



Hasil Monitoring Keamanan Siber

Beringin Kuning
Corporation

Incident Report

Disusun Oleh:
Zahran Difa Vidian

Ringkasan

Laporan ini merupakan hasil dari upaya menyeluruh dalam menginvestigasi insiden keamanan. Kejadian ini melibatkan akses tidak sah dan lateral movement menggunakan alat PsExec oleh penyerang di dalam jaringan kami.



Ikhtisar Kejadian



Tipe Insiden

Network Intrusion

Waktu Deteksi

11-10-2023 07:23

Metode Analysis

Traffic Capture Analysis

Kronologi Kejadian



Deteksi aktivitas jaringan yang tidak biasa berasal dari alamat IP 10.0.0.130.

Penyerang berhasil berpivot ke Sales-PC.

Penggunaan username ssales teridentifikasi dalam log jaringan.

Eksekusi layanan psexesvc teramati.

Penyerang mengakses share jaringan ADMIN\$ pada mesin target.

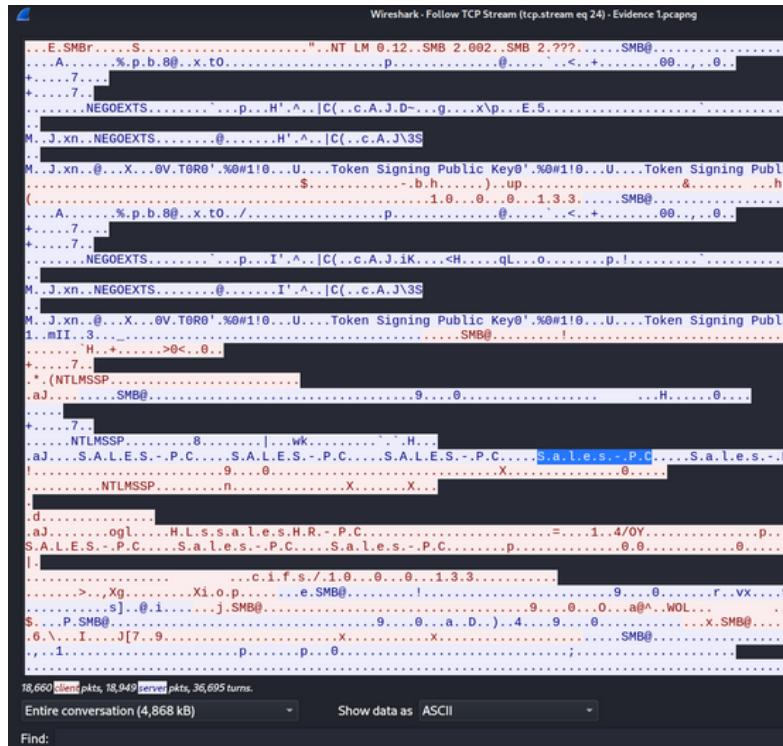
Penggunaan IPC\$ untuk komunikasi teramati.

Deteksi upaya untuk berpivot ke Marketing-PC.

Ethernet · 10	IPv4 · 10	IPv6	TCP · 77	UDP · 11
Address	Packets ▲	Bytes	Tx Packets	Tx Bytes
10.0.0.130	40,040	9 MB	20,374	5 MB
10.0.0.133	38,284	7 MB	19,047	3 MB
10.0.0.131	1,768	2 MB	621	472 kB

Source	Source Destination	Destination	Protocol	Length	Info
10.0.0.130	49096	10.0.0.133	445	SMB2	228 Session Negotiate Protocol Request
10.0.0.130	49096	10.0.0.133	445	SMB2	229 Session Setup Request: NTLMSSP_NEGOTIATE
10.0.0.130	49096	10.0.0.133	445	SMB2	295 Session Setup Request: NTLMSSP_AUTH, User: \ssales
10.0.0.130	49096	10.0.0.133	445	SMB2	184 IOCTL Request FILE_PIPE_TRANSCEIVE Tree: \\10.0.0.133\IPC\$
10.0.0.130	49096	10.0.0.133	445	SMB2	168 Tree Connect Request Tree: \\10.0.0.133\ADMIN\$
10.0.0.130	49096	10.0.0.133	445	SMB2	234 Create Request File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	SMB2	146 Close Request File:
10.0.0.130	49096	10.0.0.133	445	SMB2	382 Create Request File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	SMB2	1514 Write Request Len:65536 Off:0 File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	SMB2	1514 Write Request Len:65536 Off:0 File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	SMB2	1514 Write Request Len:65536 Off:131072 File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	SMB2	578 Write Request Len:408 Off:241664 File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	SMB2	162 GetInfo Request FILE_INFO_SMB2_FILE_NETWORK_OPEN_INFO File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	SMB2	145 Close Request File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	SMB2	494 Create Request File: PSEXEC-HR-PC-1C6C5014.key
10.0.0.130	49096	10.0.0.133	445	SMB2	178 Write Request Len:0 Off:0 File: PSEXEC-HR-PC-1C6C5014.key
10.0.0.130	49096	10.0.0.133	445	SMB2	178 Write Request Len:0 Off:0 File: PSEXEC-HR-PC-1C6C5014.key
10.0.0.130	49096	10.0.0.133	445	SMB2	194 Create Request File: PSEXESVC
10.0.0.130	49096	10.0.0.133	445	SMB2	162 GetInfo Request FILE_INFO_SMB2_FILE_STANDARD_INFO File: PSEXESVC
10.0.0.130	49096	10.0.0.133	445	SMB2	738 IOCTL Request FSCTL_PIPE_TRANSCEIVE File: PSEXESVC
10.0.0.130	49096	10.0.0.133	445	SMB2	158 Lease Break Acknowledgment
10.0.0.130	49096	10.0.0.133	445	SMB2	162 GetInfo Request FILE_INFO_SMB2_FILE_NETWORK_OPEN_INFO File: PSEXEC-HR-PC-1C6C5014.key
10.0.0.130	49096	10.0.0.133	445	SMB2	146 Close Request File: PSEXEC-HR-PC-1C6C5014.key
10.0.0.130	49096	10.0.0.133	445	SMB2	174 Write Request Len:4 Off:0 File: PSEXESVC
10.0.0.130	49096	10.0.0.133	445	SMB2	1465 Write Request Len:65535 Off:0 File: PSEXESVC

Statistik menunjukkan bahwa alamat IP 10.0.0.130 mendominasi sebagai perangkat paling aktif dalam jaringan. Melalui penelusuran lebih lanjut, diketahui bahwa alamat IP ini terlibat dalam aktivitas yang mencurigakan, terutama terkait dengan eksekusi PSEXESVC.exe.



Pelaku berhasil melakukan pivot ke host yang dikenal dengan nama SALES-PC. Informasi ini berhasil dihimpun melalui analisis TCP Stream yang mencakup kegiatan pelaku saat mencoba mengakses dan masuk ke sistem dengan menggunakan kredensial pengguna 'ssales'.

```

133 2023-10-11 07:42:08.8805972... 10.0.0.133 445 10.0.0.13...
134 2023-10-11 07:42:08.8812758... 10.0.0.130 49696 10.0.0.13...
135 2023-10-11 07:42:08.8814814... 10.0.0.133 445 10.0.0.13...
136 2023-10-11 07:42:08.8817186... 10.0.0.130 49696 10.0.0.13...
137 2023-10-11 07:42:08.8818413... 10.0.0.133 445 10.0.0.13...
138 2023-10-11 07:42:08.8829951... 10.0.0.130 49696 10.0.0.13...
139 2023-10-11 07:42:08.8834285... 10.0.0.133 445 10.0.0.13...
140 2023-10-11 07:42:08.8840526... 10.0.0.130 49696 10.0.0.13...
141 2023-10-11 07:42:08.8842891... 10.0.0.133 445 10.0.0.13...
142 2023-10-11 07:42:08.8846716... 10.0.0.130 49696 10.0.0.13...
143 2023-10-11 07:42:08.8848749... 10.0.0.133 445 10.0.0.13...
144 2023-10-11 07:42:08.8851790... 10.0.0.130 49696 10.0.0.13...
145 2023-10-11 07:42:08.8857583... 10.0.0.133 445 10.0.0.13...
146 2023-10-11 07:42:08.8862667... 10.0.0.130 49696 10.0.0.13...
147 2023-10-11 07:42:08.8862711... 10.0.0.130 49696 10.0.0.13...
148 2023-10-11 07:42:08.8862731... 10.0.0.130 49696 10.0.0.13...
149 2023-10-11 07:42:08.8862747... 10.0.0.130 49696 10.0.0.13...
150 2023-10-11 07:42:08.8862766... 10.0.0.130 49696 10.0.0.13...

```

```

Credits granted: 33
Flags: 0x00000019, Response, Signing, Priority
Chain Offset: 0x00000000
Message ID: 3
Process Id: 0x0000feff
Tree Id: 0x00000000
Session Id: 0x0000300000000039 Acct:ssales Domain: Host:HR-PC
[Account: ssales]
[Domain: ]
[Host: HR-PC]
[Authenticated in Frame: 122]

```

Pelaku menggunakan username untuk melakukan lateral movement, terlihat dari log setelah session setup request, dalam session setup response account menjadi ssales

SMB2	382 Create Request File: PSEXESVC.exe
SMB2	410 Create Response File: PSEXESVC.exe
SMB2	1514 Write Request Len:65536 Off:0 File: PSEXESVC
SMB2	1418 Write Request Len:65536 Off:65536 File: PSEX
SMB2	138 Write Response
SMB2	138 Write Response
SMB2	1514 Write Request Len:65536 Off:131072 File: PSE
SMB2	138 [TCP ACKed unseen segment] Write Response
SMB2	138 Write Response
SMB2	570 Write Request Len:400 Off:241664 File: PSEX
SMB2	138 [TCP ACKed unseen segment] Write Response
.....	0000 00 0c 29 59 23 50 00 0c 29 06 cc 75 0
	0010 01 70 03 d0 40 00 80 06 e0 b1 0a 00 0
	0020 00 85 c2 20 01 bd dd ef 94 c0 d8 89 6
	0030 20 12 6c d8 00 00 00 00 01 44 fe 53 4
	0040 01 00 00 00 00 00 05 00 01 00 30 00 0
	0050 00 00 09 00 00 00 00 00 00 00 ff fe 0
	0060 00 00 39 00 00 00 00 30 00 00 00 00 0
	0070 00 00 00 00 00 00 00 00 00 00 39 00 0
	0080 00 00 00 00 00 00 00 00 00 00 00 00 0
	0090 00 00 96 01 12 00 80 00 00 00 03 00 0
	00a0 00 00 60 00 00 00 78 00 18 00 90 00 0
	00b0 00 00 50 00 53 00 45 00 58 00 45 00 5
	00c0 43 00 2e 00 65 00 78 00 65 00 38 00 0

Memakai filter SMB2, pelaku terlihat merequest file PSEXESVC.exe dan mencoba run file tersebut. Bisa dipastikan file tersebut adalah executable service yang dipakai oleh pelaku untuk menggunakan backdoor

168 Tree Connect Request Tree: \\10.0.0.133\ADMIN\$
138 Tree Connect Response

Hasil analisis dari log adalah Pelaku menggunakan Network Share ADMIN\$, terlihat dari saat awal pelaku meminta Tree Connect Request dan saat pelaku merequest file PSEXESVC.exe dalam tree id. Ini berarti pelaku menggunakan ADMIN\$ untuk menginstall service tersebut

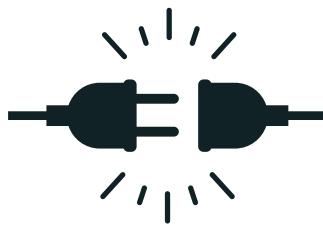
Pelaku menggunakan fasilitas jaringan berupa network share yang disebut IPC\$ untuk menjalin komunikasi antara dua mesin dalam suatu jaringan dengan memanfaatkan IPC\$ (Inter-Process Communication)

No.	Time	Source	Source I.D.	Destination	Protocol	Length	Info
1	2023-10-11 07:37:25.46965365...	10.0.0.132	30978	10.0.0.1	TCP	74	39578 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PER
2	2023-10-11 07:37:33.1874405...	10.0.0.132	34224	10.0.0.1	TCP	78	34224 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PER
3	2023-10-11 07:37:36.2328097...	10.0.0.132	34224	10.0.0.1	TCP	74	34224 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PER
4	2023-10-11 07:37:36.2328097...	10.0.0.132	34224	10.0.0.1	TCP	74	[TCP Retransmission] 34224 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PER
5	2023-10-11 07:37:43.452081...	10.0.0.132	31293	10.0.0.1	TCP	78	31293 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PER
6	2023-10-11 07:37:43.452081...	10.0.0.132	31293	10.0.0.1	TCP	74	[TCP Retransmission] 31293 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PER
7	2023-10-11 07:37:43.2631665...	10.0.0.132	41242	10.0.0.1	TCP	78	41242 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PER
8	2023-10-11 07:37:46.2534865...	10.0.0.132	41242	10.0.0.1	TCP	74	[TCP Retransmission] 41242 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PER
9	2023-10-11 07:37:49.3061296...	10.0.0.1	57621	10.0.0.1	UDP	86	57621 - 57621 Len=44
10	2023-10-11 07:37:52.3631836...	10.0.0.132	57621	10.0.0.1	UDP	86	57621 - 57621 Len=44
11	2023-10-11 07:37:57.6700484...	10.0.0.254	67	10.0.0.131	DHCP	342	DHCP ACK - Transaction ID 0x848d6234
12	2023-10-11 07:37:57.6700484...	10.0.0.254	59148	10.0.0.1	IP	68	59148 - 148 [TCP] Seq=0 Win=64240 Len=44
13	2023-10-11 07:37:58.5188773...	10.0.0.131	224.0.0.22	IGMPv3	68	Membership Report / Join group 224.0.0.251 For any source	
14	2023-10-11 07:37:58.5188773...	10.0.0.131	224.0.0.22	IGMPv3	68	Membership Report / Join group 224.0.0.252 For any source	
15	2023-10-11 07:37:58.5188773...	10.0.0.131	224.0.0.22	IGMPv3	68	Membership Report / Join group 224.0.0.253 For any source	
16	2023-10-11 07:37:58.5231965...	10.0.0.131	224.0.0.22	IGMPv3	68	Membership Report / Join group 224.0.0.254 For any source	
17	2023-10-11 07:37:58.5231965...	10.0.0.131	224.0.0.22	IGMPv3	68	Membership Report / Join group 224.0.0.255 For any source	
18	2023-10-11 07:37:58.5544383...	10.0.0.131	224.0.0.22	IGMPv3	68	Membership Report / Join group 224.0.0.252 For any source	
19	2023-10-11 07:37:58.5544383...	10.0.0.131	62447	224.0.0.252	LLN0	72	Standard query 62447 ANY Marketing-PC
20	2023-10-11 07:38:00.154739...	10.0.0.132	53140	10.0.0.1	TCP	78	53140 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PER
21	2023-10-11 07:38:00.265084...	10.0.0.132	53140	10.0.0.1	TCP	74	[TCP Retransmission] 53140 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PER
22	2023-10-11 07:38:00.4246605...	10.0.0.131	224.0.0.22	IGMPv3	68	Membership Report / Join group 239.250.255.256 For any source	
23	2023-10-11 07:38:01.054739...	10.0.0.131	224.0.0.22	IGMPv3	68	Membership Report / Join group 239.250.255.257 For any source	
24	2023-10-11 07:38:01.054739...	10.0.0.132	53140	10.0.0.1	TCP	74	[TCP Retransmission] 53140 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PER
25	2023-10-11 07:38:05.154739...	10.0.0.131	138	10.0.0.250	BROWSER	243	Host Announcement MARKETING-PC Workstation_Server_NT
26	2023-10-11 07:38:08.2656243...	10.0.0.132	30968	10.0.0.1	TCP	78	30968 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PER
27	2023-10-11 07:38:08.2656243...	10.0.0.132	30968	10.0.0.1	TCP	78	[TCP Retransmission] 30968 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PER
28	2023-10-11 07:38:09.2935297...	10.0.0.132	30968	10.0.0.1	TCP	74	[TCP Retransmission] 30968 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PER

Hasil analisis menunjukkan bahwa pelaku melakukan pivot ke Marketing-PC, pelaku menggunakan protokol LLMNR disaat berkomunikasi dengan host machine.

```
> Frame 19: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface eno33, id 0
Ethernet II Src: Vmware (00:0c:29:44:00:0f) Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Version: 2.0 (Ethernet II)
  Src MAC Address: 00:0c:29:44:00:0f (VMware)
  Dst MAC Address: ff:ff:ff:ff:ff:ff (Broadcast)
  Type: Internet Protocol Version 4 (IPv4) [0x0800]
  Version = Version: 4 (0x4)
  Header Length = 5 bytes (40 bits)
  Differentiated Services Field: 0x00 (DSFC: C0, ECN: Not-ECT)
  Total Length: 58
  Identification: 0x0000 (32380)
  ... .Flags = Flags: 0x00
  ... .0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x9f0 [validation disabled]
```

Tindakan Mitigasi



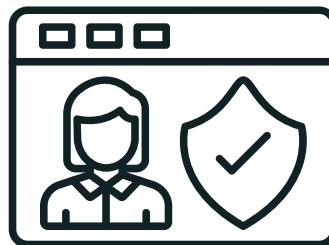
Isolasi Sistem Terpengaruh

Sales-PC dan Marketing-PC telah diisolasi dari jaringan untuk mencegah akses tidak sah lebih lanjut.



Reset Kredensial

Password untuk akun yang dikompromi (ssales) telah direset untuk mencegah akses tidak sah.



Pembatasan Akses Share Jaringan

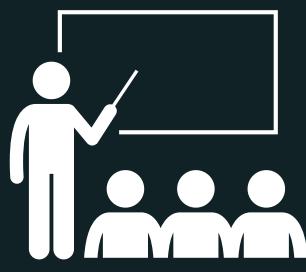
Akses ke share jaringan ADMIN\$ telah dibatasi hanya untuk personel yang diotorisasi.

Rekomendasi



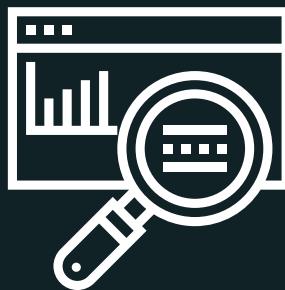
Audit Keamanan Rutin

Jadwalkan audit keamanan berkala untuk mengidentifikasi dan mengatasi kerentanan dalam jaringan.



Pelatihan Kesadaran Pengguna

Selenggarakan sesi pelatihan kesadaran keamanan siber secara teratur untuk mengedukasi pengguna tentang ancaman potensial dan taktik rekayasa sosial.



Pemantauan yang Ditingkatkan

Implementasikan SIEM untuk mendeteksi dan merespons aktivitas mencurigakan secara real-time.

Glosarium

SIEM (Security information and event management)

Solusi teknologi yang digunakan untuk mengumpulkan, menganalisis, dan mengelola informasi keamanan dari berbagai sumber di dalam suatu organisasi

PsExec

Alat atau utilitas yang dirancang untuk menjalankan perintah atau proses di jarak jauh pada komputer Windows.

LLMNR

Singkatan dari "Link-Local Multicast Name Resolution". Ini adalah protokol yang digunakan dalam jaringan komputer untuk mencari nama host lokal pada jaringan yang tidak memiliki layanan DNS (Domain Name System) yang terkonfigurasi. LLMNR dirancang sebagai alternatif untuk NetBIOS Name Resolution dan digunakan di lingkungan Windows.

IPC\$

Bagian dari mekanisme berbagi sumber daya yang dibangun di atas protokol SMB/CIFS (Server Message Block/Common Internet File System). Saat pengguna mengakses suatu komputer melalui jaringan, IPC\$ digunakan untuk melakukan proses otentifikasi dan berkomunikasi antarproses.

Lateral Movement

Serangkaian tindakan atau aktivitas yang dilakukan oleh penyerang setelah berhasil memasuki jaringan atau sistem komputer tertentu. Tujuan dari lateral movement adalah untuk memperluas kontrol penyerang atas jaringan atau infrastruktur yang diserang.

Backdoor

Sebuah pintu belakang (atau akses tersembunyi) yang sengaja ditempatkan di dalam perangkat lunak, sistem operasi, atau perangkat keras komputer untuk memberikan akses tidak sah atau tanpa izin. Backdoor dirancang untuk memungkinkan pihak tertentu, seringkali pembuat perangkat lunak atau sistem, untuk mengakses sistem atau data tanpa sepengetahuan pengguna atau pihak yang memiliki wewenang.

SMB2

Singkatan dari "Server Message Block 2", yang merupakan protokol jaringan yang digunakan dalam sistem operasi Windows. Ini adalah versi yang diperbarui dari protokol SMB yang lebih lama (SMB1). Protokol ini bertanggung jawab untuk berbagi file, pencetakan, dan layanan umum jaringan pada sistem operasi Windows.

Kesimpulan

Tanggapan cepat oleh tim jaringan telah berhasil mitigasi risiko segera yang terkait dengan kejadian ini. Namun, investigasi lebih lanjut disarankan untuk mengidentifikasi sejauh mana kompromi dan potensi eksfiltrasi data. Selain itu, menerapkan rekomendasi yang disarankan akan meningkatkan postur keamanan siber organisasi kami secara keseluruhan.

Insiden ini merupakan peringatan bahwa perusahaan perlu meningkatkan keamanan jaringannya. Perusahaan perlu melakukan langkah-langkah mitigasi untuk mencegah terjadinya insiden serupa di masa mendatang.

Sekian dan Terima kasih

Demikianlah laporan ini disusun sebagai langkah dalam menanggapi insiden pada jaringan perusahaan. Terima kasih atas kerja sama dan perhatian seluruh tim keamanan informasi dalam mengatasi serta mencegah potensi ancaman keamanan di masa mendatang.

