



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.

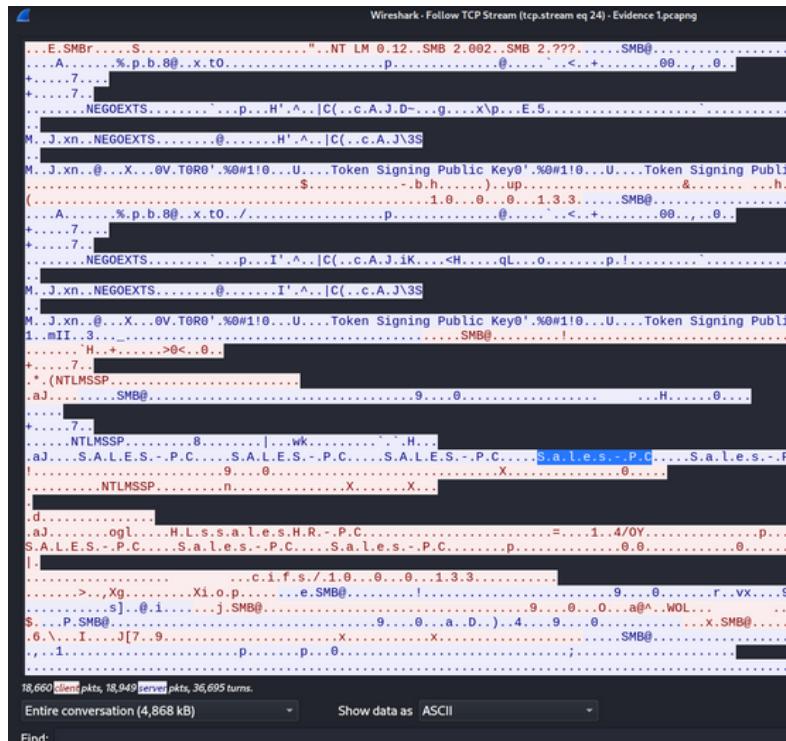
Penggunaan IPC\$ untuk komunikasi teramati.

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 IP/Destination	Destination	Protocol	Length	Info
10.0.0.130	49096	10.0.0.133	445	268	268 Negotiate Protocol Request
10.0.0.130	49096	10.0.0.133	445	229	229 Session Setup Request: NTLMSSP_NEGOTIATE
10.0.0.130	49096	10.0.0.133	445	995	995 Session Setup Request: NTLMSSP_NEGOTIATE_V2
10.0.0.130	49096	10.0.0.133	445	164	164 Tree Connect Request Tree: \\\10.0.0.133\IPC\$
10.0.0.130	49096	10.0.0.133	445	178	178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
10.0.0.130	49096	10.0.0.133	445	168	168 Tree Connect Request Tree: \\\10.0.0.133\ADMINS
10.0.0.130	49096	10.0.0.133	445	234	234 Ioctl Request FSCTL_SET_FILE_NETWORK_OPEN_INFO
10.0.0.130	49096	10.0.0.133	445	146	146 Close Request File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	382	382 Create Request File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	1514	1514 Write Request Len:65536 Off:0 File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	1514	1514 Write Request Len:65536 Off:204806 File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	578	578 Write Request Len:408 Off:2431644 File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	1509	1509 Create Request File: PSEXESVC.exe FILE_NETWORK_OPEN_INFO File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	146	146 Close Request File: PSEXESVC.exe
10.0.0.130	49096	10.0.0.133	445	494	494 Create Request File: PSEXEC-HR-PC-1C6C5014.key
10.0.0.130	49096	10.0.0.133	445	178	178 Write Request Len:0 Off:0 File: PSEXEC-HR-PC-1C6C5014.key
10.0.0.130	49096	10.0.0.133	445	194	194 Create Request File: PSEXESVC
10.0.0.130	49096	10.0.0.133	445	162	162 GetInfo Request FILE_INFO/MB2_FILE_STANDARD_INFO File: PSEXESVC
10.0.0.130	49096	10.0.0.133	445	739	739 IOCTL Request FSCTL_PIPE_TRANSCEIVE Standard: PSEXESVC
10.0.0.130	49096	10.0.0.133	445	158	158 Lease Break Acknowledgment
10.0.0.130	49096	10.0.0.133	445	162	162 GetInfo Request FILE_INFO/MB2_FILE_NETWORK_OPEN_INFO File: PSEXEC-HR-PC-1C6C5014.key
10.0.0.130	49096	10.0.0.133	445	145	145 Create Request File: PSEXEC-HR-PC-1C6C5014.key
10.0.0.130	49096	10.0.0.133	445	414	414 Create Request File: PSEXEC-HR-PC-1C6C5014.key
10.0.0.130	49096	10.0.0.133	445	174	174 Write Request Len:4 Off:0 File: PSEXESVC
10.0.0.130	49096	10.0.0.133	445	1465	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: PSEXESVC
SMB2	138 Write Response
SMB2	138 Write Response
SMB2	1514 Write Request Len:65536 Off:131072 File: PSEXESVC
SMB2	138 [TCP ACKed unseen segment] Write Response
SMB2	138 Write Response
SMB2	570 Write Request Len:400 Off:241664 File: PSEXESVC
SMB2	138 [TCP ACKed unseen segment] Write Response

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

```

0000 00 0c 29 59 23 50 00 0c 29 06 cc 75 6
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 6
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

```

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

```

129 2023-10-11 07:42:08.8617448. 10.0.0.130 49906 10.0.0.130 445 SMB2 400 Negotiate Protocol Request
130 2023-10-11 07:42:08.8617450. 10.0.0.130 49906 10.0.0.130 445 SMB2 234 Create Request File: PSEXESVC.exe
131 2023-10-11 07:42:08.8706974. 10.0.0.133 445 10.0.0.130 49906 SMB2 329 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_NEGOTIATE
132 2023-10-11 07:42:08.8701575. 10.0.0.130 49906 10.0.0.133 445 SMB2 505 Session Setup Request, NTLMSSP_AUTH, User: \sales
133 2023-10-11 07:42:08.8701577. 10.0.0.133 445 10.0.0.130 49906 SMB2 329 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_NEGOTIATE
134 2023-10-11 07:42:08.8827558. 10.0.0.130 49906 10.0.0.133 445 SMB2 164 Tree Connect Request Tree: \\10.0.0.133\IPC$
135 2023-10-11 07:42:08.8834814. 10.0.0.130 49906 10.0.0.133 445 SMB2 138 Tree Connect Response
136 2023-10-11 07:42:08.8834816. 10.0.0.130 49906 10.0.0.133 445 SMB2 378 Tree Connect Response
137 2023-10-11 07:42:08.8834813. 10.0.0.130 49906 10.0.0.133 445 SMB2 474 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
138 2023-10-11 07:42:08.8834815. 10.0.0.130 49906 10.0.0.133 445 SMB2 289 Create Request File: PSEXESVC.exe
139 2023-10-11 07:42:08.8834285. 10.0.0.130 49906 10.0.0.133 445 SMB2 138 Tree Connect Response
140 2023-10-11 07:42:08.8834287. 10.0.0.130 49906 10.0.0.133 445 SMB2 234 Create Request File: PSEXESVC.exe
141 2023-10-11 07:42:08.8834289. 10.0.0.130 49906 10.0.0.133 445 SMB2 329 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_NEGOTIATE
142 2023-10-11 07:42:08.8846716. 10.0.0.130 49906 10.0.0.133 445 SMB2 146 Close Request File:
143 2023-10-11 07:42:08.8846718. 10.0.0.130 49906 10.0.0.133 445 SMB2 146 Close Request File:
144 2023-10-11 07:42:08.8846720. 10.0.0.130 49906 10.0.0.133 445 SMB2 146 Close Request File:
145 2023-10-11 07:42:08.8846721. 10.0.0.130 49906 10.0.0.133 445 SMB2 419 Create Response File: PSEXESVC.exe
146 2023-10-11 07:42:08.8846723. 10.0.0.130 49906 10.0.0.133 445 TCP 1514 49906 -> 445 [ACK] Seq=4221 Ack=2685 Win=210504 Len=1440 [TCP segment of a re
147 2023-10-11 07:42:08.8846725. 10.0.0.130 49906 10.0.0.133 445 TCP 1514 49906 -> 445 [ACK] Seq=4281 Ack=2685 Win=210504 Len=1440 [TCP segment of a re
148 2023-10-11 07:42:08.8846727. 10.0.0.130 49906 10.0.0.133 445 TCP 1514 49906 -> 445 [ACK] Seq=4282 Ack=2685 Win=210504 Len=1440 [TCP segment of a re
149 2023-10-11 07:42:08.8846729. 10.0.0.130 49906 10.0.0.133 445 TCP 1514 49906 -> 445 [ACK] Seq=4283 Ack=2685 Win=210504 Len=1440 [TCP segment of a re
150 2023-10-11 07:42:08.8846766. 10.0.0.130 49906 10.0.0.133 445 SMB2 138 Tree Connect Request Tree: \\10.0.0.133\IPC$
```

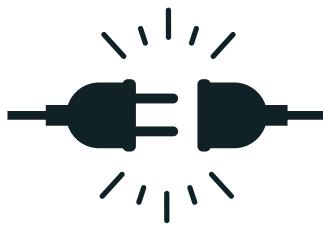
Hasil analisis dari log adalah Pelaku menggunakan Network Share ADMIN\$, terlihat dari saat awal pelaku meminta Tree Connect Request dan saat pelaku merequest file PSEXESVC.exe dalam tree id. Ini berarti pelaku menggunakan ADMIN\$ untuk menginstall service tersebut

NetworkMiner screenshot showing network traffic between two hosts. The traffic includes various SMB2 and TCP requests and responses, particularly focusing on the exchange of PSEXESVC.exe files and session setup requests.

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)

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

Tindakan Mitigasi



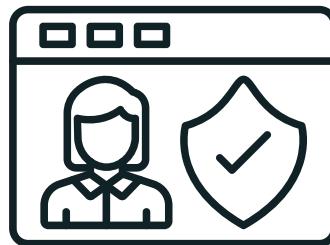
Isolasi Sistem Terpengaruh

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

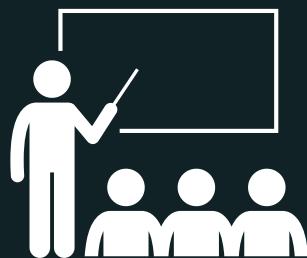
Akses ke share jaringan ADMIN\$ telah dibatasi hanya untuk personel yang diotorisasi.

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.

