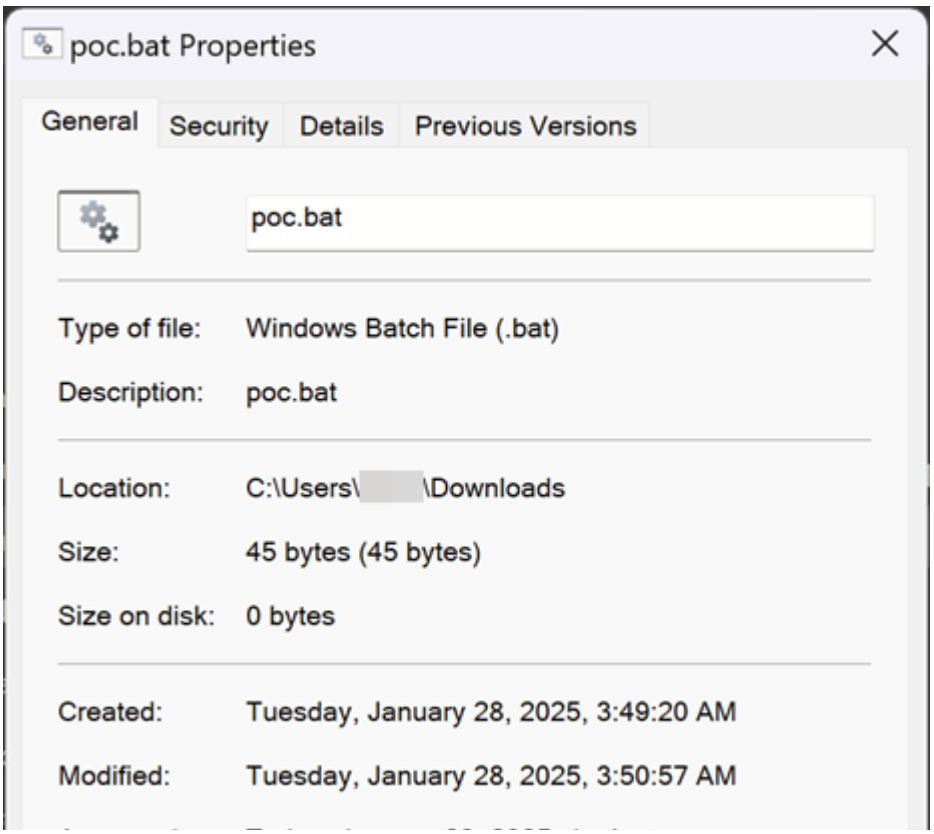
CVE-2025-0411: 7-Zip Mark-of-the-Web Bypass Vulnerability

When a user downloads a file from an untrusted source, such as the internet, Microsoft Windows implements a security feature known as the Mark-of-the-Web (MoTW). This feature marks the local copy of the file by adding an NTFS Alternate Data Stream (ADS) named *Zone.Identifier*. Within this stream, the text *ZoneId=3* is embedded, signifying that the file came from an untrusted zone, specifically the internet. This ensures that untrsuted files are not accidentally executed and allows the Windows operating system to perform extra security checks through Microsoft Defender SmartScreen.

CVE-2025-0411 allows threat actors to bypass Windows MoTW protections by double archiving contents using 7-Zip. Double archiving involves incapsulating an archive within an archive.

```
PS C:\Users\[redacted]\Downloads> Get-Content -path "C:\Users\[redacted]\Downloads\Документи та пл
атежи.7z" -stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
ReferrerUrl=http://127.0.0.1:8000/Downloads/poc/
HostUrl=http://127.0.0.1:8000/Downloads/poc/%D0%94%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D
1%82%D0%B8%20%D1%82%D0%B0%20%D0%BF%D0%BB%D0%B0%D1%82%D0%B5%D0%B6%D0%B8.7z
PS C:\Users\[redacted]\Downloads>
```

Figure 1. The Zone.Identifier of the outer encapsulated archive



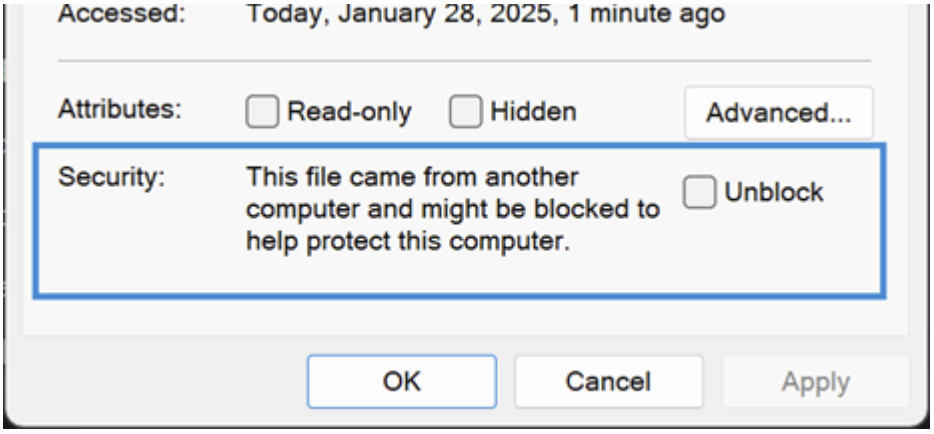


Figure 2. The Properties view of a file containing a MoTW

An MoTW designation helps prevent the automatic execution of potentially harmful scripts or applications by notifying the system and user to treat the file with caution and then directing it to perform additional analysis via Windows Defender SmartScreen.

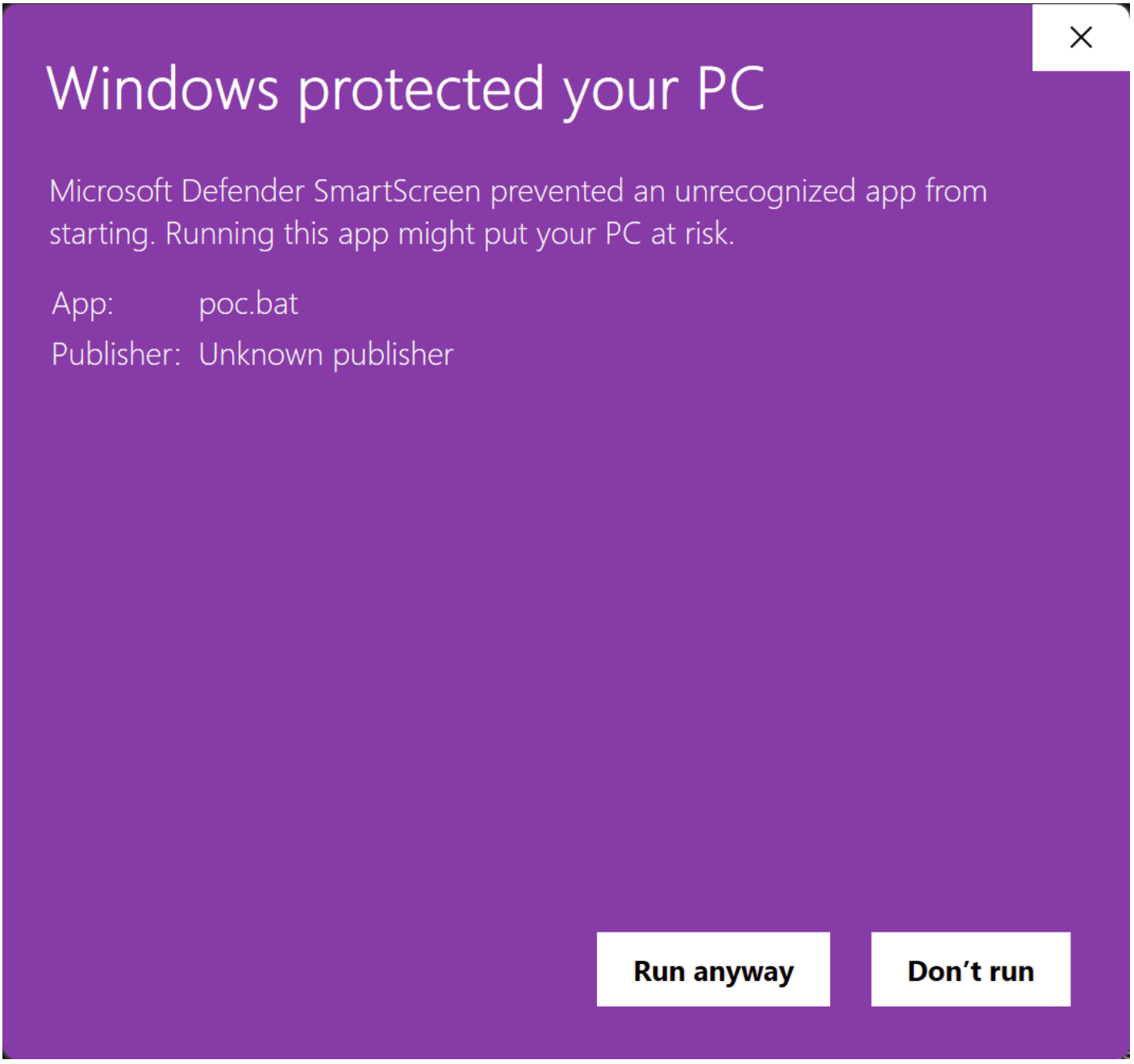


Figure 3. Windows Defender SmartScreen Security warning prompted by MoTW

Windows MoTW is an important part of the Windows security architecture and is needed for other key Windows protection mechanisms to function, such as:

Windows Defender SmartScreen, which examines files based on reputation and signature.

Microsoft Office Protected View, which protects users from threats such as malicious macros and Dynamic Data Exchange (DDE) attacks.

The root cause of CVE-2025-0411 is that prior to version 24.09, 7-Zip did not properly propagate MoTW protections to the content of double-encapsulated archives. This allows threat actors to craft archives containing malicious scripts or executables that will not receive MoTW protections, leaving Windows users vulnerable to attacks.

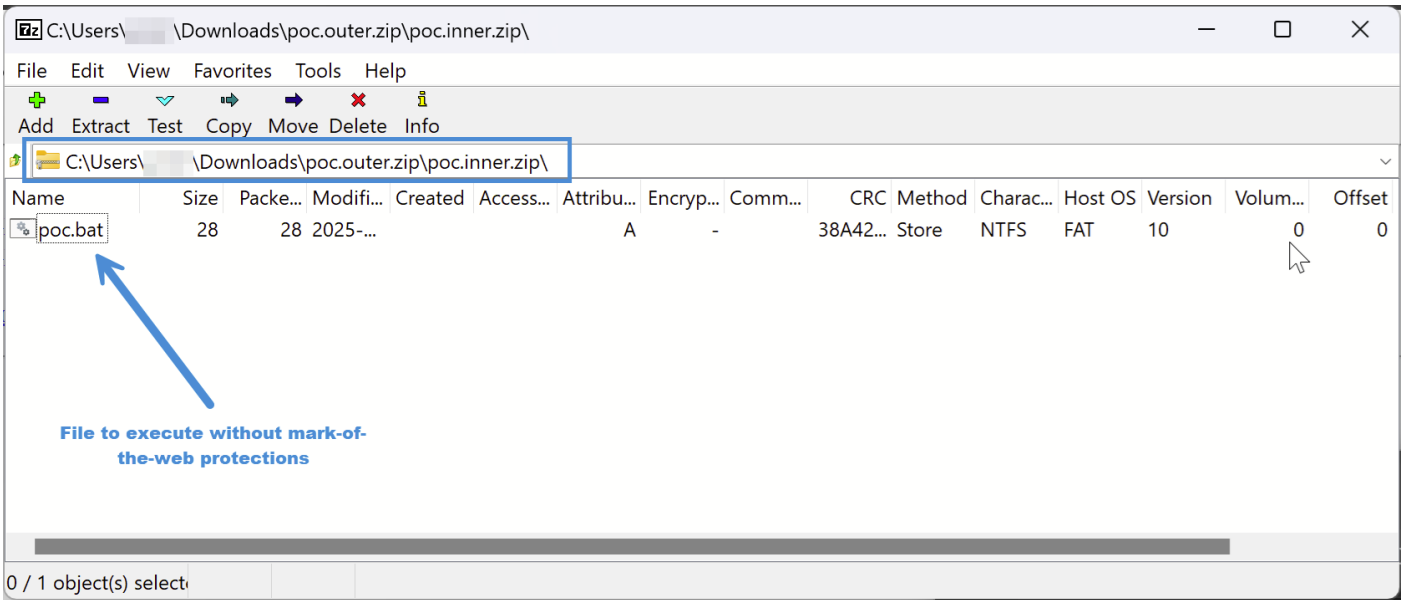


Figure 4. PoC demo of CVE-2025-0411 with encapsulated ZIP archive

In Figure 4, the *poc.bat* file has no MoTW protections since it is encapsulated inside the *poc.outer.zip\poc.inner.zip* archive. This greatly increases the risk of infection and prevents Microsoft Windows Defender SmartScreen from performing reputation and signature checks.

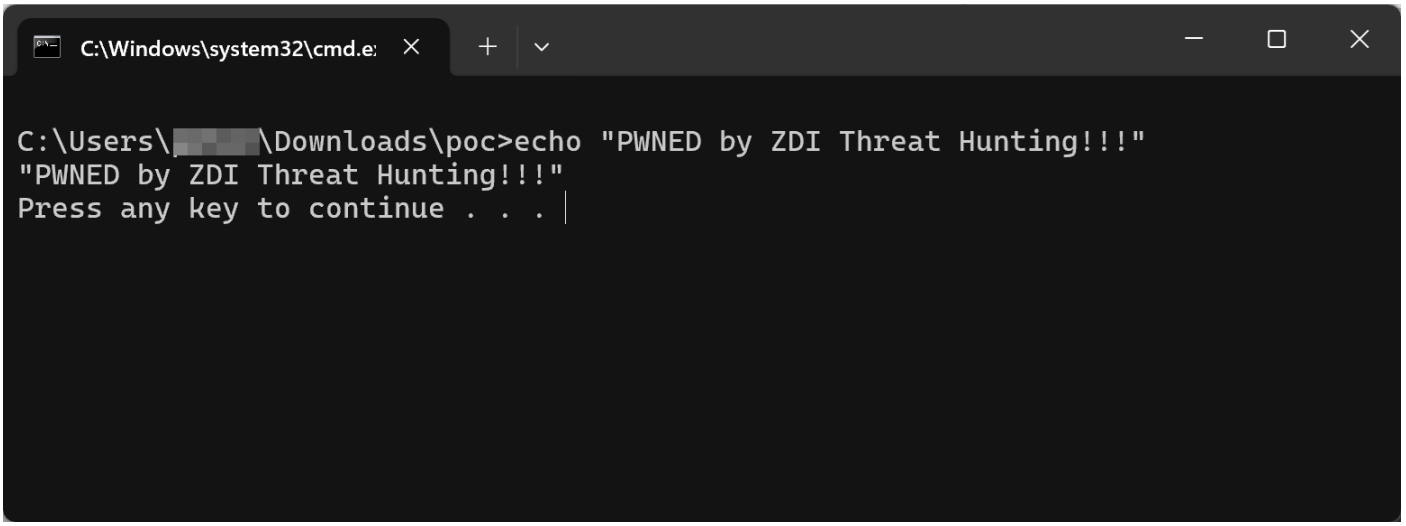


Figure 5. Users are compromised once poc.bat is executed

Now that we have covered a simple example of CVE-2025-0411, let's examine how this

vulnerability was exploited in the wild by Russian cybercrime groups.

CVE-2025-0411 exploited as a Zero Day by Russian cybercrime groups

As mentioned in our introduction, we first uncovered this zero-day exploit in the wild on September 25, 2024. This vulnerability was used to target both the Ukrainian government and other Ukrainian organizations in a SmokeLoader campaign that was likely deployed by Russian cybercrime groups.

During our investigation, we uncovered emails originating from multiple Ukranian governing bodies and Ukrainian business accounts targeting both Ukrainian municipal organizations and Ukrainian businesses.

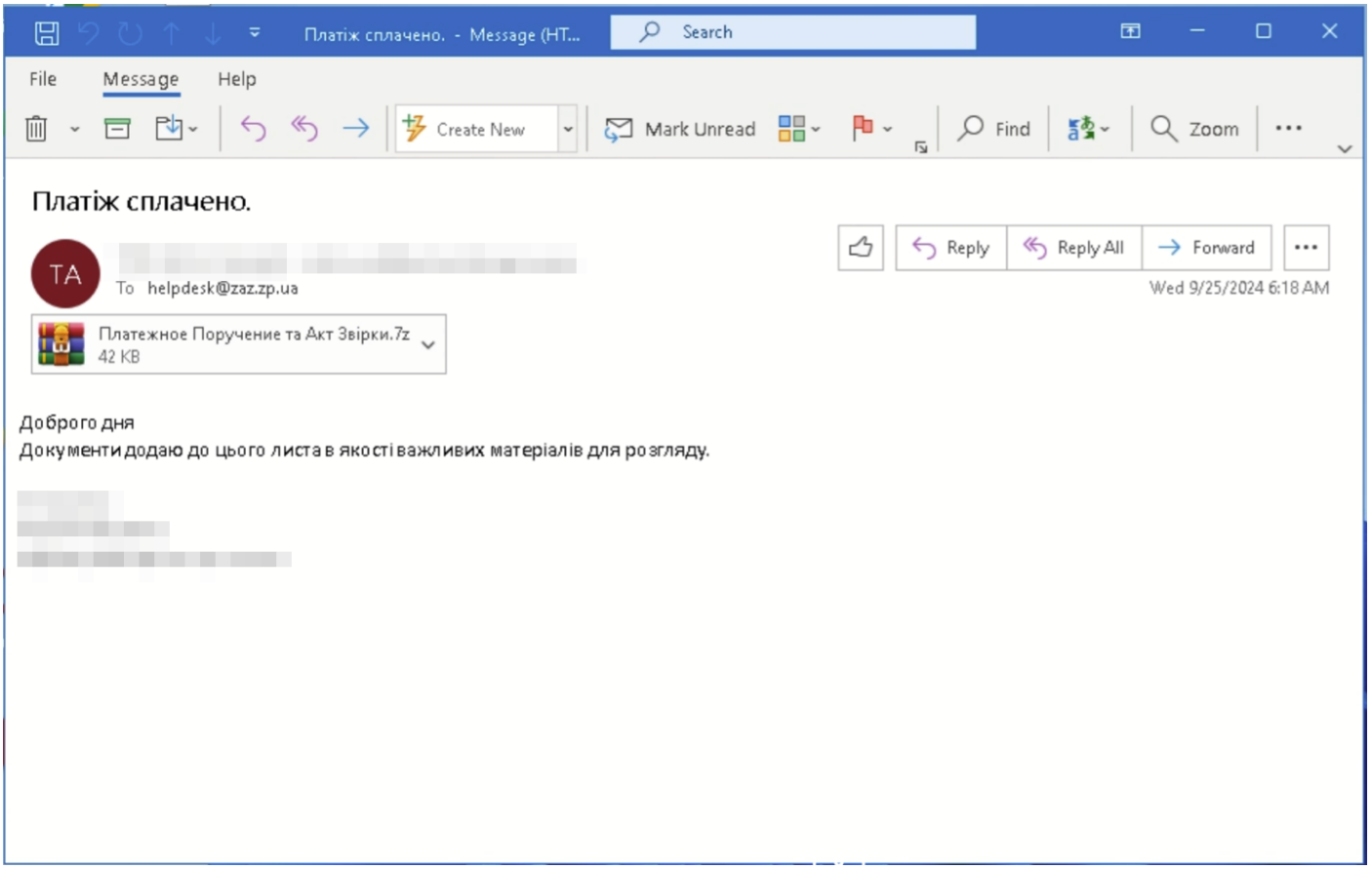


Figure 6. Sample phishing email coming from a compromised Ukrainian government email account

In Figure 6, we see a 7-Zip attachment (SHA256: ba74ecae43adc78efaee227a0d7170829b9036e5e7f602cf38f32715efa51826) coming from an email account belonging to the State Executive Service of Ukraine (SES), a former organization within the Ukrainian executive branch, that has now been merged with the Ukrainian Ministry of Justice. The recipient of this spear phishing email is the helpdesk of the Zaporizhzhia Automobile Building Plant (PrJSC ZAZ) — ZAZ being one of the largest manufacturers of automobiles, trucks, and buses within Ukraine. For some regional context, the Zaporizhzhia Oblast is an important industrial region within Ukraine which experienced some of the most intense fighting between Ukrainian and Russian forces since the start of the conflict in 2022. On March 3, 2022, the fighting culminated in

the Russian capture of the Zaporizhzhia nuclear power plant, raising concerns about a potential nuclear meltdown.

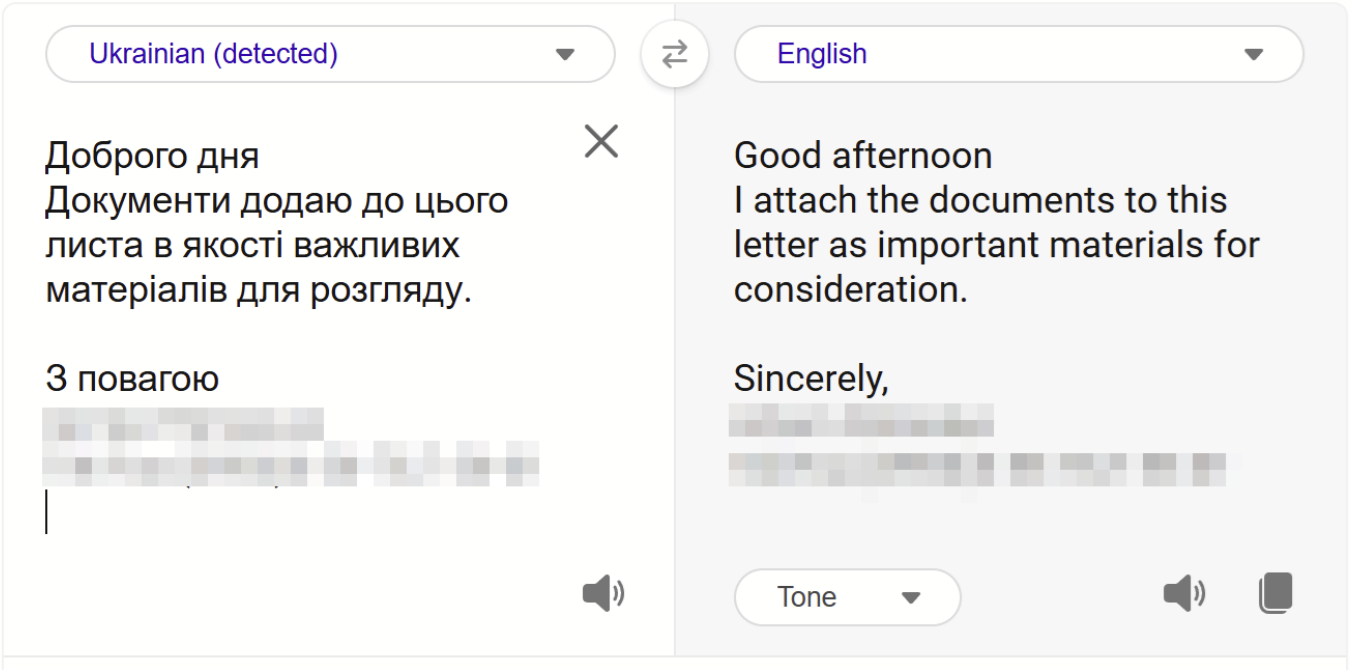


Figure 7. Email translation from Ukrainian to English

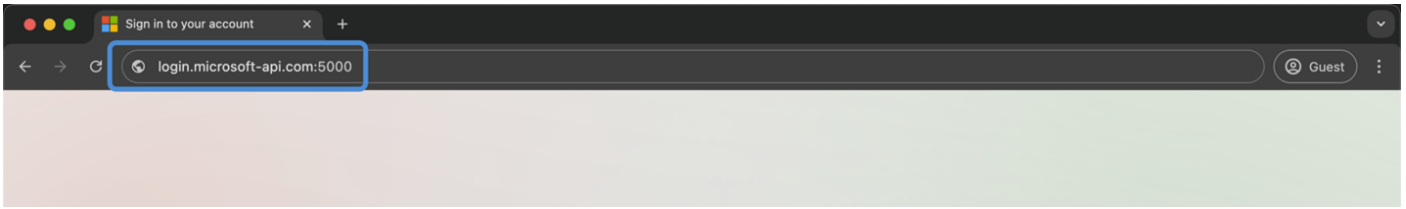
This email was first uploaded to VirusTotal on September 25, 2024.

The exploitation of CVE-2025-0411 via homoglyph attacks

Earlier, we discussed a working PoC exploit of CVE-2025-0411 that used a nested archive structure such as *poc.outer.zip/poc.inner.zip/poc.bat*. In the samples we uncovered as part of the SmokeLoader campaign, the inner ZIP archive deployed a homoglyph attack to spoof a Microsoft Windows Document (.doc) file.

A homoglyph attack is a type of attack incorporating typographic manipulation using similar-looking characters to fool victims into clicking suspicious files or visiting malicious websites. These attacks are commonly used as part of phishing campaigns. where threat actors might use homoglyphs for spoofing legitimate websites to trick users into entering their credentials for credential harvesting. These credentials would then be employed as a pivot point to further compromise an organization.

As an example, an attacker may use the Cyrillic letter *Es* (which looks exactly like the Latin letter *C* or *c*) in a domain name such as api-microsoft[.]com, with “c” here being the “Es” character instead of the Latin one, to trick users into trusting this domain —perhaps to lure them into entering sensitive details such as usernames and passwords.



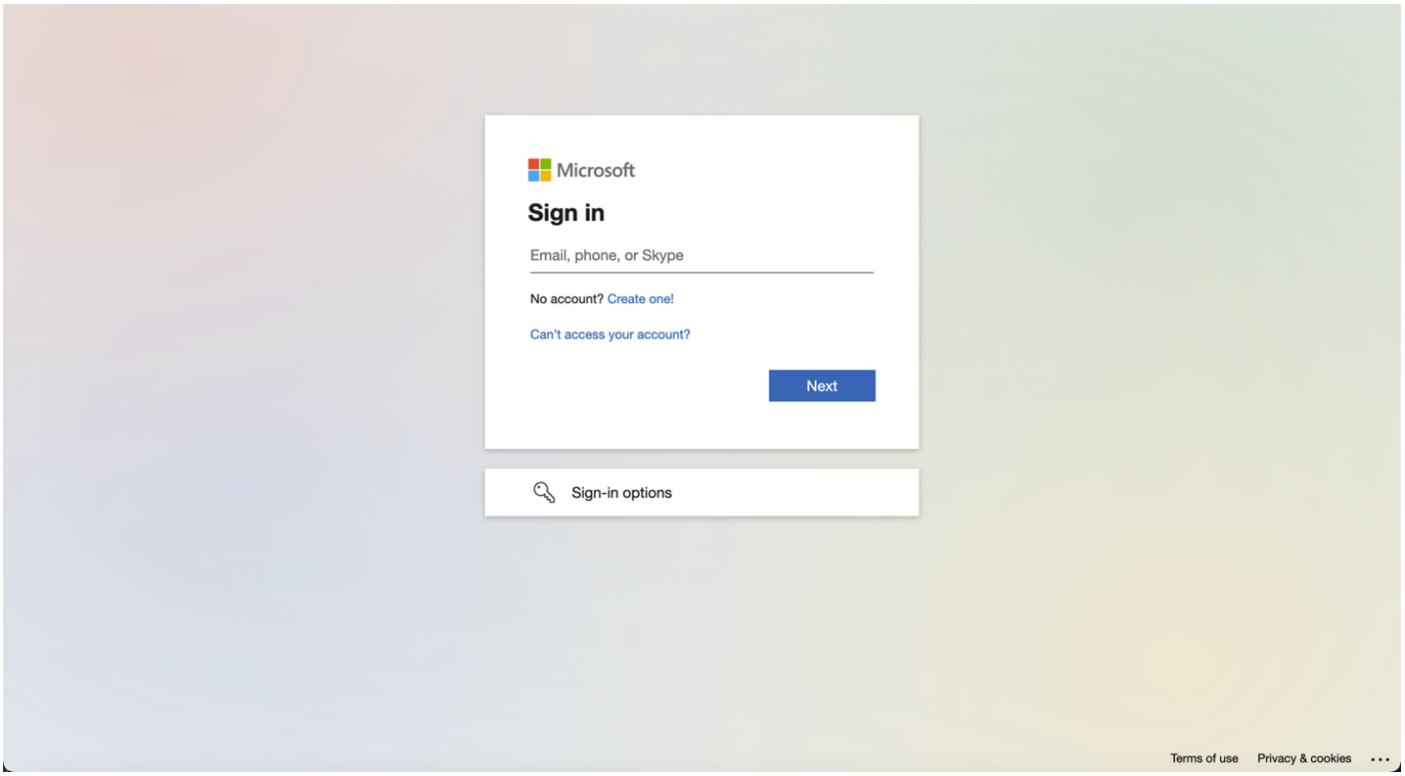
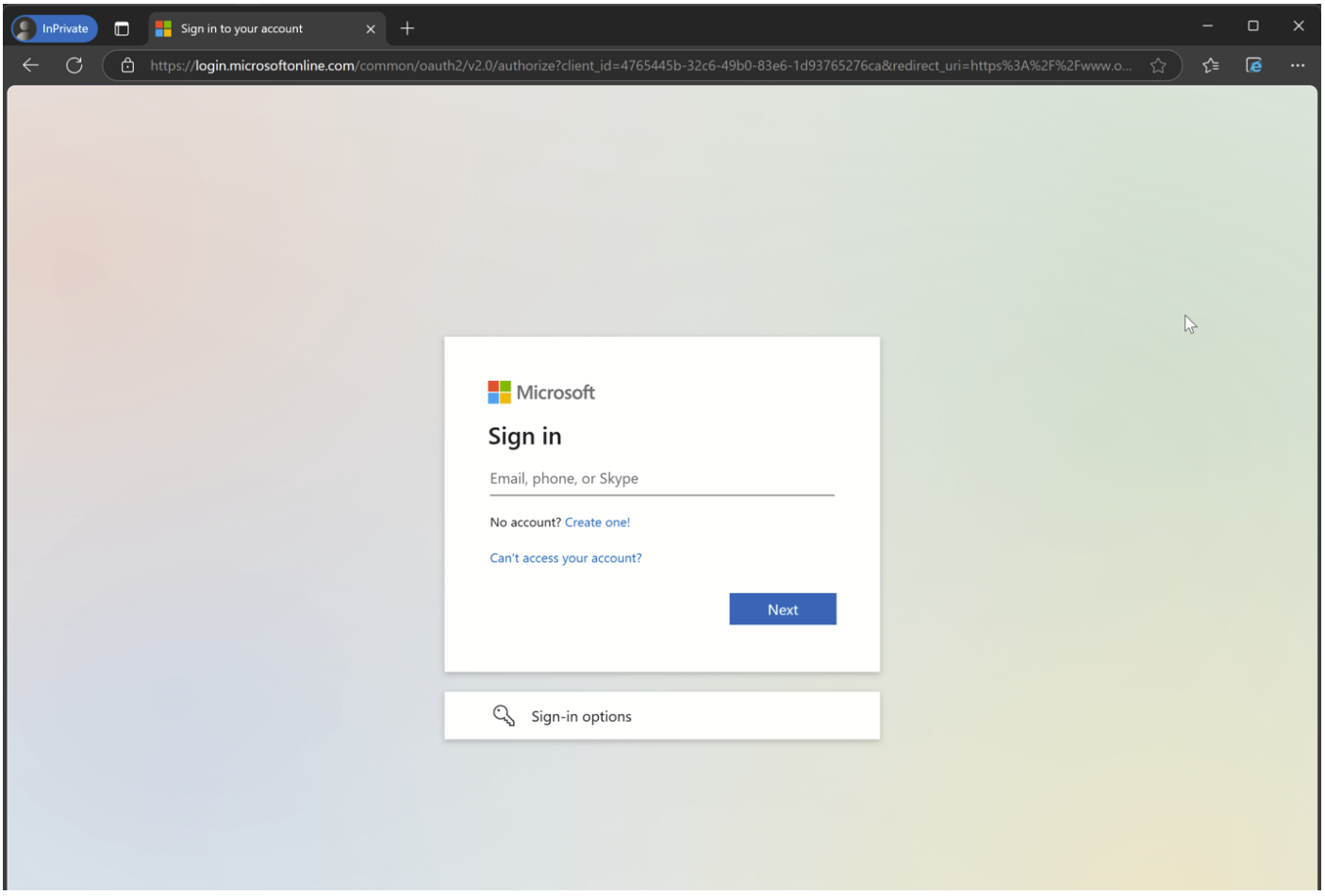


Figure 8. The letter c is replaced with the Cyrillic Es (c) homoglyph

In Figure 8, the potential for deception presented by homoglyph characters is clearly demonstrated. A fully spoofed Microsoft domain has been created by substituting the Latin character “C” with the Cyrillic character “Es” (C). This typographic manipulation effectively misleads individuals into believing that they are accessing a legitimate Microsoft domain, thereby causing them to perceive the login screen as being part of an authentic site.



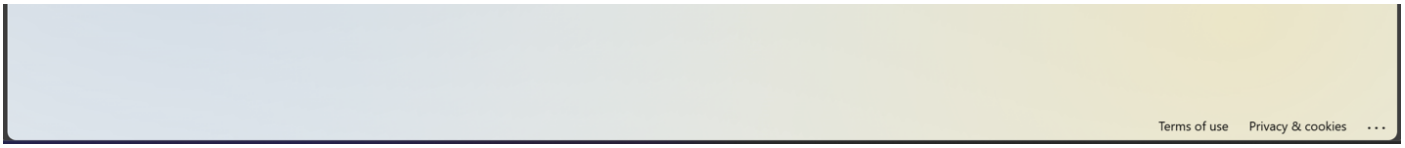


Figure 9. A real Microsoft login domain

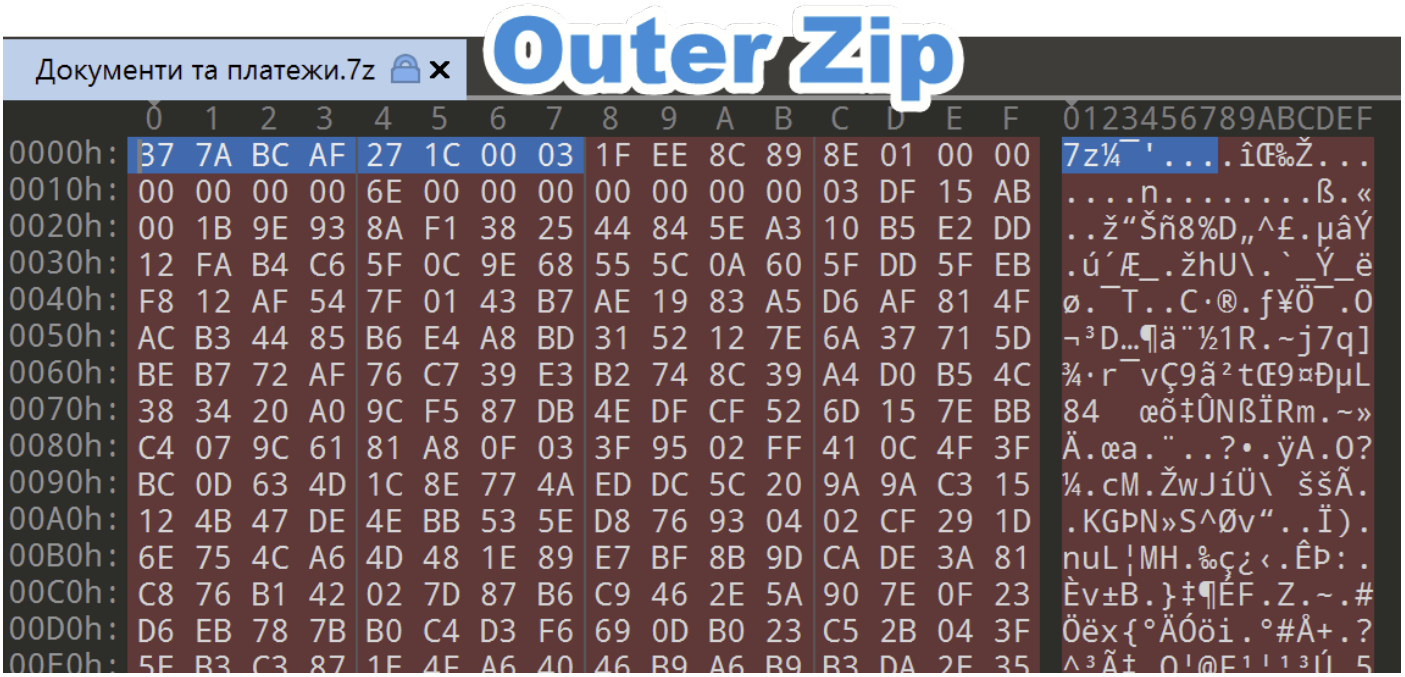
In Figure 9, the actual Microsoft login domain is depicted, with the actual Latin "C" character.

Although this domain features the TLS/SSL lock icon and the Microsoft *favicon*, these indicators alone are not always enough for verifying the domain's authenticity. A comprehensive analysis of the TLS certificate and additional technical specifics are often essential in substantiating the legitimacy of a domain. However, these technical elements can elude the average web user.

Having established an understanding of homoglyph attacks, let's return to our analysis of the in-the-wild example.

During this campaign, the threat actors implemented an additional layer of deception to manipulate users into executing the zero-day vulnerability CVE-2025-0411. By employing the Cyrillic character "Es", the attackers designed an inner archive mimicking a .doc file. This strategy effectively misleads users into inadvertently triggering the exploit for CVE-2025-0411, resulting in the contents of the archive being released without MoTW protections. Consequently, this allows for the execution of JavaScript files (.js), Windows Script Files (.wsf), and Windows Shortcut files (.url). I

Using an example from the SmokeLoader campaign, *Документи та платежи.7z* (84ab6c3e1f2dc98cf4d5b8b739237570416bb82e2edaf078e9868663553c5412), translating to "*Documents and payments*" in English, serves as the outer zip archive and *Список.doc* (7786501e3666c1a5071c9c5e5a019e2bc86a1f169d469cc4bfef2fe339aaf384), translated to "*List*", serves as the inner archive. This uses a homoglyph attack where the "c" in the ".doc" extension is a Cyrillic "Es" character.



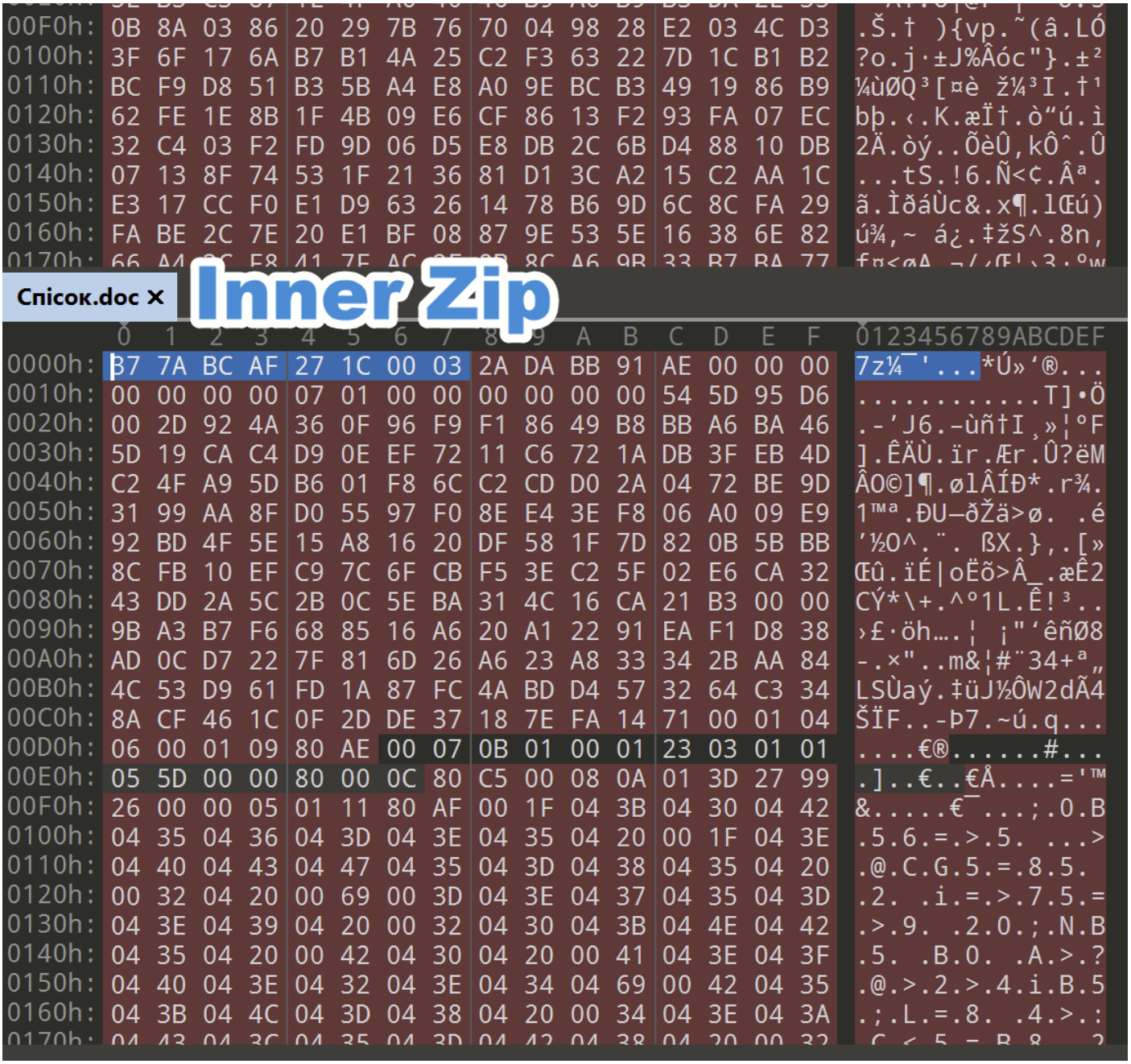
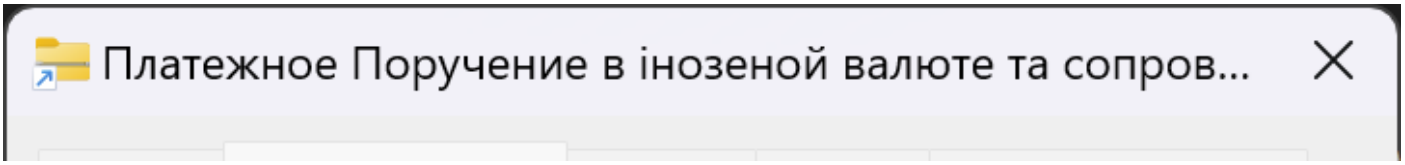


Figure 10. Hex Comparison between Документи та платежи.7z (outer archive) and Список.doc (homoglyph attack and inner archive)

In Figure 10, we can see a side-by-side comparison of both outer and inner zip archives (which contain the 7-Zip magic bytes *\x37\x7A\xBC\xAF\x27\x1C*). It is important to note that even though both archives happen to be 7-Zip archives, it does not matter what archive format is used when it comes to the exploitation of CVE-2025-0411.

Inside Список.doc, the .url file *Платежное Поручение в іноземной валюте та сопроводітельни документи від 23.09.2024р.url* (2e33c2010f95cbda8bf0817f1b5c69b51c860c536064182b67261f695f54e1d5) points to an attacker-controlled server hosting another ZIP archive.



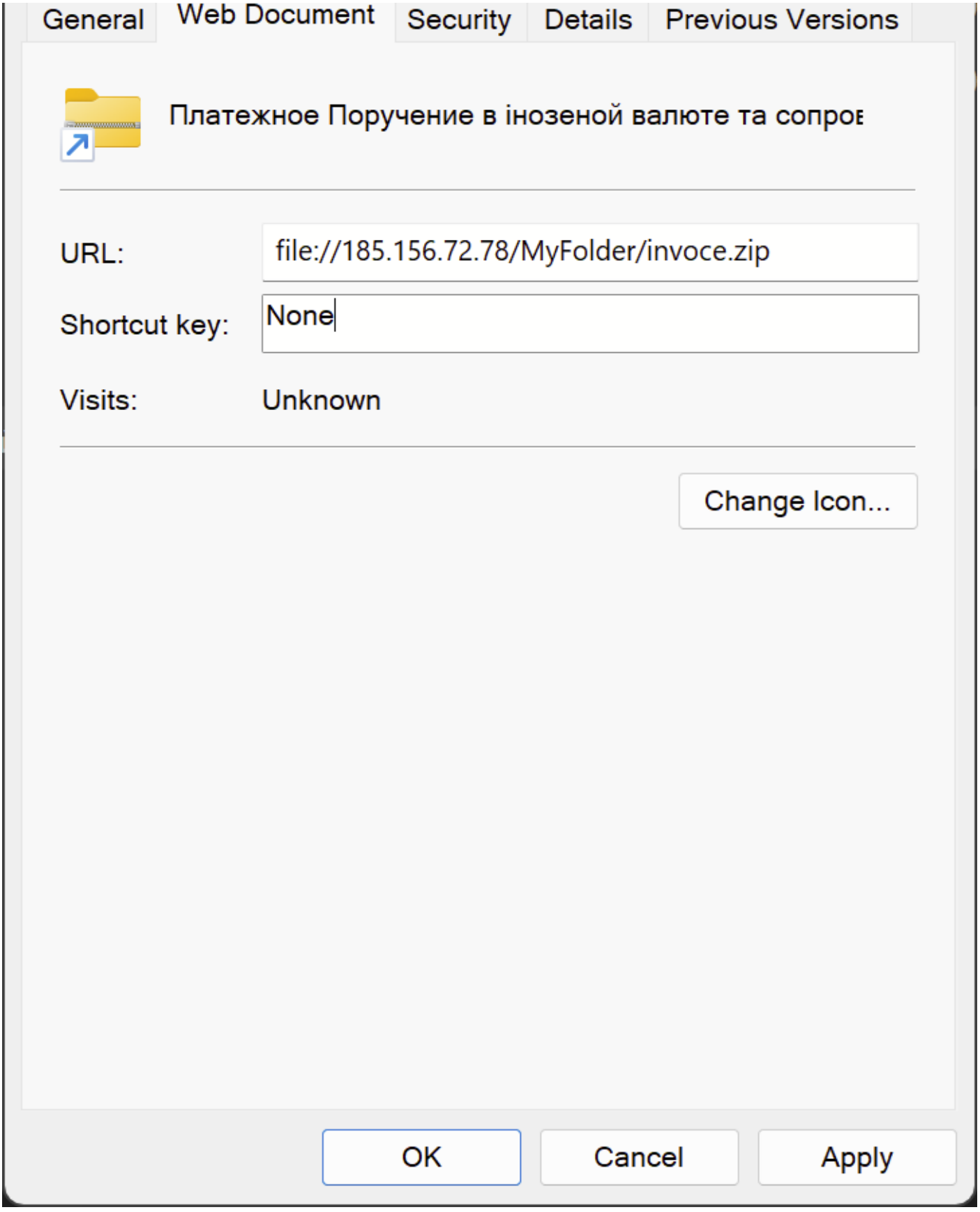
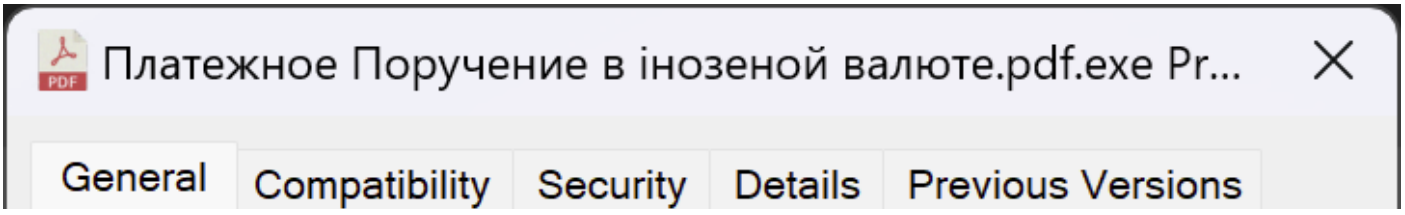


Figure 11. File properties of Платежное Поручение в іноземной валюте та сопроводітельни документи від 23.09.2024p.url



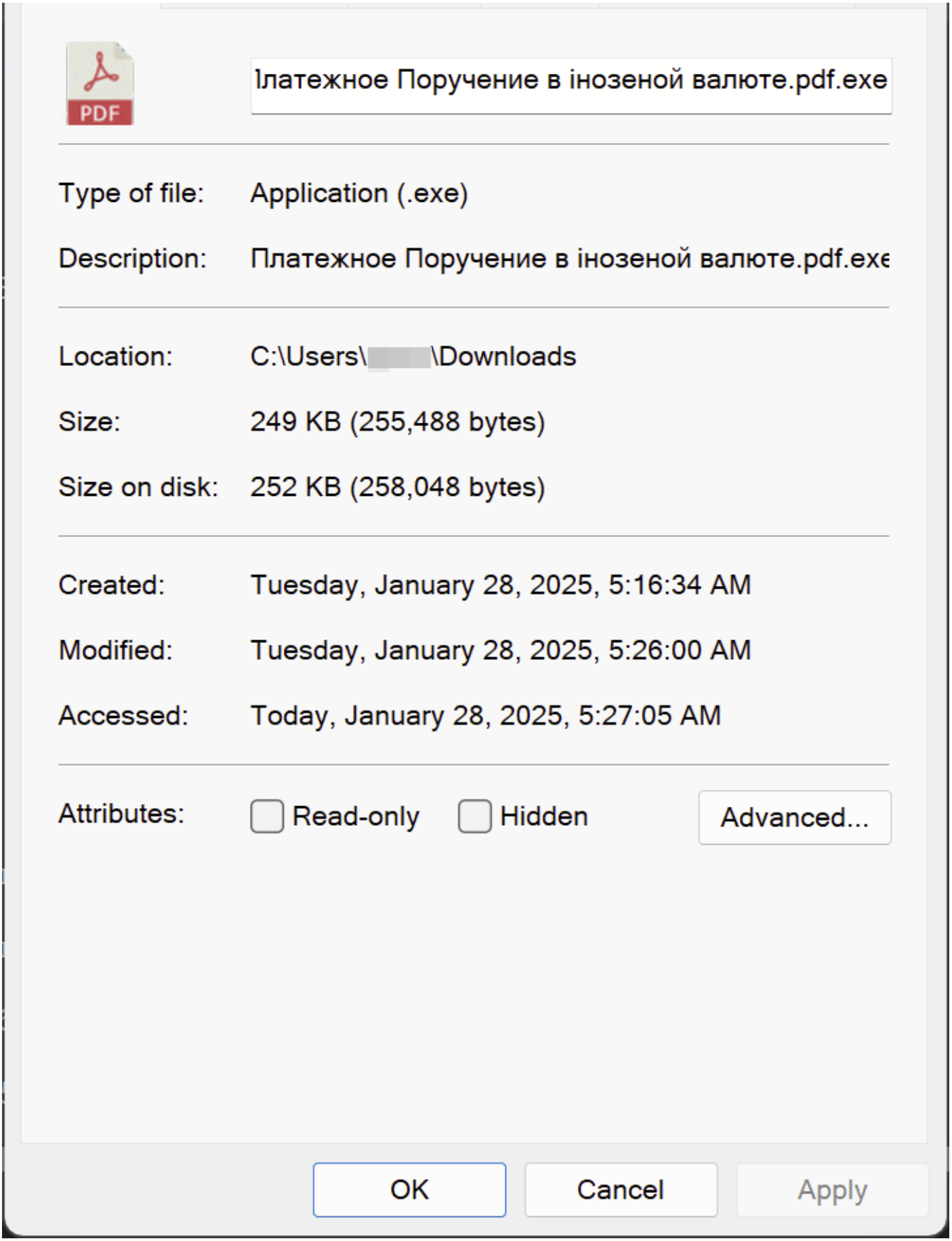


Figure 12. File properties of Платежное Поручение в иноземной валюте.pdf.exe

Once *Платежное Поручение в иноземной валюте.pdf.exe* is executed, the SmokeLoader payload is also then executed, leading to malware infection and full system compromise.

Known Ukrainian organizations affected or targeted by the zero-day exploit

Based on the data we've uncovered, the following Ukrainian government entities and other organizations may have been directly targeted and/or affected by this campaign:

State Executive Service of Ukraine (SES) – Ministry of Justice

Zaporizhzhia Automobile Building Plant (PrJSC ZAZ) – Automobile, bus, and truck manufacturer

Kyivpastrans – Kyiv Public Transportation Service

SEA Company – Appliances, electrical equipment, and electronics manufacturer

Verkhovyna District State Administration - Ivano-Frankivsk oblast administration

VUSA – Insurance company

Dnipro City Regional Pharmacy – Regional pharmacy

Kyivvodokanal – Kyiv Water Supply Company

Zalishchyky City Council – City council

Note that this compilation of organizations impacted by the CVE-2025-0411 zero-day attack is not comprehensive; there is a significant likelihood that additional organizations may have been affected or targeted by the perpetrators.

It appears that some of the compromised email accounts may have been acquired from prior campaigns, and it is possible that newly compromised accounts will be incorporated into future operations. The use of these compromised email accounts lend an air of authenticity to the emails sent to targets, manipulating potential victims into trusting the content and their senders.

One interesting takeaway we noticed in the organizations targeted and affected in this campaign is smaller local government bodies. These organizations are often under intense cyber pressure yet are often overlooked, less cyber-savvy, and lack the resources for a comprehensive cyber strategy that larger government organizations have. These smaller organizations can be valuable pivot points by threat actors to pivot to larger government organizations.

Recommendations

To minimize the risks associated with CVE-2025-0411 and similar vulnerabilities, we recommend that organizations adhere to the following best practices:

Ensure that all instances of 7-Zip are updated to version 24.09 or later. This version addresses the CVE-2025-0411 vulnerability.

Implement strict email security measures, including the use of email filtering and anti-spam technologies to detect and block spear-phishing attacks.

Train employees to recognize and report phishing attempts. Regularly update them on the latest phishing tactics, including homoglyph attacks on files and filetypes, as discussed in this entry.

Educate users on zero-day and n-day vulnerabilities and their role in preventing their exploitation.

Educate users on the importance of MoTW and its role in preventing the automatic execution of potentially harmful scripts or applications.

Disable the automatic execution of files from untrusted sources and configure systems to prompt users for verification before opening such files.

·Implement domain filtering and monitoring to detect and block homoglyph-based phishing attacks.

Use URL filtering to block access to known malicious domains and regularly update blacklists with newly identified threat domains.

Trend Vision One™

Trend Vision One™ is a cybersecurity platform that simplifies security and helps enterprises detect and stop threats faster by consolidating multiple security capabilities, enabling greater command of the enterprise's attack surface, and providing complete visibility into its cyber risk posture. The cloud-based platform leverages AI and threat intelligence from 250 million sensors and 16 threat research centers around the globe to provide comprehensive risk insights, earlier threat detection, and automated risk and threat response options in a single solution.

Trend Vision One Threat Intelligence

To stay ahead of evolving threats, Trend Vision One customers can access a range of Intelligence Reports and Threat Insights within Vision One. Threat Insights helps customers stay ahead of cyber threats before they happen and allows them to prepare for emerging threats by offering comprehensive information on threat actors, their malicious activities, and their techniques. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and effectively respond to threats.

CVE-2025-0411: Analysis of a Zero-Day Vulnerability and its Use in Cyber Espionage

Trend Vision One Threat Insights App

Emerging Threats: CVE-2025-0411: Analysis of a Zero-Day Vulnerability and its Use in Cyber Espionage

Hunting Queries

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

malName:*SMOKELOADER* AND eventName:MALWARE_DETECTION AND LogType: detection

More hunting queries are available for Trend Vision One customers with Threat Insights Entitlement enabled.

Conclusion

It is important that everyone using 7-Zip update to 7-Zip version 24.09 immediately, especially since CVE-2025-0411 has been under active exploitation since at least September 2024, with PoC concepts existing as well.

The exploitation of CVE-2025-0411 signifies another instance of a zero-day vulnerability being used in the context of the ongoing cyber front of the Russo-Ukrainian conflict. This situation illustrates the dynamic nature of the current cyber conflict, particularly the employment of advanced zero-day deployment techniques, notably through homoglyph attacks.

To the best of our knowledge, this represents the first occasion in which a homoglyph attack has been integrated into a zero-day exploit chain, thereby elevating concerns regarding the progression of such attacks beyond traditional methods such as credential harvesting, phishing, and website spoofing.

Furthermore, this campaign highlights the need for organizations to enhance their cybersecurity training programs by incorporating an understanding of homoglyph attacks, especially in relation to files, file extensions, and zero-day exploitation rather than limiting the focus to web spoofing alone. The Trend ZDI Threat Hunting team engages in proactive efforts to identify zero-day exploitation in the wild, therefore safeguarding organizations against real-world threats prior to vendor awareness.

We'll be back with more findings as we have them. Until then, you can follow the Trend ZDI team on Twitter, Mastodon, LinkedIn, or Bluesky for the latest in exploit techniques and security patches.

Indicators of Compromise

The indicators of compromise for this entry can be found here.

Tags