Another proxy to connect to our database

Last updated by | Vitor Tomaz | Oct 1, 2020 at 8:01 AM PDT

Another proxy to connect to our database

Friday, October 21, 2016
0:33

I've been working on an advisory case for SQL Auditing and I have found another "point of access" for our customers.

I have found that even either server and database don't have configured SQL Auditing, we are able to connect to the server/database using servername.database.secure.windows.net (and in the table/blob storage auditing). So, the next time, if we are not able to connect using servername.database.windows.net we could use servername.database.secure.windows.net due to

10.212.3.218	10.164.97.44	TCP	TCP:[ReTransmit #9858]Flags=...AP..., SrcPort=1729
10.164.97.44	10.212.3.218	TCP	TCP:Flags=...A...., SrcPort=MS WBT Server(3389), Ds
10.164.97.44	10.212.3.218	TCP	TCP:[Dup Ack #9860]Flags=...A...., SrcPort=MS WBT
10.212.3.218	10.164.97.44	RDPBCGR	RDPBCGR:
10.212.3.218	10.164.97.44	TCP	TCP:[ReTransmit #9862]Flags=...AP..., SrcPort=1729
10.164.97.44	datasec-neu-2-a3.cloudapp.net	TDS	TDS:Data, Version = 7.300000(No version information
10.164.97.44	datasec-neu-2-a3.cloudapp.net	TCP	TCP:[ReTransmit #9864]Flags=...AP..., SrcPort=5836
10.212.3.218	10.164.97.44	RDPBCGR	RDPBCGR:
10.212.3.218	10.164.97.44	TCP	TCP:[ReTransmit #9866]Flags=...AP..., SrcPort=1729
10.164.97.44	10.212.3.218	TCP	TCP:Flags=...A...., SrcPort=MS WBT Server(3389), Ds
10.164.97.44	10.212.3.218	TCP	TCP:[Dup Ack #9868]Flags=...A...., SrcPort=MS WBT
datasec-neu-2-a3.cloudapp.net	10.164.97.44	TDS	TDS:Data, Version = 7.300000(No version information
datasec-neu-2-a3.cloudapp.net	10.164.97.44	TCP	TCP:[ReTransmit #9870]Flags=...AP..., SrcPort=1433
10.212.3.218	10.164.97.44	RDPBCGR	RDPBCGR:
10.212.3.218	10.164.97.44	TCP	TCP:[ReTransmit #9872]Flags=...AP..., SrcPort=1729
10.164.97.44	10.212.3.218	TCP	TCP:Flags=...A...., SrcPort=MS WBT Server(3389), Ds
10.164.97.44	10.212.3.218	TCP	TCP:[Request Fast-Retransmit from Seq746968284]Fla
10.164.97.1	10.164.97.7	ARP	ARP:Request, 10.164.97.1 asks for 10.164.97.7
10.164.97.1	10.164.97.7	ARP	ARP:Request, 10.164.97.1 asks for 10.164.97.7
10.164.97.44	datasec-neu-2-a3.cloudapp.net	TCP	TCP:Flags=...A...., SrcPort=58368, DstPort=1433, Pa
10.164.97.44	datasec-neu-2-a3.cloudapp.net	TCP	TCP:[Dup Ack #9878]Flags=...A...., SrcPort=58368, D
10.212.3.218	10.164.97.44	RDPBCGR	RDPBCGR:
10.212.3.218	10.164.97.44	TCP	TCP:[ReTransmit #9880]Flags=...AP..., SrcPort=1729
10.164.97.44	10.212.3.218	TCP	TCP:Flags=...A...., SrcPort=MS WBT Server(3389), Ds
10.164.97.44	10.212.3.218	TCP	TCP:[Dup Ack #9882]Flags=...A...., SrcPort=MS WBT
10.212.3.218	10.164.97.44	TCP	TCP:Flags=...A...., SrcPort=1729, DstPort=MS WBT S
10.212.3.218	10.164.97.44	TCP	TCP:[Dup Ack #9884]Flags=...A...., SrcPort=1729, Ds
10.164.97.44	10.212.3.218	UDP	UDP:SrcPort = MS WBT Server(3389), DstPort = 5417
10.164.97.44	10.212.3.218	UDP	UDP:SrcPort = MS WBT Server(3389), DstPort = 5417
10.164.97.44	10.212.3.218	UDP	UDP:SrcPort = MS WBT Server(3389), DstPort = 5417

How good have you found this content?