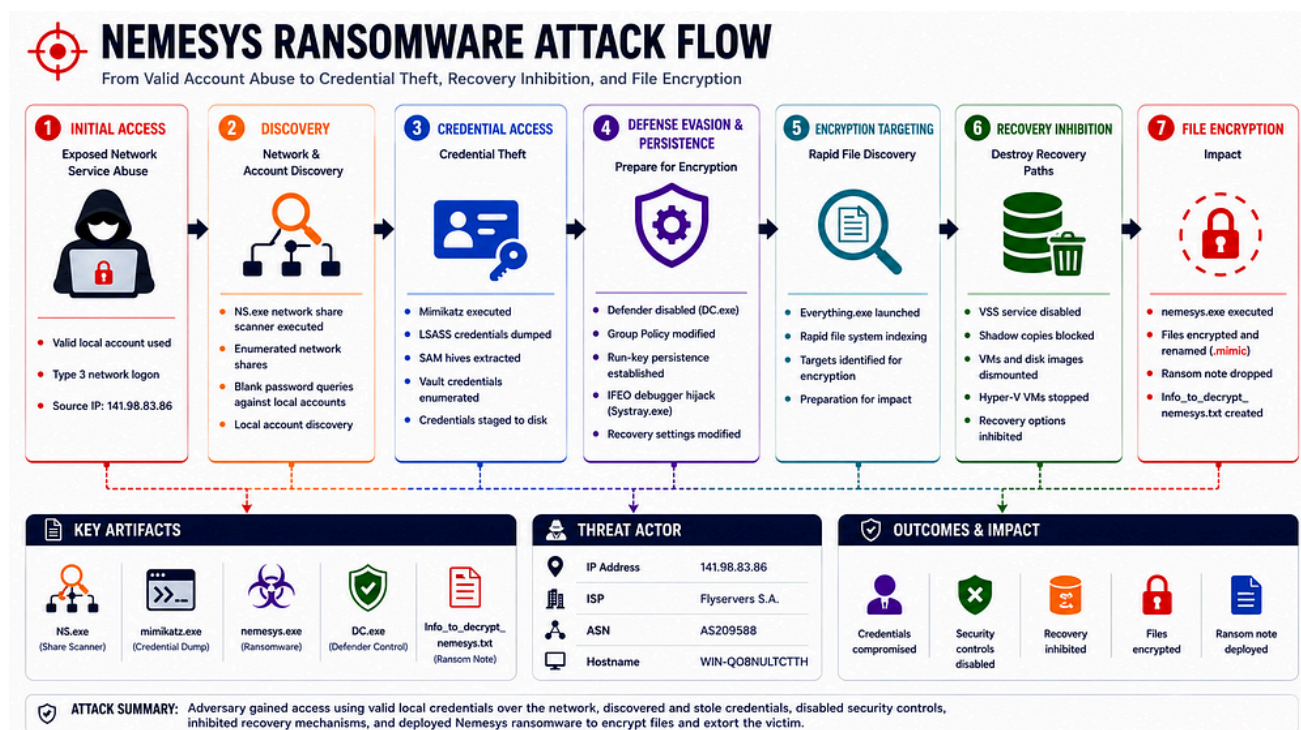


Inside a Nemesis Ransomware Deployment

medium.com/@shahzeb.m/inside-a-nemesis-ransomware-deployment-c3061ef3487e

Shahzeb M

June 3, 2026



Nemesis Ransomware Attack Flow

Ransomware-as-a-Service, so hot right now. This incident bears the hallmarks of Dharma and Phobos affiliated campaigns, groups that have been running the same playbook since 2016 and 2018, getting in through exposed remote services and leaving the same ransom note template behind. The whole thing went down in less time than it takes me to get out of bed on a Monday.

Here's what happened.

The Actor Already Had The Keys

On 2026-04-01 18:09:44 UTC a threat actor (WIN-Q08NULTCTTH) from Panama (141.98.83.86) logged into the web server using valid credentials for a local account. The logon was a Type 3, network authentication, with no failed attempts preceding it. A sweep of similar IPs revealed that an IP from the same ISP was logging in using local account credentials as early as 2026-02-18 across several devices, weeks before the ransomware deployed. The question isn't just how they got in. It's what may have been happening before someone pulled the trigger.

4624		141.98.83.86	WIN-Q08NULTCTTH
4624		141.98.83.86	WIN-Q08NULTCTTH

An All Too Familiar Toolkit

The automim1 toolkit landed on disk, mimikatz, LaZagne, and over 20 NirSoft tools, arriving pre-packaged. Credentials were dumped from LSASS and critical registry hives saved to the threat actor's staging directories.

CommandLine ↕

```
.\mimikatz\x64\mimikatz.exe "privilege::debug" "log .\!logs\Result.txt" "sekurlsa::logonPasswords"
"token::elevate" "lsadump::sam" exit
```

Credential Access, mimikatz.exe executing sekurlsa::logonPasswords and lsadump::sam

✓	CommandLine ↕
	reg.exe save hklm\sam c:\users\ [REDACTED] \appdata\local\temp\gxgmuwdadin
\\lazagne.exe	cmd.exe /c "reg.exe save hklm\sam c:\users\ [REDACTED] \appdata\local\temp\gxgmuwdadin"
	reg.exe save hklm\system c:\users\ [REDACTED] \appdata\local\temp\zmizrhjiqj
\\lazagne.exe	cmd.exe /c "reg.exe save hklm\system c:\users\ [REDACTED] \appdata\local\temp\zmizrhjiqj"
	reg.exe save hklm\security c:\users\ [REDACTED] \appdata\local\temp\rbdprytwx
\\lazagne.exe	cmd.exe /c "reg.exe save hklm\security c:\users\ [REDACTED] \appdata\local\temp\rbdprytwx"

Credential Access, reg.exe saving SAM, SYSTEM and SECURITY hives to Temp

Then the attacker opened Passwords.txt, NTLM.txt and Result.txt in Notepad, a manual review step confirming the harvest was complete before the ransomware triggered. Credential access was a separate objective here.

Persistence Before Detonation

Before nemesys.exe ran, a Run key was written to HKCU...\Run\nemesys pointing to a randomized AppData directory. nemesys.exe extracted a password-protected SFX archive and re-executed from the persistent AppData location via dllhost.exe.

TargetObject	Details
HKU\S-1-5-21-3772984715-3855048566-1297946058-1000\Software\Microsoft\Windows\CurrentVersion\RunNotification\nemesys	DWORD (0x00000001)
HKU\S-1-5-21-3772984715-3855048566-1297946058-1000\Software\Microsoft\Windows\CurrentVersion\Run\nemesys	"C:\Users\[REDACTED]\AppData\Local\1A0E4D54-2869-FFA5-37FD-1DF75A0FC5BA\nemesys.exe"

Persistence, Run key written to HKCU...\Run\nemesys

Defender Goes Down First

Join Medium for free to get updates from this writer.

Remember me for faster sign in

DC.exe disabled Defender, then re-ran as SYSTEM. Group Policy modified to enforce the changes network-wide. From this point on, the host was blind.

CommandLine	User	IntegrityLevel
"C:\Users\[REDACTED]\AppData\Local\1A0E4D54-2869-FFA5-37FD-1DF75A0FC5BA\DC.exe" /SYS 1	NT AUTHORITY\SYSTEM	System

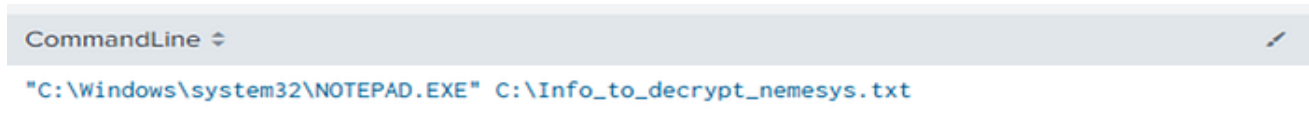
Defense Evasion, DC.exe disabling Windows Defender as SYSTEM

Everything.exe And The Encryption Run

Everything.exe launched for rapid file system indexing for encryption targeting. VSS was disabled, shadow copy recovery blocked. PowerShell dismounted all Hyper-V VMs and disk images. Clean shutdown and recovery prevented. SeTakeOwnershipPrivilege exercised 77 times by nemesys.exe, all successful.

TargetFilename	CommandLine
	C:\Windows\system32\cmd.exe /c cls
C:\Users\[REDACTED]\AppData\Local\Temp\2\3582-490\NS.exe	"C:\Users\[REDACTED]\AppData\Local\Temp\2\3582-490\NS.exe"
C:\Users\[REDACTED]\Videos\NS.exe	"C:\Users\[REDACTED]\Videos\NS.exe"

Discovery, NS.exe dropped and executed from Videos folder



Impact, Ransom note created and displayed in Notepad

The ransom note contains verbiage like that used in Dharma (CrySiS) and Phobos ransomware campaigns. Initial infection is typically through remote services abuse. These Ransomware-as-a-Service groups target healthcare, government and small businesses.

All your files have been encrypted!
Due to a security problem with your PC. If you want to restore them, write us to the e-mail: nemesys@onionmail.org
Write this ID in the title of your message
Your personal ID: 

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us.
After payment we will send you the tool that will decrypt all your files.
Free decryption as guarantee
Before paying you can send us up to 3 files for free decryption.
The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)
How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
<https://www.binance.com/en/how-to-buy/bitcoin>
Also you can find other places to buy Bitcoins and beginners guide here:
<http://www.coindesk.com/information/how-can-i-buy-bitcoins/>
Attention!
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Nemesys ransom note

```
1 All your files have been encrypted!
2 All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail moremo123123@
3 Write this ID in the title of your message [snip]
4 In case of no answer in 24 hours write us to these e-mails: moremo123123@cock.li
5 You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption too
6 Free decryption as guarantee
7 Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 10Mb (non archived), and files sh
8 How to obtain Bitcoins
9 The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method a
10 Also you can find other places to buy Bitcoins and beginners guide here: http://www.coindesk.com/information/how-can-i-buy-bitcoins/
11 Attention!
12 Do not rename encrypted files.
13 Do not try to decrypt your data using third party software, it may cause permanent data loss.
14 Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of
```

Dharma (CrySiS) ransom note, for comparison

Impact and Detection

A 30-day trend revealed that multiple accounts had interacted with malware hashes and filenames found during the incident. Files encrypted, credentials accessed, shadow copies blocked, no evidence of data exfiltration observed.

~ Dwell time: 3 minutes, 25 seconds.

To detect Dharma/Phobos ransomware activity in your environments, we highly suggest creating detection around behavioural access on LSASS & critical credential hives. It's also important to restrict network access to remote ports and network shares due to this being a common TTP of these threat actor groups. For further suggestions on how to detect & defend your environment against these attacks, reach out.

INDICATORS OF COMPROMISE	CD-NEMESYS-RANSOMWARE	TYPE	VALUE
--------------------------	-----------------------	------	-------