Prepared By: Gopi Gor

Date: 02/09/2024

Endpoint Security Investigation

This report analyses 3 different parts of endpoint security and plays a role in incident reporting. This report has been created using Sumologic for lab purposes. Previously parsed logs have been used to run the scripts. Considering a role of an SOC analyst, a report has been prepared for Audit Log cleared, Changes to Domain Admins and detecting compromised user accounts along with business implications.

Audit Log Cleared

As an SOC analyst, I would first try to understand the details of the alert and check whether it has been alerted correctly. I would gather other information like what other logs were cleared in that timespan, what were the system logs within that period and user-based activity in that time. Further, if all the information I collected shows some pattern, I would trigger this to higher authorities for further investigations and remediations. The criticality I would assign to this kind of event with the event ID 1102 would be **high.** This would be because an audit log cleared could mean a lot of things like malicious activity in a specific timeframe or hiding some kind of evidence in case of a security breach. The dashboards I would use could be those which show system logs and anomalies in them. We could also use the Enterprise Audit Dashboard for User activities, which would show us all user activities and then use the Audit Records dashboard to gather all information about the Audit Logs.

The business implications for audit logs can be high because this would mean that the organization loses trust from their customers and its prone to data breaches and deferment from compliance standards. The company could suffer from a lot of financial damage, and it may even affect the reputation for them overall. If we consider short-term risks, there could be a security breach up to any level that may occur and changes in operations due to the compromise. In long-term risks, the organization could be facing charges, or large fines for not being compliant, when it may or may not even by their fault because the audit trails were not found.

The remediation for this would be continuous monitoring of audit logs and by trying to understand the reason of clearance of logs and what other services have been affected by the current audit clearing. We could try to assess what was the cost of this on the organization and the impact it has or may have on the working and operations.

Changes to Domain Admins

The changes to domain admins can be really dangerous, and as an SOC analyst, to investigate this alert, I would first look at all the users that are currently in the system and then check all the permissions given to each user. This would mean looking at AD logs, user groups and user permissions. After this, the specific users with domain permissions can be verified for malicious user activities. The criticality given to this alert would be **high**, because domain admins have permissions to make major changes on the whole domain, and if this has been raised as an alert, it could be really alarming and can affect the whole domain. The dashboards I would use for this alert would Azure Active Directory – Group Management, Authentication/Authorization, User management. We could also use the Enterprise Audit - User Activities dashboard to understand the user activities related to the specific domain admin users.

The business implications of changes to an domain admin could mean that an adversary has the complete control over the active directory, and permissions to groups and users in the whole domain. This could mean a complete network compromise and affect all critical activities, change user permissions, lockout permissions and all settings related to user activities. The whole company would be at a risk. The short-term risks could be data loss and theft and could be service disruptions and loss of account passwords and logins. The long-term risks would be something that can run exploit tools locally to be running background processes without knowledge of people and cause financial losses and compliance fines.

For remediation, the users that are not trusted due to some activity, could be first isolated from the domain or network and assessed in detail. Then, new access control rules and authentication rules can be set up. All the policies and procedures can be assessed thoroughly for all Active Domain services. All known vulnerabilities that were exploited can be remediated too.

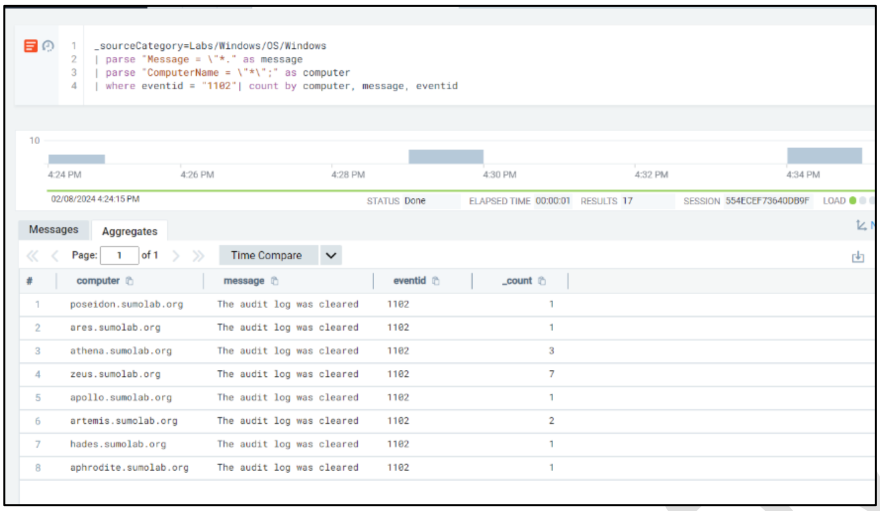
Detecting Compromised User Accounts

As an SOC Analyst, the first step I would take is to determine the accounts that are compromised and check all their details such as logon/logoff and all the locations it is logged in. I would also verify the domain groups that user belongs to and what all permissions the user has been assigned. After this, I would resort to going through different threat intelligence feeds to cross-examine the things I have discovered. Overall, the incident needs to be checked for all reasons according to user logins and user details. The criticality that I would assign to this alert type would be **high** because these compromised accounts can steal personal and sensitive information about the user and/or other users in the same domain. The dashboards I would use for this alert type would include user session activities, AD failed sign in events, AD successfully signed in events and many other useful dashboards related to users in the Enterprise Audit.

The business impact would be that leading to data breaches and compromised user accounts, and financial losses occurring in different domains. In this case, the access granted to these accounts could be affecting the assets of the organization and the sensitive information of the users, employees and customers of the organization. The short-term risks could be data theft, identity theft, unauthorized access and damage to availability of resources. The long-term risks would surely be the complete reputational damage of the company and loss of trust in customers and clients.

The remediation can be to remove all the compromised accounts, resetting all passwords, and various endpoint remediation services. Since users are getting compromised, the users of all applications and domain accounts should be made sure and aware of in every way possible via awareness sessions, quick games to learn more, the importance of their data and the problems that occur to them and the organization if their data is stolen.

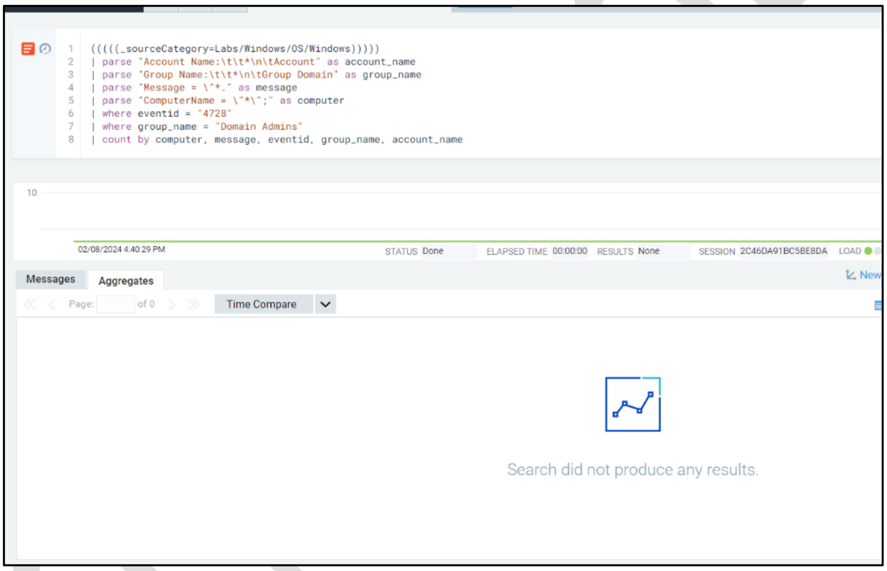
Appendix



```
_sourceCategory=Labs/Windows/OS/Windows
| parse "Message = \"*." as message
| parse "ComputerName = \"*\";" as computer
| where eventid = "1102"| count by computer, message, eventid
```

02/08/2024 4:24:15 PM STATUS Done ELAPSED TIME 00:00:01 RESULTS 17 SESSION 554ECEF73640DB9F LOAD

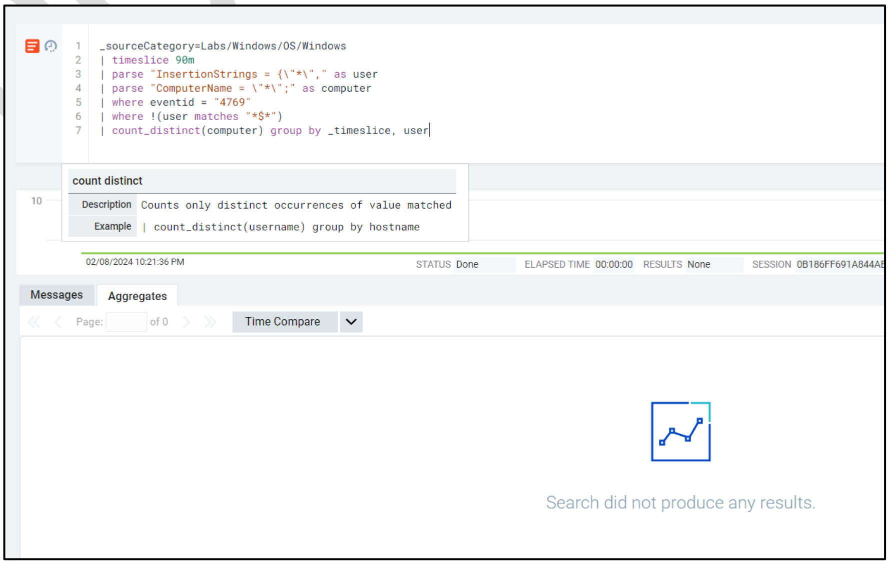
#	computer	message	eventid	_count
1	poseidon.sumolab.org	The audit log was cleared	1102	1
2	ares.sumolab.org	The audit log was cleared	1102	1
3	athena.sumolab.org	The audit log was cleared	1102	3
4	zeus.sumolab.org	The audit log was cleared	1102	7
5	apollo.sumolab.org	The audit log was cleared	1102	1
6	artemis.sumolab.org	The audit log was cleared	1102	2
7	hades.sumolab.org	The audit log was cleared	1102	1
8	aphrodite.sumolab.org	The audit log was cleared	1102	1



```
(((((_sourceCategory=Labs/Windows/OS/Windows)))))
| parse "Account Name:\t\t*\n\tAccount" as account_name
| parse "Group Name:\t\t*\n\tGroup Domain" as group_name
| parse "Message = \"*." as message
| parse "ComputerName = \"*\";" as computer
| where eventid = "4728"
| where group_name = "Domain Admins"
| count by computer, message, eventid, group_name, account_name
```

02/08/2024 4:40:29 PM STATUS Done ELAPSED TIME 00:00:00 RESULTS None SESSION 2C46DA91BC5BE8DA LOAD

Search did not produce any results.



```
_sourceCategory=Labs/Windows/OS/Windows
| timeslice 90m
| parse "InsertionStrings = {\"*\"," as user
| parse "ComputerName = \"*\";" as computer
| where eventid = "4769"
| where !(user matches "*$*")
| count_distinct(computer) group by _timeslice, user
```

count distinct

Description Counts only distinct occurrences of value matched

Example | count_distinct(username) group by hostname

02/08/2024 10:21:36 PM STATUS Done ELAPSED TIME 00:00:00 RESULTS None SESSION 0B186FF691A844AE

Search did not produce any results.

References

1. https://support.alertlogic.com/hc/en-us/articles/115004121423-Windows-Security-Event-Log-Cleared
2. https://www.cyberis.com/article/why-you-need-protect-da-domain-admin
3. https://www.code42.com/blog/compromised-account-attacks-are-growing-heres-what-you-can-do/
4. https://cyberint.com/blog/thought-leadership/compromised-credentials-tactics-risks-mitigation/