Incident report

Executive summary:

On April 28 at 00:30 we received an alert from IDS suspicious network activity. After investigation we discovered that our public-facing MSSQL server was brute-forced and used to deliver a C2 beacon, injecting it into a legitimate Windows process for privilege escalation. As a result, several malicious files were uploaded, including Blue Sky ransomware. Incident was contained, compromised server isolated, all signatures of malicious presence were eliminated before any significant data breach or encryption.

Incident details:

Name: SQL Brute-force

Date/Time: 28.4.24 00:29:56 UTC Incident type: ransomware, brute-force

Impact assessment:

Scope:

Devices affected -1 (DESKTOP-7EQVM78)

Users affected - (sa)

Data types:

credentials

hosts

Downtime - 22 minutes

Summary:

Timeline:

00:29.56 - port scan, port 1433 discovered

00.23.30	- port so	an, port 1700 disc	OVCICU	
23 2.02/033	07.90.21.04	07.90.21.01	TCF	74 JOUAN - 7 440 [JIR] JEGO RIII-JELZO LEII-O ROJ-1400 JACK_FLIRI IJVAL-JEJJJJJJZZO IJECI -O RJ-120
26 2.827853	87.96.21.84	87.96.21.81	TCP	74 59724 → 199 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739226 TSecr=0 WS=128
27 2.827853	87.96.21.84	87.96.21.81	TCP	74 36474 → 554 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739226 TSecr=0 WS=128
28 2.827870	87.96.21.81	87.96.21.84	TCP	54 443 → 50674 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29 2.827894	87.96.21.81	87.96.21.84	TCP	54 199 → 59724 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30 2.827916	87.96.21.81	87.96.21.84	TCP	54 554 → 36474 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31 2.828003	87.96.21.84	87.96.21.81	TCP	74 46058 → 587 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739226 TSecr=0 WS=128
32 2.828016	87.96.21.81	87.96.21.84	TCP	54 587 → 46058 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33 2.828106	87.96.21.84	87.96.21.81	TCP	74 42870 → 22 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739227 TSecr=0 WS=128
34 2.828120	87.96.21.81	87.96.21.84	TCP	54 22 → 42870 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35 2.828372	87.96.21.84	87.96.21.81	TCP	60 36884 → 445 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0
36 2.828466	87.96.21.84	87.96.21.81	TCP	74 49584 → 143 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739227 TSecr=0 WS=128
37 2.828466	87.96.21.84	87.96.21.81	TCP	74 40410 → 25 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739227 TSecr=0 WS=128
38 2.828481	87.96.21.81	87.96.21.84	TCP	54 143 → 49584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
39 2.828505	87.96.21.81	87.96.21.84	TCP	54 25 → 40410 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40 2.828594	87.96.21.84	87.96.21.81	TCP	74 45444 → 110 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739227 TSecr=0 WS=128
41 2.828608	87.96.21.81	87.96.21.84	TCP	54 110 → 45444 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42 2.828695	87.96.21.84	87.96.21.81	TCP	74 53088 → 139 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739227 TSecr=0 WS=128
43 2.828918	87.96.21.81	87.96.21.84	TCP	66 139 → 53088 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
44 2.829023	87.96.21.84	87.96.21.81	TCP	74 54728 → 135 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739227 TSecr=0 WS=128
45 2.829023	87.96.21.84	87.96.21.81	TCP	74 47628 → 1723 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739227 TSecr=0 WS=128
46 2.829023	87.96.21.84	87.96.21.81	TCP	74 52384 → 1025 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739227 TSecr=0 WS=128
47 2.829023	87.96.21.84	87.96.21.81	TCP	74 36350 → 1720 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739227 TSecr=0 WS=128
48 2.829023	87.96.21.84	87.96.21.81	TCP	60 53088 → 139 [ACK] Seq=1 Ack=1 Win=32128 Len=0
49 2.829093	87.96.21.81	87.96.21.84	TCP	66 135 → 54728 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
50 2.829126	87.96.21.81	87.96.21.84	TCP	54 1723 → 47628 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
51 2.829147	87.96.21.81	87.96.21.84	TCP	54 1025 → 52384 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
52 2.829194	87.96.21.81	87.96.21.84	TCP	54 1720 → 36350 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
53 2.829409	87.96.21.84	87.96.21.81	TCP	74 33350 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739228 TSecr=0 WS=128
54 2.829409	87.96.21.84	87.96.21.81	TCP	60 54728 → 135 [ACK] Seq=1 Ack=1 Win=32128 Len=0
55 2.829409	87.96.21.84	87.96.21.81	TCP	74 47596 → 993 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739228 TSecr=0 WS=128
56 2.829409	87.96.21.84	87.96.21.81	TCP	74 32952 → 995 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739228 TSecr=0 WS=128
57 2.829427	87.96.21.81	87.96.21.84	TCP	54 80 → 33350 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58 2.829523	87.96.21.81	87.96.21.84	TCP	54 993 → 47596 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59 2.829548	87.96.21.81	87.96.21.84	TCP	54 995 → 32952 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60 2.829637	87.96.21.84	87.96.21.81	TCP	74 59710 → 8080 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739228 TSecr=0 WS=128
61 2.829651	87.96.21.81	87.96.21.84	ТСР	54 8080 → 59710 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62 2.829738	87.96.21.84	87.96.21.81	TCP	74 48262 → 8888 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739228 TSecr=0 WS=128
63 2.829752	87.96.21.81	87.96.21.84	TCP	54 8888 → 48262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
64 2.832891	87.96.21.84	87.96.21.81	TCP	74 57842 → 111 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155739231 TSecr=0 WS=128

00:30:06 – dictionary attack started on MSSQL server (EID 18456)

```
MSSQLSERVER
MSSQLSERVER
                                                  18456 (4)
MSSQLSERVER
                                                  18456
                                                        (4)
MSSQLSERVER
                                                  18456
MSSOLSERVER
                                                  18456 (4)
MSSQLSERVER
                                                  18456
MSSQLSERVER
                                                  18456
MSSOLSERVER
                                                 18456 (4)
MSSOI SERVER
                                                 18456
MSSQLSERVER
                                                 18456
MSSQLSERVER
```

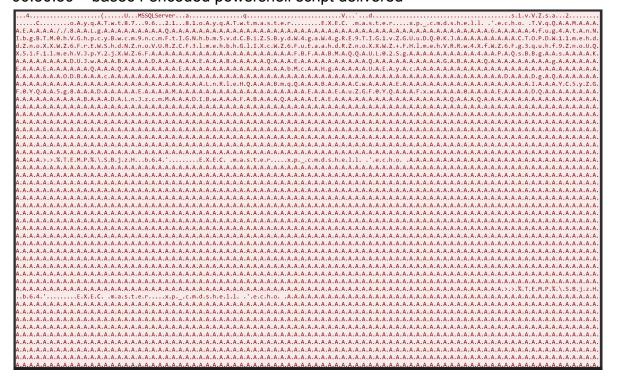
00:30:13 - successful login (EID 18454)

MSSQLSERVER	18454 (4)
MCCOLCED\/ED	15/57 /2\

00:30:13 - xp_cmdshell enabled

```
Urgent Pointer: 0
  [Timestamps]
  [SEQ/ACK analysis]
   TCP payload (222 bytes)
  [PDU Size: 222]
Tabular Data Stream
  Type: SQL batch (1)
  Status: 0x01, End of message
  Length: 222
  Channel: 0
  Packet Number: 1
  Window: 0
  TDS Query Packet
     Query: EXEC sp_configure 'show advanced options', 1; RECONFIGURE; EXEC sp_configure 'xp_cmdshell', 1; RECONFIGURE;
                                                        ··)U^··
   00 0c 29 55 5e 8f 00 0c 29 36 be 8f 08 00 45 00
   01 06 95 ad 40 00 40 06
                             ca df 57 60 15 54 57 60
                                                           @ @
                                                                  -W`-TW
   15 51 82 71 05 99 48 ad b9 1e ba 74 3d d6 50 18
                                                                 \cdot \cdot \cdot t = \cdot P
   00 f9 53 6d 00 00 01 01 00 de 00 00 01 00 45 00
   58 00 45 00 43 00 20 00 73 00 70 00 5f 00 63 00
                                                       X E C
                                                       onfigure
'show a
   6f 00 6e 00 66 00 69 00 67 00 75 00 72 00 65 00
   20 00 27 00 73 00 68 00 6f 00 77 00 20 00 61 00
   64 00 76 00 61 00 6e 00 63 00 65 00 64 00 20 00
```

00:30:39 - base64 encoded powershell script delivered



00:32:08 – script mounted winlogon.exe gaining administrative privileges

Information	n 4/23/2024 1:01:17 PM Po	werShell (PowerShell) 600	Provider Lifecycle
Information	n 4/23/2024 1:01:17 PM Po	werShell (PowerShell) 600	Provider Lifecycle
Information	n 4/23/2024 1:01:18 PM Po	werShell (PowerShell) 400	Engine Lifecycle
Information	n 4/23/2024 1:07:43 PM Wi	indows Error Reporting 1001	None
Information	n 4/23/2024 1:11:10 PM MS	SSQLSERVER 18453	(4)
ent 400, Por	werShell (PowerShell)		
General De	letails		
Engine sta	ate is changed from None to Available.		
Engine sta	ate is changed from None to Available.		
Details:	NewEngineState=Available		
Details:			
Details:	NewEngineState=Available		
Details:	NewEngineState=Available PreviousEngineState=None SequenceNumber=17 HostName=MSFConsole		
Details:	NewEngineState=Available PreviousEngineState=None SequenceNumber=17 HostName=MSFConsole HostWesion=0.1		
Details:	NewEngineState=Available PreviousEngineState=None SequenceNumber+17 HostName=MSFConsole HostVersion=0.1 HostOstdid=1093665cc-ce22-41d0-8356-4245271c31e8		
Details:	NewEngineState=Available PreviousEngineState=None SequenceNumber=17 HotsName=MSFConsole HotsWissin=0,1 HotsItsIn=05866c.ce22.41d0-8356-4245271c31e8 HotsApplication=windopon.ee		
Details:	NewEngineState=Available PreviousEngineState=None SequenceNumber+17 HostName=MSFConsole HostVersion=0.1 HostOstdid=1093665cc-ce22-41d0-8356-4245271c31e8		

00:32:12 - 00:32:14 - malicious files uploaded to the server

Protoco	ol Length Info
HTTP	127 GET /checking.ps1 HTTP/1.1
HTTP	210 GET / HTTP/1.1
HTTP	217 GET /del.ps1 HTTP/1.1
HTTP	122 GET /del.ps1 HTTP/1.1
HTTP	130 GET /ichigo-lite.ps1 HTTP/1.1
HTTP	135 GET /Invoke-PowerDump.ps1 HTTP/1.1
HTTP	133 GET /Invoke-SMBExec.ps1 HTTP/1.1
HTTP	229 GET /extracted_hosts.txt HTTP/1.1
HTTP	135 GET /Invoke-PowerDump.ps1 HTTP/1.1
HTTP	124 GET /javaw.exe HTTP/1.1
HTTP	122 GET /del.ps1 HTTP/1.1
HTTP	130 GET /ichigo-lite.ps1 HTTP/1.1
HTTP	135 GET /Invoke-PowerDump.ps1 HTTP/1.1
HTTP	133 GET /Invoke-SMBExec.ps1 HTTP/1.1
HTTP	229 GET /extracted_hosts.txt HTTP/1.1
HTTP	135 GET /Invoke-PowerDump.ps1 HTTP/1.1
HTTP	124 GET /javaw.exe HTTP/1.1

00:34:09 - server isolated

00:49:00 – all malicious files identified and quarantined, file system, memory and registry check executed, sa user disabled, SQL server reconfigured

Logs and evidence Network capture | Event log

Tools used: wireshark, event viewer, network miner, virustotal

loCs:

Ip address 87.96.21.84

Hashes:

BB4D98715655D6A8C812C18C92EAAB5CC57EEC74ECA581F2760EE4880BAF74D2 checking.ps1 9136924205CF55FA3A3EDBD0191CCA190E559B1619C07743E6DD7A3CD022D33F del.ps1 38FE562136ADE372FC4CEDDE67826AEEA8404E93A54A4A4736DDB4C8C8D4C96D ichigo-lite.ps1 3B463C94B52414CFAAD61ECDAC64CA84EAEA1AB4BE69F75834AAA7701AB5E7D0 Invoke-PowerDump.ps1 2211A127A4467FB15A2112DD48EBE26DF2660F97E6B8BE95DB57BBAFAB806412 Invoke-SMBExec.ps1 3E035F2D7D30869CE53171EF5A0F761BFB9C14D94D9FE6DA385E20B8D96DC2FB javaw.exe

Containment and eradication:

Containment:

IP 87.96.21.84 blocked

User sa disabled

Affected endpoint isolated

Eradication:

Malware removed

Memory and registry integrity checked

SQL server privileges updated, xp cmdshell disabled

Recovery:

SQL server patched

Audit for rogue accounts conducted

Lessons learned:

Root cause – weak high privileged SQL account policy led to successful bruteforce, not permanently disabled OS command execution and lack of detection rules for suspicious network and endpoint activity allowed malware delivery. Unlimited privileges for SQL server. Incident had potential for significant impact due to strong persistence and evasion presence in ransomware accompanying powershell scripts.

I recommend implementing lockout policy, MFA for administrative accounts, software privilege audit and updating detection rules.

Analysis of logs, network traffic and captured malware showed a well staged attack, armed with a tailored dictionary for successful brute-force attack and an organisation's list of host IP's, which can mean a prior data breach.

Analysis of accessed evidence allows us to anticipate, what were adversary's vectors of attack according to MITRE ATT&CK

Valid Accounts - T1078

Brute Force - T1110

Command and Scripting Interpreter: Visual Basic - T1059.005

Scheduled Task - T1053.005

Windows Command Shell - T1059.003

PowerShell - T1059.001

Disable or Modify Tools - T1562.001

Process Injection - T1055

LSASS Memory - T1003.001

System Owner/User Discovery - T1033

Network Share Discovery - T1135

Data Encrypted for Impact - T1486

SMB/Windows Admin Shares - T1021.002

Web Protocols - T1071.001

Service Execution - T1569.002

Modify Registry - T1112

Obfuscated Files or Information - T1027

Windows Service - T1543.003

Masquerade Task or Service - T1036.004