Dangerous events

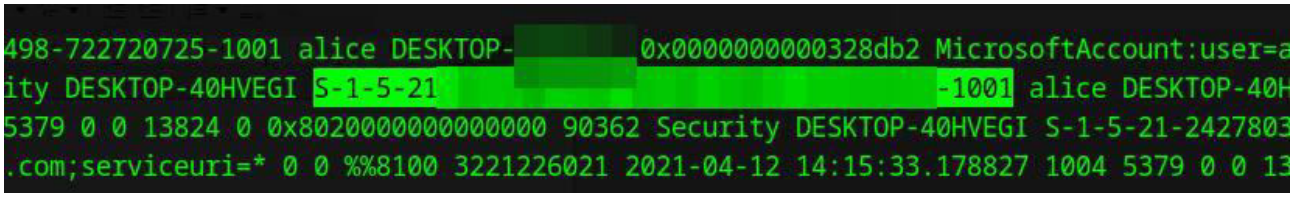
Q1. Which targeted user email address is mentioned in the received file? (Points: 100) Primim un zip (desi pare ca evtx) asa ca trebuie sa ii dam unzip iar din cli observ ca e un base64 si ii dam cat la fisier | base64 -d pentru decriptare.Dupa ce avem fisierul in fata ne intreaba de adresa de email deci putin cheat dam grep la @email.com : cat fisier | base64 -d | grep @gmail.com

Q2. Which is the name of the mentioned working station? (Points: 100)

Direct din prima se observa numele repetat de 10 ori :

Q3. What security identifier (SID) is associated with the targeted Subject? (Points: 100)

Desi nu merge sa fie luata cu grep la inceputul fisierului se vede SID (S vine de la security identifier,**1** reprezintă **nivelul de revizuire** (revizia SID-ului), care este mereu **1**;**5** reprezintă **autoritatea identificatorului** și este specific pentru **NT Authority**. Aceasta indică faptul că SID-ul este asociat cu Windows și cu sistemul de securitate NT. În Windows, autoritatea 5 este folosită pentru a identifica conturile și grupurile implicate în securitatea sistemului, cum ar fi conturile utilizatorilor sau grupurile de pe sistemul local.



Q4. Can you please tell us if the attacker has attempted to perform user enumeration on our stations? If yes, please tell us the event ID which confirms that this action was executed. (Points: 100)

Dupa o cautare mica descopar ca ID normal este 4798 https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4798 banuiala mea fiind aprovata dupa ce descopar in fisier ID care se potrivesc cu acesta.

Q5. Can you please tell us if the attackers have attempted to read the stored credentials from the Credential Manager which is active on our stations? Only the event ID is needed (Points: 100)

Din nou caut ID precis pentru acest event si descopar intr-un articol “The 5379 event occurs when a user performs a read operation on stored credentials in Windows Credential Manager (WCM). Since the successful read from WCM correlates with a failed login in JumpCloud it's very likely that there's an issue with the credentials cached by WCM.”.Din nou este adevarat pentru ca atunci cand dau grep ID acesta este prezent.La ultimele 2 intrebari este cam evident oricum raspunsul ca sunt MAXIM 5-6 id prezente pe acolo asa ca a fost destul de usor de vazut.

Trolled by masquerade8077