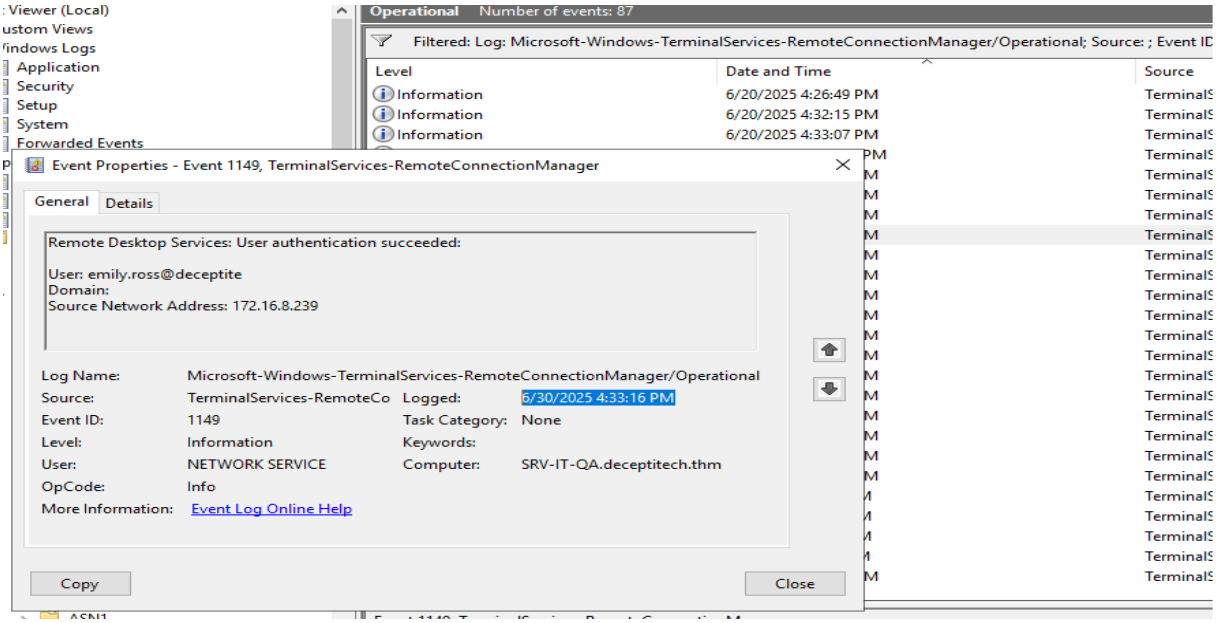
Elevating Movement

Here I am for investigate windows so this is the hard part for me

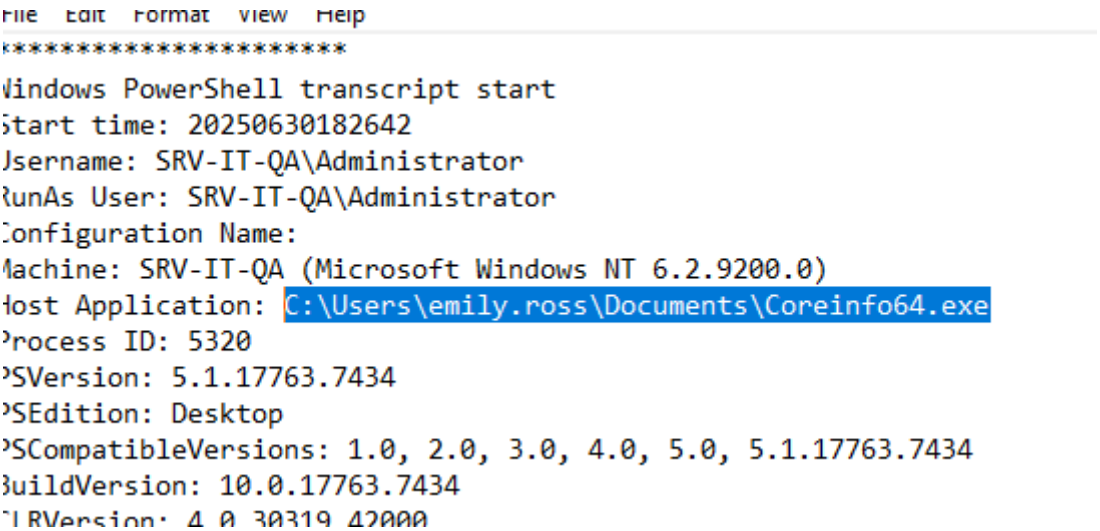
When did the attacker perform RDP login on the server?
Answer Format Example: 2025-01-15 19:30:45

To find this anwer I have tried nevigated on Windows security event id 4624 but I have encountered issue then a little searching I found the RDP login can be recorded in TerminalServices / RemoteConnectionManager Event ID 1149 so that I have filtered operational logins and behalf of emily rose I found the answer.



What is the full path to the binary that was replaced for persistence and privesc?

I had a difficulty to find this answer then after carefully navigation I thought that this is named privesc process so that administrator path may contain trick for the answer. So it happened I thought. I opened path “Users -> Administrators -> Documents ->20250630”



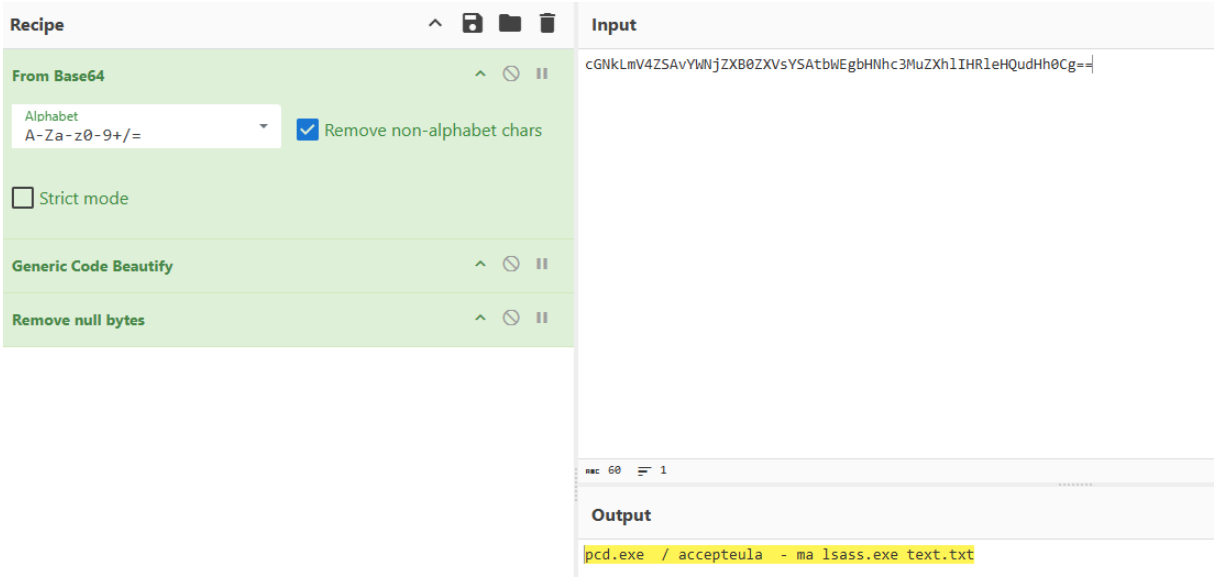
What is the type or malware family of the replaced binary?

Meterpreter is a sophisticated tool which is used to post exploitation. After the connect to computer it executes command, collect data and controlling on the system. So it is a shell which is hide himself and work silently. It works on RAM and It is not written on system disk.

Which full command line was used to dump the OS credentials?

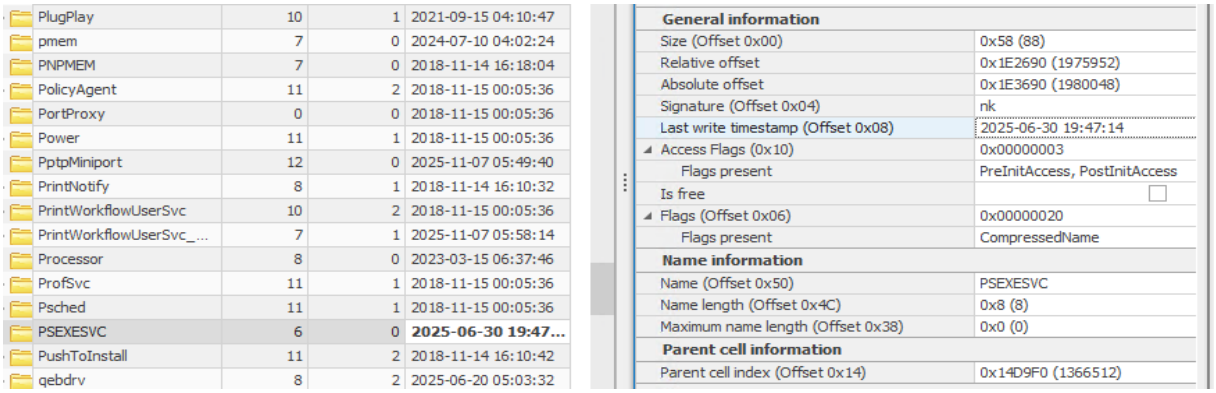
```
t]::FromBase64String("W01TRi5Qb3dlcnNoZWxsLk1ldGVycHJldGVyLkNvcmVdOjpTZXRJbnZvY2F0aW9uUG9pbn
```

```
t]::FromBase64String("cGNkLmV4ZSAvYWNjZXB0ZXVsYSAtbWEgbHNhc3MuZXhlIHRleHQudHh0Cg==")))
```



Using the stolen credentials, when did the attacker perform lateral movement?
Answer Format Example: 2025-01-15 19:30:45

To find this anwer we should look at C:\Windows\System32\config\SYSTEM\ is a hive file, stores so many registery keys. We can call it them as a data structure. Registry explorer is a viewer which is shows registry keys. We have focused on PSEXESVC because this one is indicator registry that is created temporary service on the target machine. Whenever service created or modified associated registry key updates itself.



PlugPlay	10	1	2021-09-15 04:10:47
pmem	7	0	2024-07-10 04:02:24
PNPMEM	7	0	2018-11-14 16:18:04
PolicyAgent	11	2	2018-11-15 00:05:36
PortProxy	0	0	2018-11-15 00:05:36
Power	11	1	2018-11-15 00:05:36
PptpMiniport	12	0	2025-11-07 05:49:40
PrintNotify	8	1	2018-11-14 16:10:32
PrintWorkflowUserSvc	10	2	2018-11-15 00:05:36
PrintWorkflowUserSvc_...	7	1	2025-11-07 05:58:14
Processor	8	0	2023-03-15 06:37:46
ProfSvc	11	1	2018-11-15 00:05:36
Psched	11	1	2018-11-15 00:05:36
PSEXESVC	6	0	**2025-06-30 19:47...**
PushToInstall	11	2	2018-11-14 16:10:42
qebdrv	8	2	2025-06-20 05:03:32

General information	
Size (Offset 0x00)	0x58 (88)
Relative offset	0x1E2690 (1975952)
Absolute offset	0x1E3690 (1980048)
Signature (Offset 0x04)	nk
Last write timestamp (Offset 0x08)	2025-06-30 19:47:14
Access Flags (0x10)	0x00000003
Flags present	PreInitAccess, PostInitAccess
Is free	☐
Flags (Offset 0x06)	0x00000020
Flags present	CompressedName
Name information	
Name (Offset 0x50)	PSEXESVC
Name length (Offset 0x4C)	0x8 (8)
Maximum name length (Offset 0x38)	0x0 (0)
Parent cell information	
Parent cell index (Offset 0x14)	0x14D9F0 (1366512)