THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

NetWalker

Threat Actor Ransomware

CATEGORY

Ransomware

SEVERITY

High

Platforms

Windows, Linux

IMPACT

- Unauthorized Access to Information
- Extraction of Confidential Data
- Disclosure of Critical Details.
- Financial Losses

Description

NETWALKER

NetWalker is a ransomware group that emerged in late 2019 and is known for its sophisticated double extortion tactics. The group encrypts victim data and exfiltrates sensitive information, threatening to publicly release it if the ransom is not paid. Their operations involve infiltrating networks, escalating privileges, and deploying ransomware, often using tools like Mimikatz and legitimate software (LOLBINS) such as PSTools, AnyDesk, and NLBrute. They commonly exploit phishing campaigns and Remote Desktop Protocol (RDP) vulnerabilities for initial access. NetWalker has been linked to high-profile attacks, particularly targeting the healthcare and education sectors, and frequently leverages global events like the COVID-19 pandemic to increase their attack surface.

Operated by the threat actor "CIRCUS SPIDER," NetWalker is currently active in the Asia Pacific region, with a focus on critical sectors like healthcare. Similar to groups such as Maze and Egregor, they use advanced techniques and legitimate tools to evade detection. Indicators of their attacks include suspicious email attachments, unusual network traffic, and the presence of NetWalker executables. Recent campaigns show an increased reliance on phishing and RDP vulnerabilities, demonstrating the group’s adaptability and persistent threat to enterprise networks.

Kill Chain

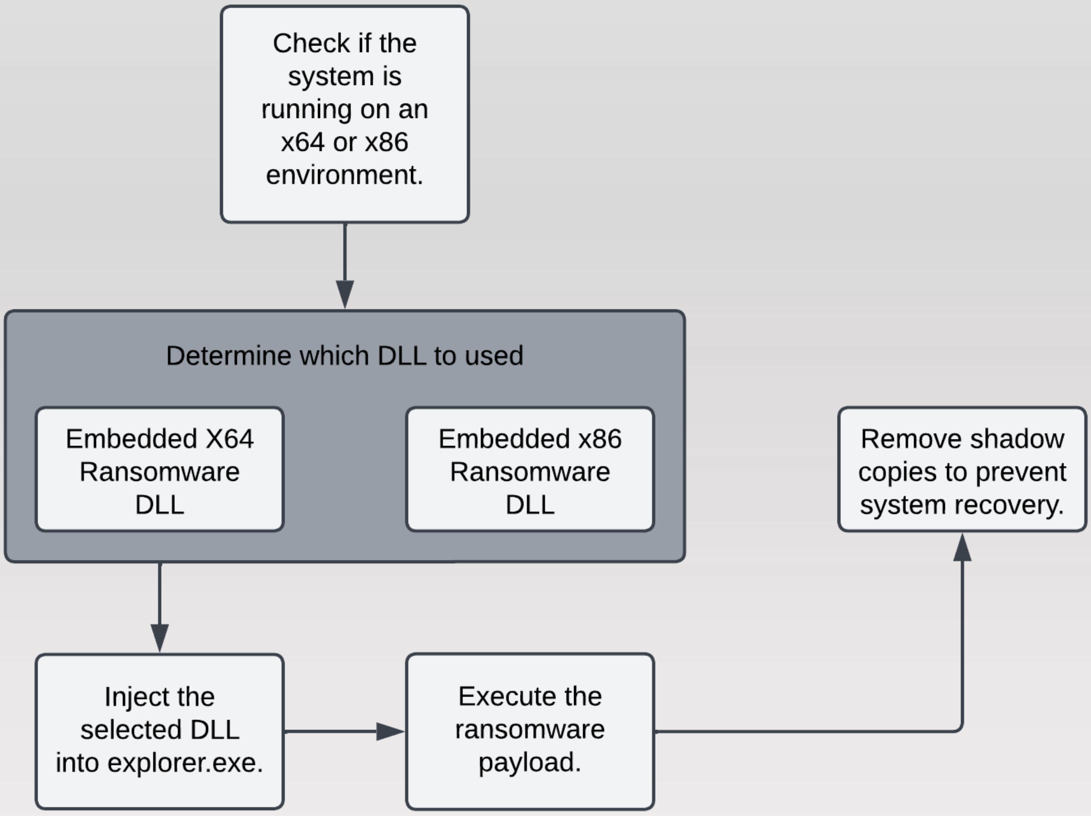
Check if the system is running on an x64 or x86 environment.
Determine which DLL to used
Embedded X64 Ransomware DLL
Embedded x86 Ransomware DLL
Remove shadow copies to prevent system recovery.
Inject the selected DLL into explorer.exe.
Execute the ransomware payload.

Figure 1 Kill Chain

Indicator of Compromise

SHA256

b2adf8ec7ab5193c7358f6acb30b003493466daee33ea416e3f703e744f73b7d
1c12ff296e7d9f90391e45f8a1d82d8140edf98d616a7da28741094d60d4779d
0bad18cb64b14a689965540126e0adbc952f090f1fb7b6447fe897a073860cdb
a8d350bbe8d9ccfbb0c3e9c2dd9251c957d18ce13ae405ceb2f2d087c115db15
e68dd7f20cd31309479ece3f1c8578c9f93c0a7154dcf21abce30e75b25da96b
2d07f0425dc465b3a1267a672c1293f9a3d0cd23106b7be490807fea490978ea

Indicator of Compromise

MD5

3fca66f91ecb3fd64655c10e22c4158b
4cc42763de2b6799f477054147023ba9
4e620b7ad2d7dc872bd42c25e876e153
5715ba9c7ee68a57e0caae883f62e011
e5abff4ad250cacc91335e47be4fcdc2
4164b6d8c0dc3bdbba3605d584a59ad1

Remediation

- **Patch and Secure Systems:** Regularly update software, close RDP vulnerabilities, and enforce multi-factor authentication (MFA).
- **Monitor and Detect Threats:** Use EDR tools, SIEM, and log monitoring to identify suspicious activities and potential breaches.
- **Incident Response Plan:** Develop, test, and implement a robust incident response plan to isolate and contain ransomware attacks.
- **Backup and Recovery:** Maintain encrypted offline backups and ensure a tested recovery process to restore data in case of an attack.

ThreatCure

Cyber Threat Advisory

Secure your byte world

NetWalker

Threat Actor Ransomware

Get Started Today

For more information about the ThreatCure ShieldOps Platform or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE