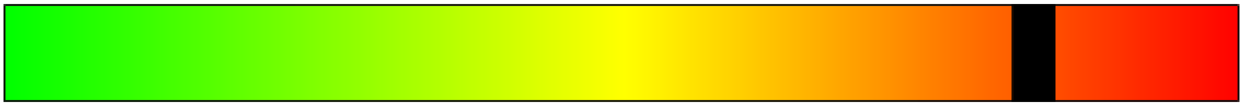
SOC Prime, Inc.

www.socprime.com

USA +1 888 484 7555
UK +44 203 769 3384
EU / INTL +370 655 57760

Threat Hunting Report for ACME Corp

Severity: High - Insider Threat / Red Team



Investigation Overview:

On 9/10/2022 at 22:00 UTC a newly created local account “Adminnistrator” was observed enumerating domain controllers and file shares. Based on preliminary analysis, physical access to the host is likely. Host logs stopped forwarding shortly after activity began.

Enumeration is typical of early adversary activity once they’ve established a foothold. Based on the likelihood of physical access to the host, we identify this as probable red team or insider threat activity.

[attachment containing logs]

Affected Host Information:

Hostname: DESKTOP-AAB2XJ
IP: 10.10.100.85
Domain: user.intranet.acme.example
Primary User SAM Account Name: longhornss
Primary User Name: Samantha Longhorn
Primary User Last Login: 9/20/2022 15:39 UTC

Timeline:

1. 9/20/2022 22:00 UTC: Account “Adminnistrator” is created on host DESKTOP-AAB2XJ a windows 10 host by the system account (DESKTOP-AAB2XJ$). The account is placed into the local administrators group.
2. 9/20/2022 22:04 UTC: Account “Adminnistrator” is logged into locally.
3. 9/20/2022 22:01 UTC: Account “Adminnistrator” uses Window’s utility nltest to enumerate ACME Corp domain controllers.
4. 9/20/2022 22:03 UTC: Account “Adminnistrator” runs the powershell cmdlet test-netconnection to test RDP access to domain controller acme-dc2.intranet.acme.example.
5. 9/20/2022 22:04 UTC: Account “DESKTOP-AAB2XJ$” accesses the SYSVOL and NETLOGON shares from acme-dc2.intranet.acme.example.
6. 9/20/2022 22:06 UTC: Machine account DESKTOP-AAB2XJ$ is observed pulling active directory information for domain administrators using powershell.
7. 9/20/2022 22:08 UTC: DESKTOP-AAB2XJ is observed as the source host attempting to anonymously connect to SMB file shares.
8. 9/20/2022 22:10 UTC: Logs stop forwarding from host

SOC Prime Activity:

1. Based on the severity of the incident, the emergency phone recall has been initiated for ACME Corp and the basic details have been forwarded in a less formal document at 9/20/2022 22:30 UTC. SOC Lead Jacob Smith was contacted at 9/20/2022 22:31 UTC.
    a. SOC Lead Jacob Smith was unable to confirm if a Red Team or Cyber Threat Emulation was scheduled at ACME.
2. A dashboard has been customized to monitor this account’s activity. Please check: splunk.intranet.acme.example/THA_001_Activity
3. Activity related to this account will be scoped and any new findings will be shared via addendums to this advisory.

Recommended Actions:

1. Validate attached logs.
2. Begin deconfliction of activity with CISO / CTO as possible red team indicators.
3. Identify host location within customer site and have building security check room & confirm serial that DESKTOP-AAB2XJ is at Samantha Longhorn’s desk.
4. Provide SOC Prime with notifications of valid account creation in the SIEM. This will enable us to provide further clarity and confidence in further hunting exercises.