НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

КІБЕРАТАКИ ХАКЕРСЬКОГО УГРУПОВАННЯ APT28 З ВИКОРИСТАННЯМ ВРАЗЛИВОСТІ CVE-2023-23397

Атаки угруповання APT28 з використанням CVE-2023-23397

Нещодавно Урядова команда реагування CERT-UA виявила та повідомила про нову критичну вразливість у поштовому клієнті Microsoft Outlook, якій було присвоєно ідентифікатор CVE-2023-23397. Успішна експлуатація цієї вразливості може призвести до несанкціонованого доступу до мережі організації через витік хешу Net-NTLMv2. За стандартом CVSS вразливість отримала високу оцінку – 9,8 із 10 балів.

Експлуатацію цієї вразливості здійснює російське угруповання APT28, яке пов'язане з ГРУ ГШ рф. У своїх атаках, APT28 фокусується на зборі розвідданих та операціях кібершпигунства в інтересах російського уряду.

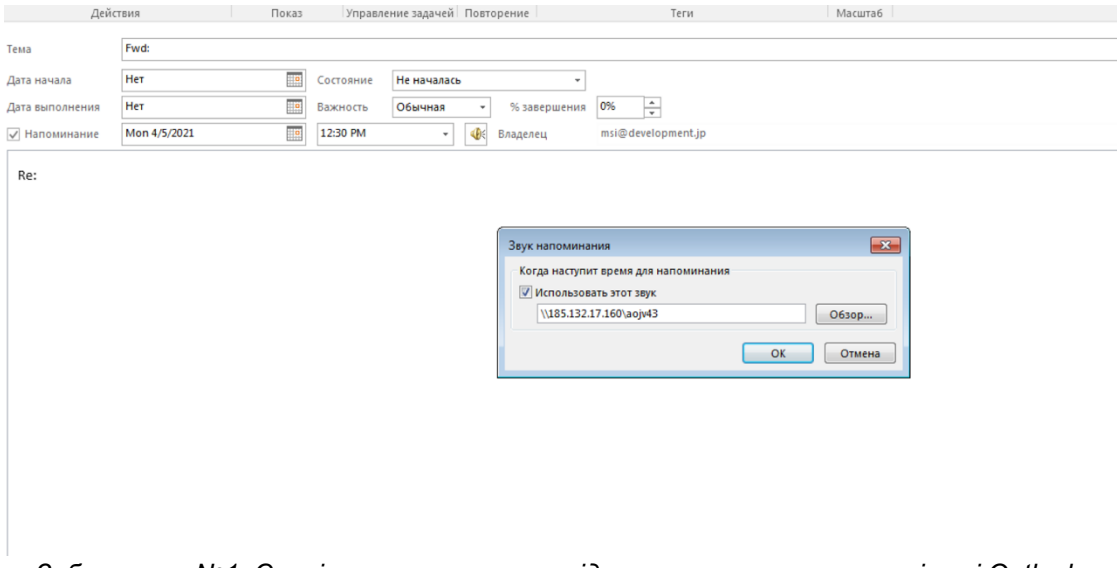
Перша спроба здійснення атаки з використанням даної вразливості була зафіксована у березні 2022 року, на той час це була так звана вразливість нульового дня, тобто для неї не існувало виправлення.

За останній рік було зафіксовано низку атак на підприємства та організації країн Європи та Близького Сходу.

Опис вразливості

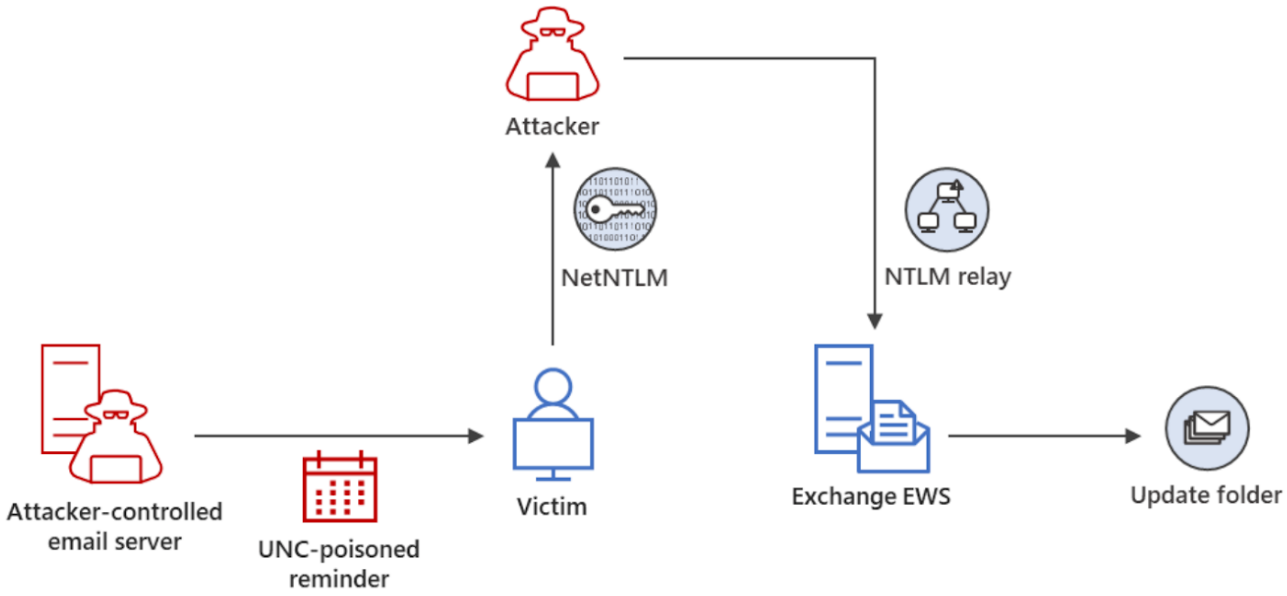
Для експлуатації CVE-2023-23397 зловмисник повинен доставити жертві спеціально підготовлене повідомлення у поштовому клієнті Microsoft Outlook. Таке повідомлення містить параметр PidLidReminderFileParameter, для якого встановлено спільний UNC шлях до сервера зловмисника, що призводить до витоку хешу Net-NTLMv2.

Для експлуатації вразливості не потрібна жодна взаємодія з користувачем.



Зображення №1. Спеціально створене повідомлення у поштовому клієнті Outlook.

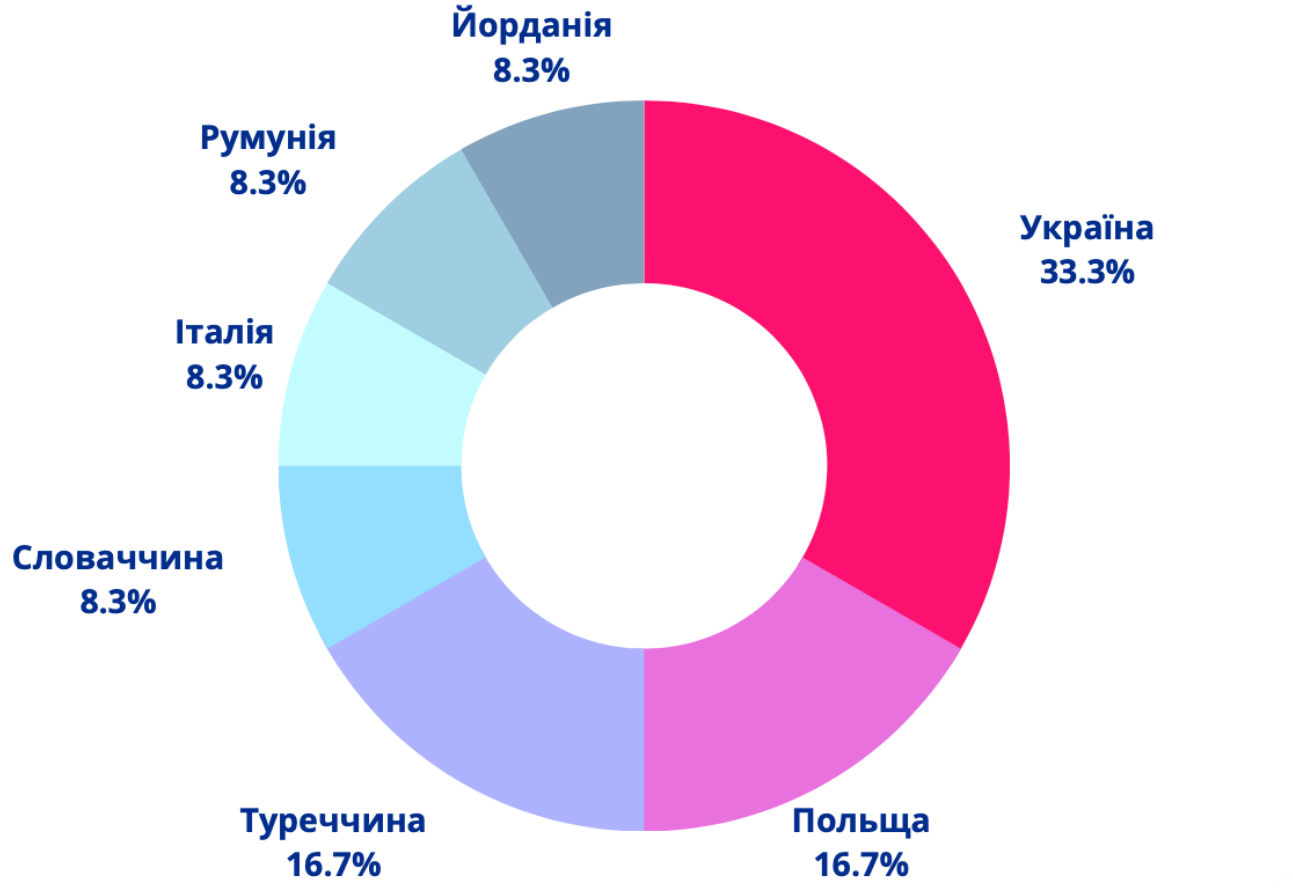
Користувачеві не потрібно взаємодіяти з повідомленням: вразливість спрацьовує, коли виконується нагадування у відкритому клієнті Outlook. При з'єднанні з віддаленим сервером SMB надсилається Net-NTLMv2 хеш користувача, який зловмисник може потім використати для автентифікації в інших системах, які підтримують автентифікацію NTLM, в тому числі Exchange Server.



Зображення №2. Експлуатація CVE-2023-23397 для отримання несанкціонованого доступу до Exchange Server (Джерело: Microsoft)

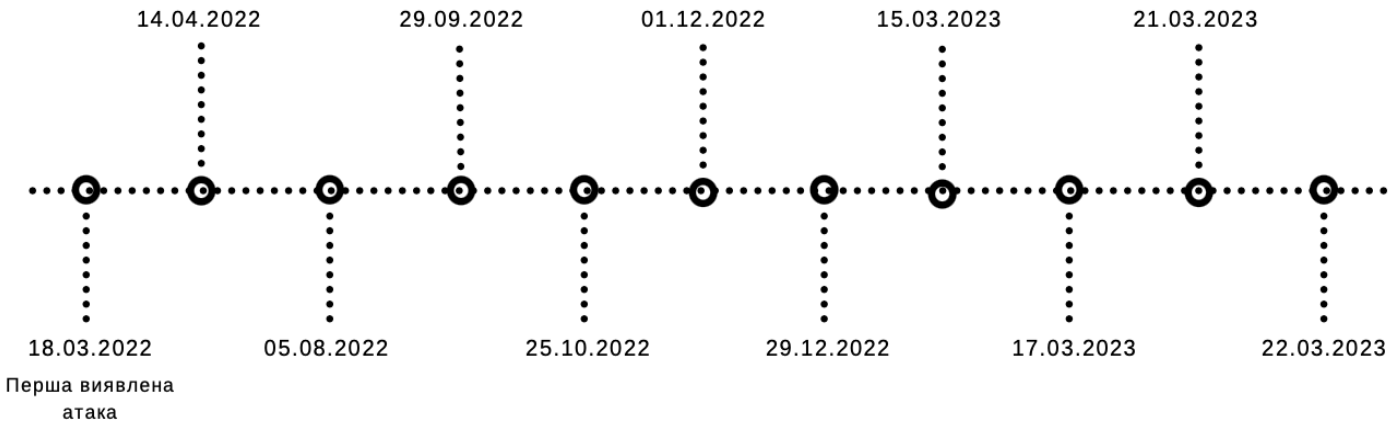
Атаки угруповання APT28

Діяльність угруповання APT28 бере початок у 2007 році та в основному націлена на викрадення конфіденційної інформації, пов'язаної з урядами, армією та організаціями у сфері безпеки. У своїх останніх атаках з використанням вразливості CVE-2023-23397 хакери націлювались на підприємства та організації країн Європи та Близького Сходу, серед яких є оператори газотранспортних систем, приватні підприємства супутникової розвідки та систем радіолокації, установи МЗС та НАТО, компанії розробники та постачальники IT-рішень.



Зображення №3. Цілі, які були атаковані з використанням CVE-2023-23397, по країнам

Перша атака була виявлена у березні 2022 року після початку повномасштабного вторгнення рф в Україну. Тільки після того, як стало зрозуміло, що військове вторгнення зазнало провалу, хакери APT28 почали діяти та використовувати вразливість CVE-2023-23397, яку вони очевидно підготували завчасно. Адже дослідження та виявлення такої вразливості та розробка експлоїту для неї потребує значних ресурсів та часу. Також підтвердженням того, що ці атаки здійснювались одним угрупованням, є повторне використання деяких IP-адрес та поштових адрес при різних атаках.



Зображення №4. Часові рамки атак

Очікується, що після публікації опису вразливості вона буде активно використовуватись іншими хакерськими угрупованнями, через легкість використання та ефективність. В мережі у вільному доступі вже є зразки PoC експлойту для вразливості CVE-2023-23397.

Рекомендації щодо виявлення спроб експлуатації та усунення вразливості є на офіційних ресурсах Держспецзв'язку [1] та Microsoft [2].

Також, наведені нижче індикатори компрометації ви можете знайти на платформі обміну інформацією про кіберзагрози NCSCC-UA MISP.

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/

Індикатори компрометації

ФАЙЛОВІ:

Лист: 2022-03-18 - лист.eml
MD5: 9f4172d554bb9056c8ba28e32c606b1e
Додаток: winmail.dat
MD5: 0658f137afa793b361ec93c462cbf41b

Лист: Silence..eml
MD5: e6efaabb01e028ef61876dd129e66bac
Додаток: Text.txt
MD5: 7b69acfdd6523394a4fc28d54aa3e839

Лист: fecyxb602692907076.eml
MD5: c221547f440e600473ea378c692dcc44
Додаток: winmail.dat
MD5: c673416d3c155219459b4475b8e2b264

Лист: Alarm!.msg
MD5: e1c030cfc3f1a842d93c4f47b19780d7

Лист:
582442ee950d546744f2fa078adb005853a453e9c7f48c6c770e6322a888c2cf.msg
MD5: 2bb4c6b32d077c0f80cda1006da90365

Лист: emsulv926761298840.eml
MD5: 7ee19e6bd9f55ebc0dd6413c68346de6
Додаток: subj.docx
MD5: cfb590eeeff8735f31709b0348b445b2

Лист: 1peZvV-0009KN-AL.eml
MD5: 3b698278f225f1e5bace9d177a1a95e0
Додаток: winmail.dat
MD5: c673416d3c155219459b4475b8e2b264

Лист:
eedae202980c05697a21a5c995d43e1905c4b25f8ca2fff0c34036bc4fd321fa_happy_birthday.msg
MD5: 3d4362e8fe86d2f33acb3e15f1dad341

Лист: Information.msg
MD5: 43a0441b35b3db061cde412541f4d1e1

Лист: Fwd_.msg
MD5: b21dde4c19e2f6fc08a922e25de38cf5

Лист: Fwd_.msg
MD5: eadb4b16755ac36aa9f4a85ebf23fd4c

Лист: Information!.msg
MD5: d0e6c5c888ff0baa7db12c776617112d

Мережеві:

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

Для того, щоб повідомити про кіберінцидент, пишіть нам на електронну адресу: report@ncscc.gov.ua

Звіт розроблено за сприяння Інституту дослідження кібервійни (Institute of Cyber Warfare Research)