Detecting malicious activity against Microsoft Exchange servers

Summary:

The Polish Cyber Command, as part of its activities in cyberspace, has observed the use of technique[1] that involved the modification of permissions to mailbox folders within Microsoft Exchange servers. It allows an attacker to provide covert, unauthorized access to email correspondence and was used after gaining access to email accounts through CVE-2023-23397 (Microsoft Outlook Vulnerability) or password-spraying. Activities using CVE-2023-23397 were first discovered by CERT-UA[2] and publicly described by Microsoft[3]. In the case of actions taken against entities in Poland, this was reported by CSIRT NASK[4]. As a result of the analyses carried out by POL Cyber Command, malicious actions against public and private entities in Poland were confirmed.

In order to identify and mitigate this threat, POL Cyber Command has developed a set of tools that can be run in Microsoft Exchange email environment. In the present case, within the framework of the National Cybersecurity System, actions were conducted in collaboration with CSIRT MON, CSIRT GOV, CSIRT NASK, Military Counterintelligence Service and with the support of Microsoft. Nevertheless, POL Cyber Command assesses that at the time of report publication, this technique is actively used by the adversary. POL Cyber Command recommends the use of developed tools for identifying activities within one's own resources.

Activities observed by POL Cyber Command associated with the exploitation of the CVE-2023-23397 vulnerability and a widespread campaign where the adversary uses password-spraying technique overlap with the actions described by USA and British government[5] entities and the Microsoft[6] company as related to the activity groups "APT28" and "Forrest Blizzard".

Description:

The first stage of the adversary's actions is to gain access to the mailbox. The malicious activity observed so far consists of bruteforce[1] attacks. Another observed vector for gaining access to mailboxes is the exploitation of the CVE-2023-23397[2] vulnerability, which allows the theft of a user's NTLM hash.

In the next stage of malicious activity, the adversary modifies folder permissions within the victim's mailbox[3]. In most cases, the modifications are to change the default permissions of the "Default" group (all authenticated users in the Exchange organization) from "None" to "Owner". By making this type of modification, the contents of folders that have been granted this permission can be read by any authenticated person within the organization[4]. In the default configuration, the folder permissions in mailboxes are set to "None" for the "Default" and "Anonymous" user groups, as shown in the figure below (Fig. 1). The exception is the Calendar folder, which default permission level allows to read only whether the user has a busy or free appointment in the calendar – "AvailabilityOnly, Free/Busy Time".

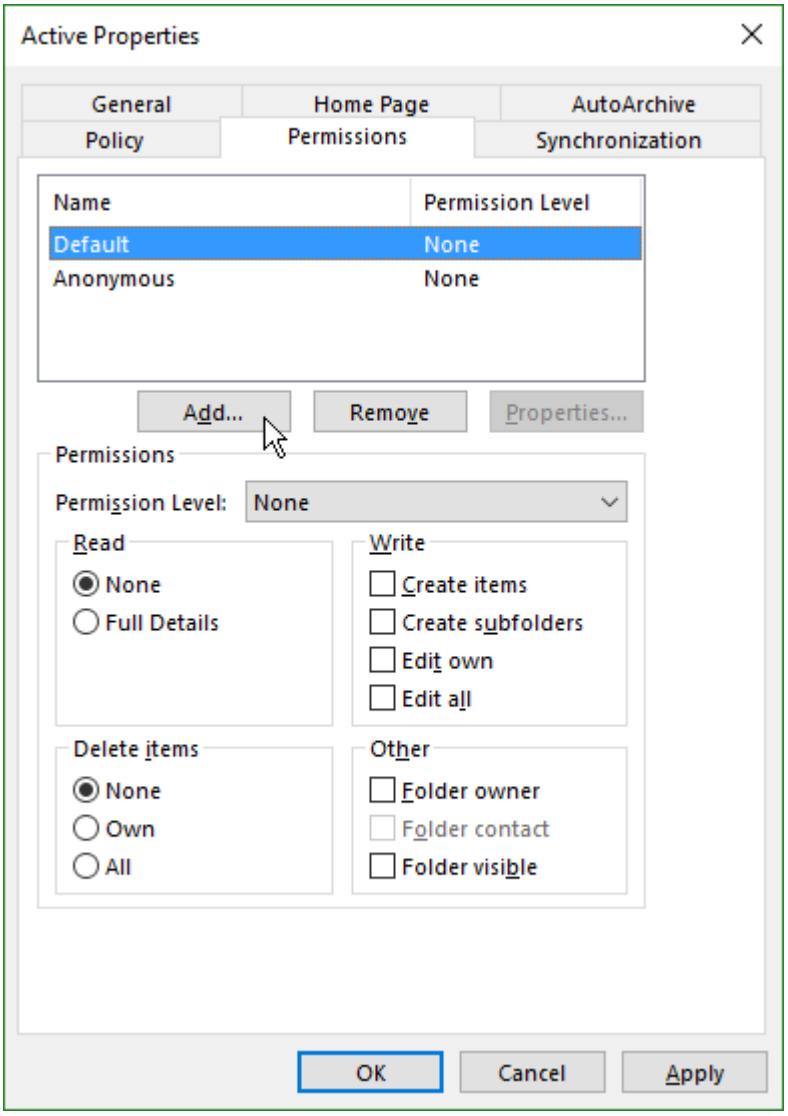

Figure 1 Default permission level settings for a folder in MS Exchange mailbox.

In cases identified by POL Cyber Command, folders permissions were modified, among others, in mailboxes that were high-value information targets for the adversary. As a result of this change, the adversary was able to gain unauthorized access to the resources of high-value informational mailboxes through any compromised email account in the Exchange organization, using the Exchange Web Services (EWS) protocol. It should be emphasized that the introduction of such modifications allows for the maintenance of unauthorized access to the contents of the mailbox even after losing direct access to it. Figure 2 presents a diagrammatic view of the described process.

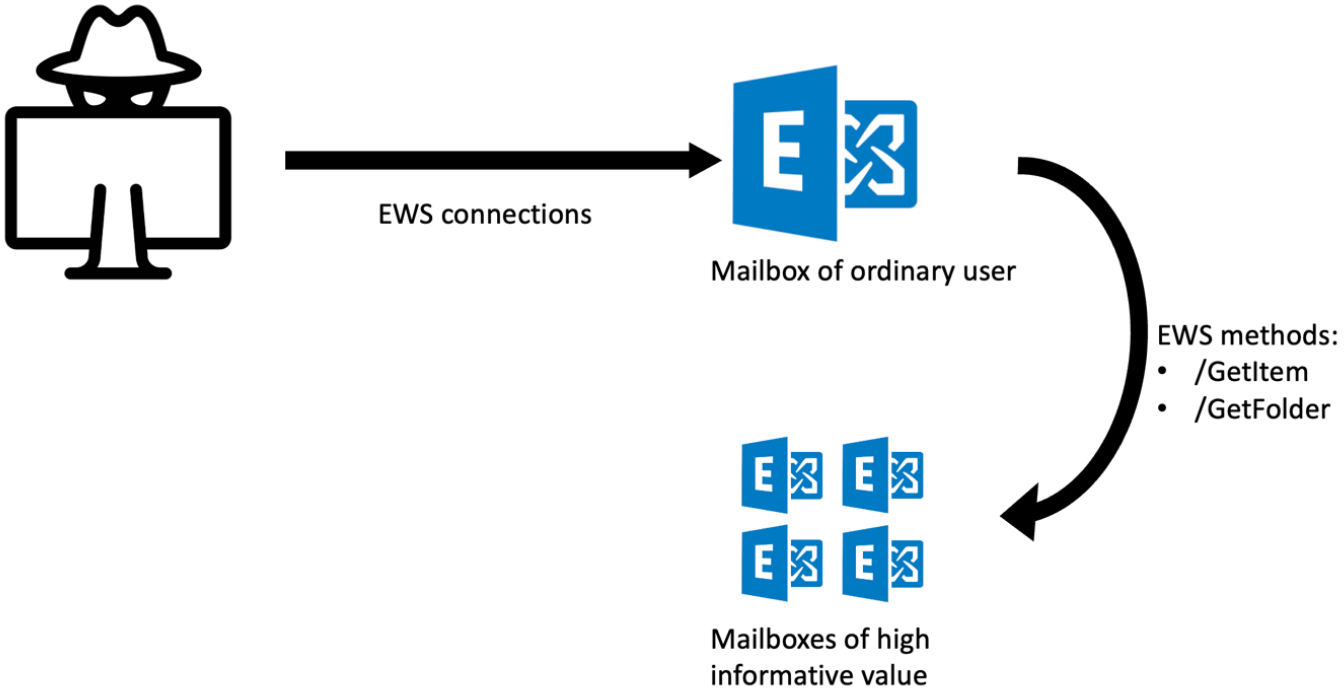

Figure 2 The process of reading and exfiltration of the contents of high informational value mailboxes via the mailbox of any authenticated user.

Another indicator that can be used to detect malicious activity is when and how permissions are modified. A characteristic feature of the described activity is the modification of permissions to all folders within the mailbox in a relatively short time (a few seconds), which physically excludes the possibility of making these changes manually by the user. An example of modifying the permissions of all mailbox folders is shown in Fig. 3. At the same time, it should be emphasized that any unusual modifications to folder permissions may indicate malicious activity.

Mailbox Owner	Folder	Path	Date of Modification	Group	Permission Level
<redacted>	Top of Information Store	\	28/03/2022 13:11:00	Default	Owner
<redacted>	Archive	\Archive	28/03/2022 13:11:01	Default	Owner
<redacted>	Synchronization errors	\Synchronization errors	28/03/2022 13:11:02	Default	Owner
<redacted>	Local failures	\Synchronization errors\Local failures	28/03/2022 13:11:04	Default	Owner
<redacted>	Server failures	\Synchronization errors\Server failures	28/03/2022 13:11:05	Default	Owner
<redacted>	Conflicts	\Synchronization errors\Conflicts	28/03/2022 13:11:06	Default	Owner
<redacted>	Conversation Action Settings	\Conversation Action Settings	28/03/2022 13:11:07	Default	Owner
<redacted>	Deleted Items	\Deleted Items	28/03/2022 13:11:15	Default	Owner
<redacted>	Drafts	\Drafts	28/03/2022 13:11:16	Default	Owner
<redacted>	Files	\Files	28/03/2022 13:11:20	Default	Owner
<redacted>	Conversation History	\Conversation History	28/03/2022 13:11:22	Default	Owner
<redacted>	Inbox	\Inbox	16/09/2023 12:59:21	Default	Owner
<redacted>	Journal	\Journal	28/03/2022 13:11:25	Default	Owner
<redacted>	Junk	\Junk	28/03/2022 13:11:26	Default	Owner
<redacted>	Notes	\Notes	28/03/2022 13:11:27	Default	Owner
<redacted>	Outboox	\Outboox	28/03/2022 13:11:28	Default	Owner
<redacted>	Sent Items	\Sent Items	28/03/2022 13:11:30	Default	Owner
<redacted>	To-do	\To-do	28/03/2022 13:11:33	Default	Owner

Figure 3 An example of a script developed by POL Cyber Command showing the modified permissions.

The above actions, in POL Cyber Command assessment, indicate a high level of adversary sophistication and thorough knowledge of the architecture and mechanisms of the Microsoft Exchange mail system. Identification of this type of attack is challenging due to the intentional avoidance of using any offensive

tools that could be detected by cybersecurity systems. Building a custom detection requires the analysis of event logs, which are saved by default on mail servers.

Among the attacker's OPSEC (Operations Security) measures, it can be noted that they utilize commercial services of VPN, which geolocation indicates the territory of Poland, as well as the addresses of local Internet service providers. This allows the attacker to partially blend into trusted network traffic. In addition, in the cases analysed by POL Cyber Command , it was found that different IP addresses were used against different targets.

POL Cyber Command assesses that the technique in question (MITRE ATT&CK – T1098.002) could have been used against a number of domestic and foreign entities, both government and private sector, with particular emphasis on those targeted in the Silence campaign and related to the compromise of Microsoft Exchange mail servers.

Recommendations:

POL Cyber Command recommends the implementation of the following guidelines. In case of detecting any concerning permission modifications, POL Cyber Command advises contacting the relevant national-level CSIRT team.

1. Running the toolkit provided by POL Cyber Command and implementation of countermeasures as instructed. Tools and instructions can be found in the ZIP attachment.

2. Implementing mechanisms to detect connections to a mailbox that shares folders with another mailbox based on event logs from the location:

    a. %ExchangeInstallPath%Logging\HttpProxy\Ews\

    b. %ExchangeInstallPath%Logging\Ews\

    c. %ExchangeInstallPath%logging\Mapihttp\Mailbox\

3. Verification of accounts that are assigned the ApplicationImpersonation role[11].
4. Verification of mailbox delegation settings in the entire Exchange organization.

Attachment:

[4] MITRE ATT&CK classified and described this technique as T1098.002.

[7] Especially password spraying

[9] At the moment, it has been identified that the described activity pertains to mailboxes within Microsoft Exchange server environments.

[10] The default security policies allow the user to make such modifications within their mailbox.