FIREWALL

SSH-DICT

SELECT

SRC, DST, COUNT(\*) numberOfAttempts

FROM [skodahacker1].[dbo].[firewal3]

GROUP BY SRC, DST, PROTO, DPT

HAVING SRC not like '192.168.56.%' AND SRC not like '192.168.50.%' AND PROTO = 'TCP' AND DPT = 22

ORDER BY numberOfAttempts DESC

TELNET ANOMALY

SELECT

SRC, DST, COUNT(\*) numberOfAttempts

FROM [skodahacker1].[dbo].[firewal3]

GROUP BY SRC, DST, PROTO, DPT

HAVING PROTO = 'TCP' AND DPT = 23

ORDER BY numberOfAttempts DESC

SCANS- horizontal

SELECT

SRC, DST, COUNT(\*) numberOfConnections, count(distinct(DPT)) as numberOfPortScans

FROM [skodahacker1].[dbo].[firewal3]

GROUP BY SRC, DST

HAVING SRC NOT like('192.168.50.%') and SRC NOT Like('192.168.56.%')

ORDER BY numberOfPortScans DESC

SCAN-Vertical

SELECT

SRC, DST, COUNT(\*) numberOfConnections, count(distinct(DPT)) as numberOfPortScans

FROM [skodahacker1].[dbo].[firewal3]

GROUP BY SRC, DST

HAVING SRC not like '192.168.56.%' AND

SRC not like '192.168.50.%'

ORDER BY numberOfPortScans DESC

Pri vyhodnocovani vysledku scanu sme si vsimli ze vsetky IP s SrcIp mimo nas subnet komunikuju cez nas firewall len s uzlom 10.0.2.15. Blizsie informacie o tomto uzly nebolo mozne dalej ziskat.

Timto sme dospeli k zaveru ze v aktualnej vzorke dat sa pravdeposobne nenachada ziadny prebiehajuci utok z vonkajsej siete na nasu. Dalsia cast riesenie je zalozena na analyze dat z vnutornej siete.

Query: Horizontal Scan attack detection

SELECT [Application Name] AppName,[SourceAddress], [DestinationAddress], count(\*) as TotalCount, (count(distinct([Destination Port]))\*1.0 / count(\*)) uniquePortsRatio

FROM [skodahacker1].[dbo].[processed\_PC6\_security]

group by [Application Name],[Source Address], [Destination Address]

having count(\*) > 100

order by uniquePortsRatio desc

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **AppName** | **SourceAddress** | **DestinationAddress** | **TotalCount** | **UniquePortsRatio** |
| svchost.exe | 224.0.0.252 | 192.168.50.105 | 13126 | 0.413225658997 |
| svchost.exe | ff02::1:3 | fe80::b170:9f2f:aa4:3f77 | 13124 | 0.409326424870 |
| svchost.exe | 224.0.0.252 | 192.168.50.102 | 28130 | 0.338713117667 |
| svchost.exe | ff02::1:3 | fe80::652d:d842:9d60:519f | 28130 | 0.338713117667 |
| svchost.exe | 224.0.0.252 | 192.168.50.101 | 27624 | 0.338509991311 |
| svchost.exe | ff02::1:3 | fe80::b5cc:7d2d:cf8f:2d8a | 27624 | 0.338509991311 |
| svchost.exe | 239.255.255.250 | 192.168.50.102 | 9448 | 0.229784081287 |
| svchost.exe | 239.255.255.250 | 192.168.50.101 | 9941 | 0.220199175133 |
| svchost.exe | 239.255.255.250 | 192.168.50.105 | 8726 | 0.207540683016 |
| chrome.exe | 192.168.50.106 | 93.184.220.66 | 104 | 0.019230769230 |
| chrome.exe | 192.168.50.106 | 192.0.77.32 | 106 | 0.018867924528 |

QUERY: Vertical Scan Attack

SELECT [Application Name] AppName, [Source Address], [Destination Port], count(\*) as TotalCount, (count(distinct([Destination Address]))\*1.0 / count(\*)) uniqueAddressRatio

FROM [skodahacker1].[dbo].[processed\_PC6\_security]

group by [Application Name],[Source Address], [Destination Port]

having count(\*) > 100

order by uniqueAddressRatio desc

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AppName | Source Address | Destination Port | TotalCount | uniqueAddressRatio |
| System | 192.168.50.106 | 137 | 4829 | 0.372747980948 |
| chrome.exe | 192.168.50.106 | 80 | 6656 | 0.186598557692 |
| chrome.exe | 192.168.50.106 | 443 | 52341 | 0.092661584608 |
| chrome.exe | 192.168.50.106 | 53 | 277 | 0.010830324909 |
| svchost.exe | 192.168.50.106 | 67 | 204 | 0.009803921568 |
| System | 192.168.50.255 | 138 | 346 | 0.008670520231 |
| svchost.exe | 239.255.255.250 | 58720 | 124 | 0.008064516129 |

Query: ProcessHashControl

SELECT [Image], [FIleVersion], count(\*)

FROM [skodahacker1].[dbo].[processed\_PC2\_sysmon]

group by [Image], [FileVersion]

having count(distinct(Hashes)) > 1

results = 0

000000000000000000000000000000000000000000

ANalyzovat konkretny malware v service logoch

Prihlasenie na stroj?

SELECT [Message], ImageLoaded, Hashes, [Signature], Signed

FROM [skodahacker1].[dbo].[processed\_PC1\_sysmon]

group by [Message], ImageLoaded, Hashes, [Signature], Signed

having [Message] = 'Driver loaded:'

SELECT

SRC, PROTO, count(\*) cnt

FROM [skodahacker1].[dbo].[firewal3]

GROUP BY SRC, PROTO

having count(\*) > 10

ORDER BY PROTO, cnt DESC