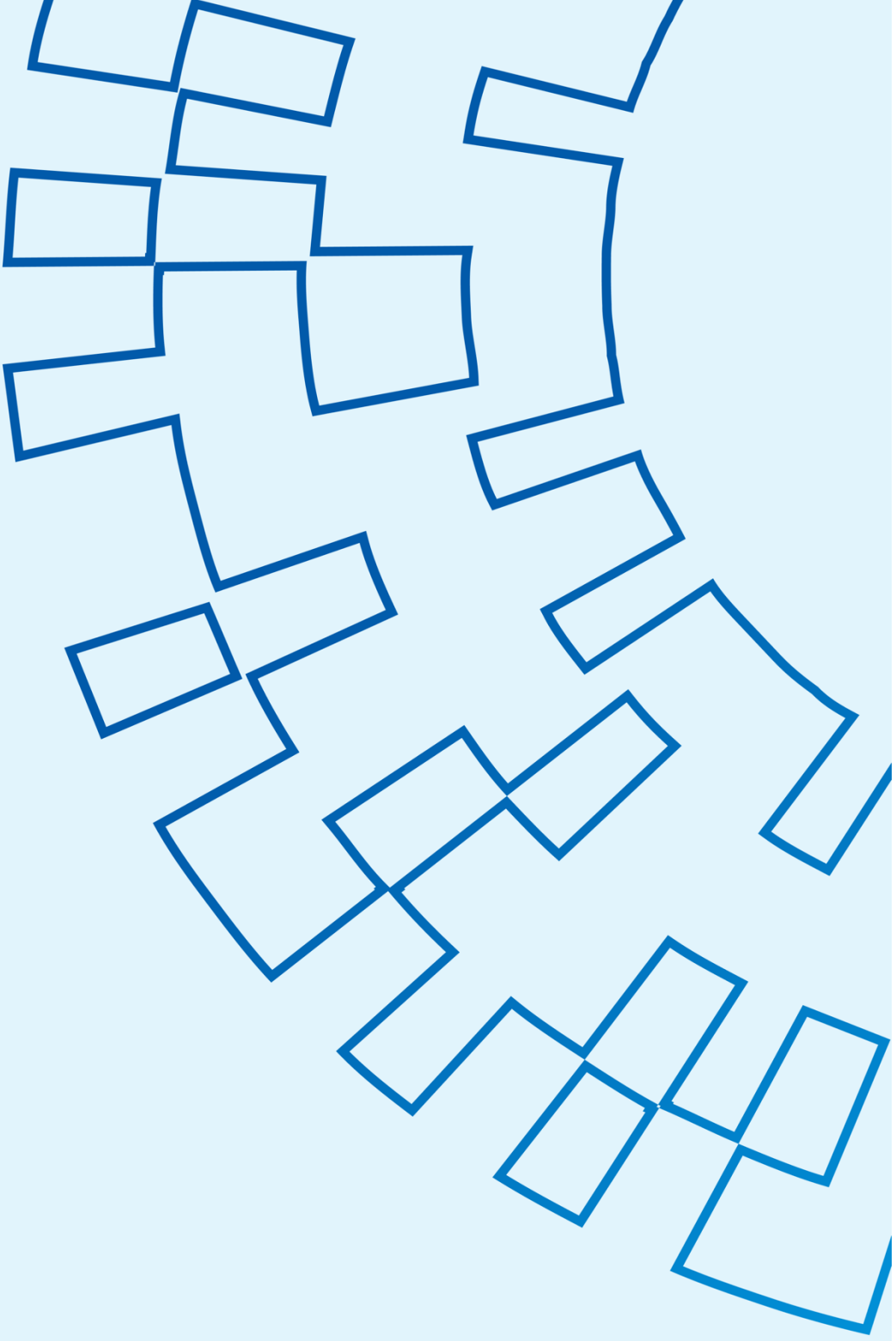
НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ



APT28 CYBERATTACKS USING THE CVE-2023-23397 VULNERABILITY

APT28 cyberattacks using the CVE-2023-23397 vulnerability

Recently, CERT-UA (Computer Emergency Response Team of Ukraine) has discovered and reported about a new critical vulnerability in the Microsoft Outlook email client, which has been assigned the identifier CVE-2023-23397. Successful exploitation of this vulnerability could lead to unauthorized access to an organization's network via Net-NTLMv2 hash leak. The vulnerability carries a great threat as it has achieved 9.8 out of 10 points of CVSS Base Score.

This vulnerability is exploited by the russian nation-state adversary group APT28, which is tightly tied to the russian military intelligence service (GRU). In its attacks, APT28 focuses on intelligence gathering and cyber espionage operations for the benefit of the russian government.

NCSCC discovered attacks conducted by APT28 with the help of CVE-2023-23397 and analyzed their targets with the overall picture of victimology and time frame of attacks. The first attempt to carry out an attack using this vulnerability was recorded in March 2022, at that time it was a zero-day vulnerability for which no patch existed.

Over the past year, more than 10 attacks on organizations in Europe and the Middle East have been recorded.

Vulnerability description

To exploit CVE-2023-23397 attacker must deliver a specially crafted message to the victim in the Microsoft Outlook email client. Such message contains a PidLidReminderFileParameter property that is set to a shared UNC path to the attacker's server, resulting in a Net-NTLMv2 hash leak.

No user interaction is required to exploit the vulnerability.

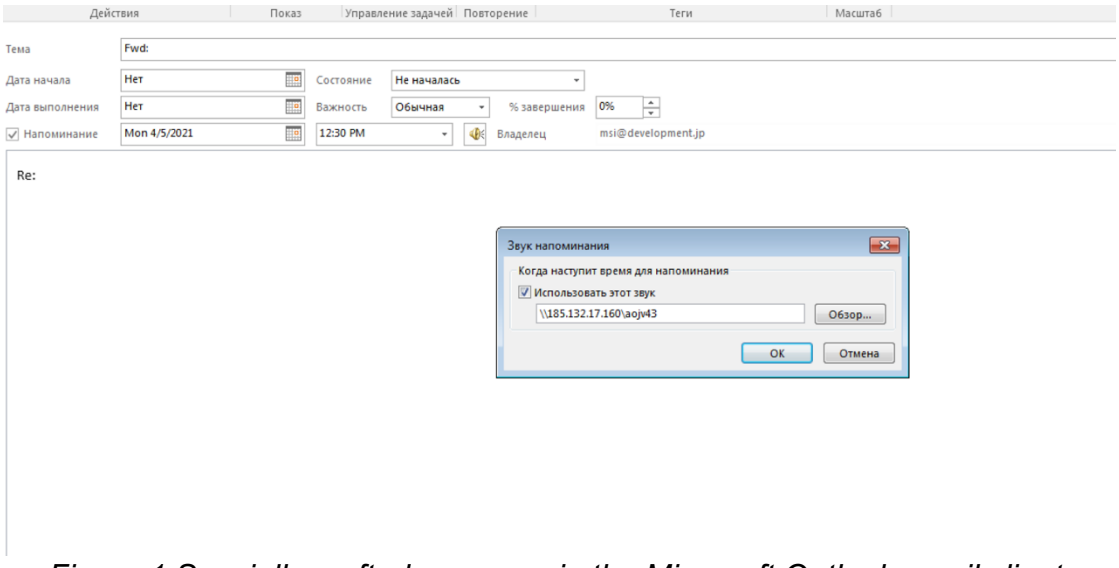


Figure.1 Specially crafted message in the Microsoft Outlook email client.

The user does not need to interact with the message: the vulnerability is triggered when a reminder is executed in an open Outlook client. When connecting to a remote SMB server, the user's Net-NTLMv2 hash is sent, which attacker can then use to authenticate to other systems that support NTLM authentication, including Exchange Server.

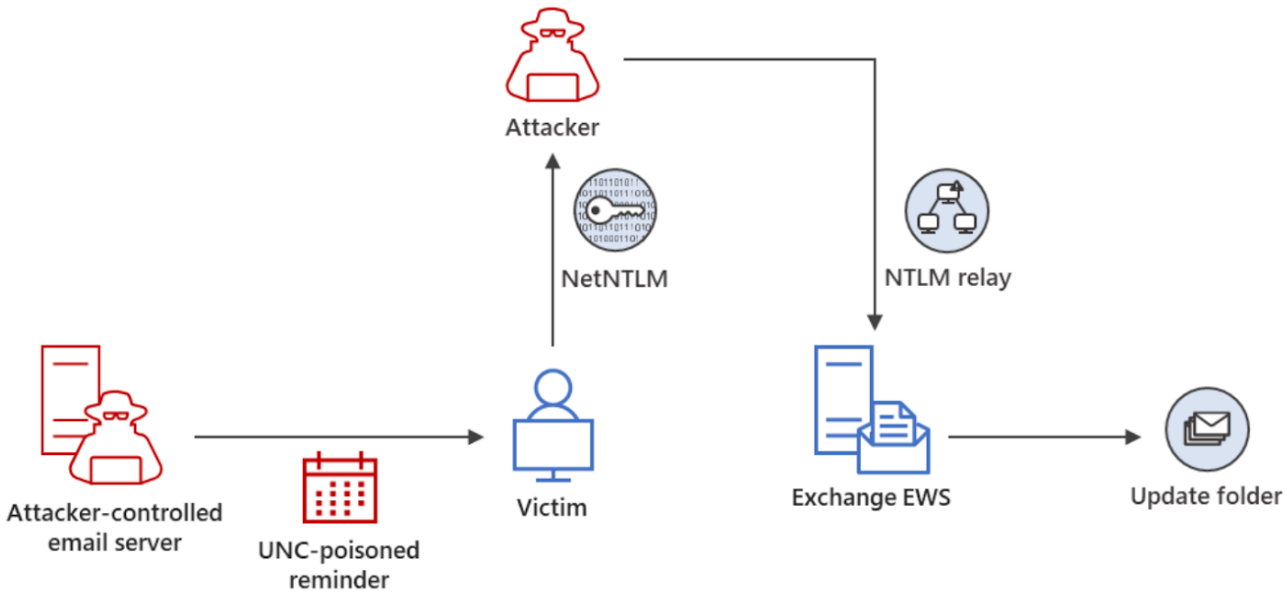


Figure.2 Exploitation of CVE-2023-23397 to gain unauthorized access to Exchange Server (Source: Microsoft)

APT28 attacks

The APT28 group dates back to 2007 and is primarily focused on stealing sensitive information related to governments, the military, and security organizations. In their latest attacks exploiting the CVE-2023-23397 vulnerability, hackers targeted businesses and organizations in Europe and the Middle East, including gas transmission system operators, private satellite intelligence and radar companies, foreign affairs entities and NATO agencies, and IT solution developers and vendors.

Assessing the selection of organizations that have been targeted in attacks over the past year, it can be argued that russian intelligence and government are focused on military satellite intelligence and radar technologies, collecting information through diplomatic missions of Ukraine's neighboring countries on arms supplies, penetrating the gas transmission system operators to commit sabotage, and penetrating the systems of IT solution developers for further spreading among customers at the supply chain level.

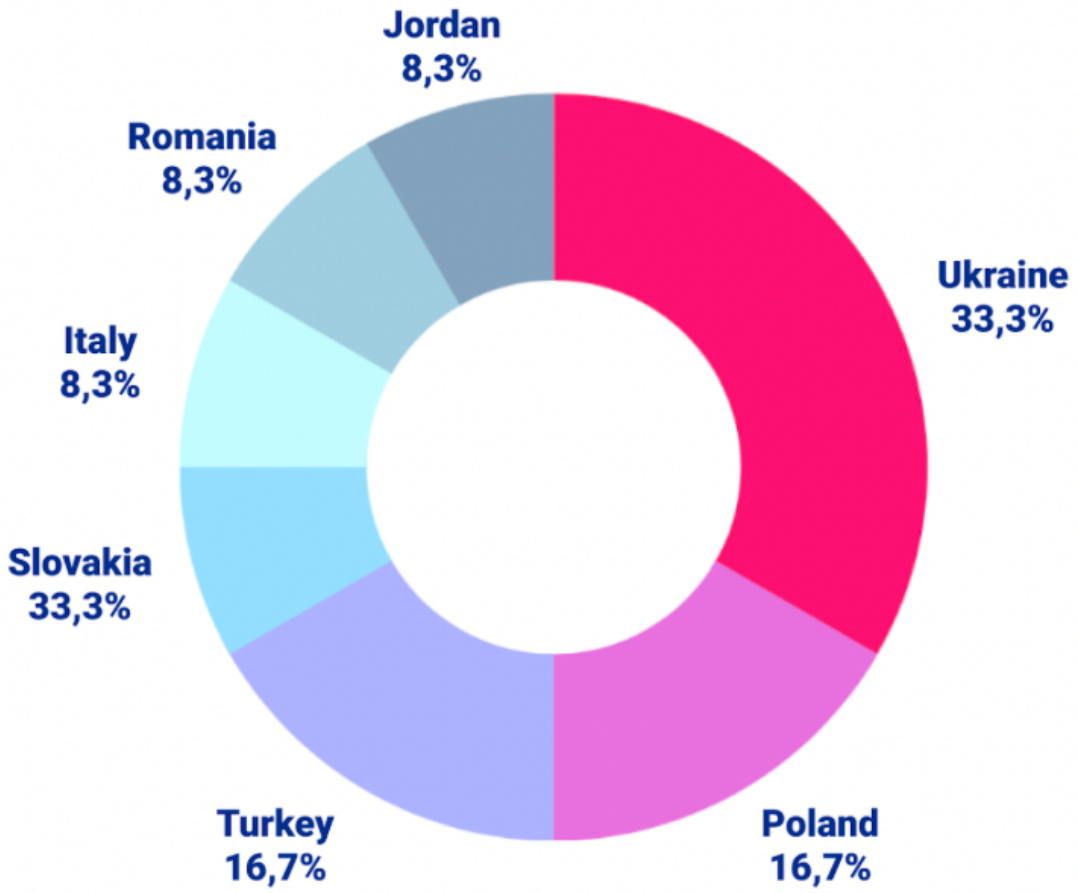


Figure.3 Targets attacked with CVE-2023-23397 by countries.

The first attack was detected in March 2022 after the full-scale invasion had begun. It was only after it became clear that the military invasion had failed that APT28 hackers began to act and exploit the CVE-2023-23397 vulnerability, which they obviously prepared in advance, as researching and identifying such a vulnerability and developing an exploit for it requires significant resources and time. Another confirmation that these attacks were carried out by the same group is the reuse of some IP addresses and email addresses in different attacks.

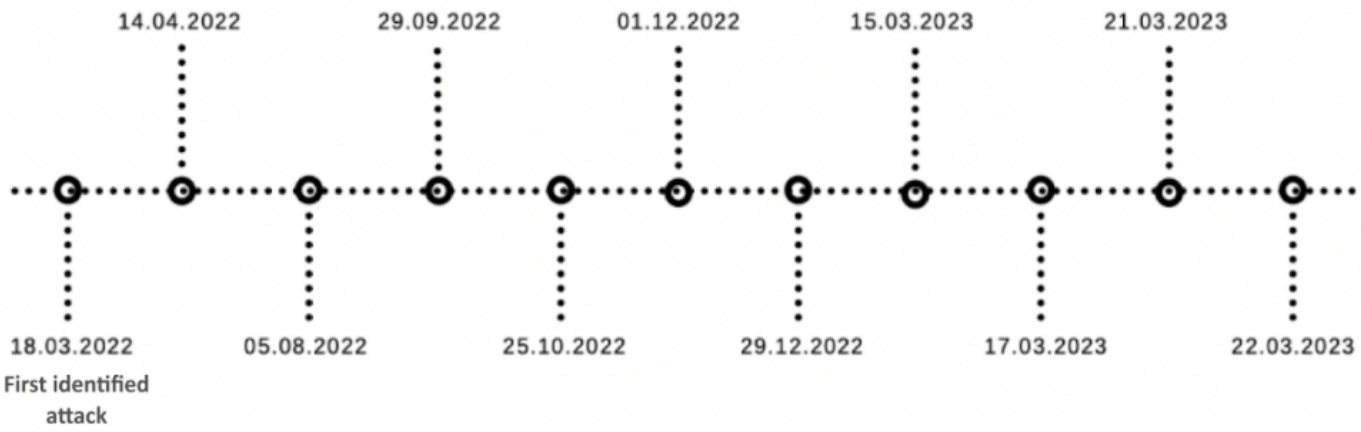


Figure.4 Time frame of attacks

It is expected that after the vulnerability description is published, it will be actively used by other hacker groups due to its ease of use and effectiveness. The PoC exploit samples for the CVE-2023-23397 vulnerability are already freely available online.

Recommendations on how to detect exploitation attempts and patch the vulnerability are available on the official resources of the State Service of Special Communications and Information Protection of Ukraine [1] and Microsoft [2].

1. https://cip.gov.ua/ua/news/dodatkovi-rekomendaciyi-shodo-viyavlennya-sprob-ekspluataciyi-ta-usunennya-vrazlivosti-ms-outlook-cve-2023-23397
2. https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/

Indicators of compromise

FILE:

Letter: 2022-03-18 - лист.eml
MD5: 9f4172d554bb9056c8ba28e32c606b1e
Attachment: winmail.dat
MD5: 0658f137afa793b361ec93c462cbf41b

Letter: Silence..eml
MD5: e6efaabb01e028ef61876dd129e66bac
Attachment: Text.txt
MD5: 7b69acfdd6523394a4fc28d54aa3e839

Letter: fecyxb602692907076.eml
MD5: c221547f440e600473ea378c692dcc44
Attachment: winmail.dat
MD5: c673416d3c155219459b4475b8e2b264

Letter: Alarm!.msg
MD5: e1c030cfc3f1a842d93c4f47b19780d7

Letter:
582442ee950d546744f2fa078adb005853a453e9c7f48c6c770e6322a888c2cf.msg
MD5: 2bb4c6b32d077c0f80cda1006da90365

Letter: emsulv926761298840.eml
MD5: 7ee19e6bd9f55ebc0dd6413c68346de6
Attachment: subj.docx
MD5: cfb590eeeff8735f31709b0348b445b2

Letter: 1peZvV-0009KN-AL.eml
MD5: 3b698278f225f1e5bace9d177a1a95e0
Attachment: winmail.dat
MD5: c673416d3c155219459b4475b8e2b264

Letter:
eedae202980c05697a21a5c995d43e1905c4b25f8ca2fff0c34036bc4fd321fa_happy_birthday.msg
MD5: 3d4362e8fe86d2f33acb3e15f1dad341

Letter: Information.msg
MD5: 43a0441b35b3db061cde412541f4d1e1

Letter: Fwd_.msg
MD5: b21dde4c19e2f6fc08a922e25de38cf5

Letter: Fwd_.msg
MD5: eadb4b16755ac36aa9f4a85ebf23fd4c

Letter: Information!.msg
MD5: d0e6c5c888ff0baa7db12c776617112d

NETWORK:

5.199.162.132\SCW
maint@goldenloafuae.com

213.32.252.221\silence
tv@coastalareabank.com

61.14.68.33\rem
commercial@vanadrink.com

85.195.206.7\lrmng
sarah@cosmicgold469.co.za

113.160.234.229\istanbul
jayan@wizzsolutions.com

85.195.206.7\power
commercial@vanadrink.com

61.14.68.33\rem
commercial@vanadrink.com

101.255.119.42\event\2431
accounts@regencyservice.in

168.205.200.55\test
franch1.lanka@bplanka.com

185.132.17.160\aojv43
m.salim@tsc-me.com

69.162.253.21\pets
m.salim@tsc-me.com

181.209.99.204\information

To report a cyber incident please send us an email: report@ncscc.gov.ua

The report was developed with the assistance of Institute of Cyber Warfare Research