

Forum:[Hack Forums](#)

Thread: [New 'Curly COMrades' APT Using NGEN COM Hijacking in Georgia, Moldova Attacks](#)

Stanley - August 21, 2025, 10:55 pm

New 'Curly COMrades' APT Using NGEN COM Hijacking in Georgia, Moldova Attacks

A previously undocumented threat actor dubbed Curly COMrades has been observed targeting entities in Georgia and Moldova as part of a cyber espionage campaign designed to facilitate long-term access to target networks.

"They repeatedly tried to extract the NTDS database from domain controllers -- the primary repository for user password hashes and authentication data in a Windows network,"

<https://thehackernews.com/2025/08/new-curly-comrades-apt-using-ngen-com.html>

JoseMar - September 2, 2025, 8:57 am

(Aug 21, 2025 10:55 PM)Stanley Wrote: [\[CITE\]](#) New 'Curly COMrades' APT Using NGEN COM Hijacking in Georgia, Moldova Attacks

A previously undocumented threat actor dubbed Curly COMrades has been observed targeting entities in Georgia and Moldova as part of a cyber espionage campaign designed to facilitate long-term access to target networks.

"They repeatedly tried to extract the NTDS database from domain controllers -- the primary repository for user password hashes and authentication data in a Windows network,"

<https://thehackernews.com/2025/08/new-curly-comrades-apt-using-ngen-com.html>

They're really getting creative with the names, "Curly COMrades." Honestly, the way they hijack COM objects is pretty clever, in a scary way. It's like they're hiding in plain sight inside the system.

W1NK1LL3RX - September 2, 2025, 9:30 am

(Aug 21, 2025 10:55 PM)Stanley Wrote: [\[CITE\]](#) New 'Curly COMrades' APT Using NGEN COM Hijacking in Georgia, Moldova Attacks

A previously undocumented threat actor dubbed Curly COMrades has been observed targeting entities in Georgia and Moldova as part of a cyber espionage campaign designed to facilitate long-term access to target networks.

"They repeatedly tried to extract the NTDS database from domain controllers -- the primary repository for user password hashes and authentication data in a Windows network,"

<https://thehackernews.com/2025/08/new-curly-comrades-apt-using-ngen-com.html>

That's wild. Sounds like a really advanced group if they're going after domain controllers and password hashes. Definitely not the kind of attack you'd want slipping under the radar.

sharn - September 14, 2025, 11:12 am

Dumping NTDS and LSASS shows they want full access.

They are after credentials, not just files.

plops - September 14, 2025, 1:45 pm

Wow they really are going after long term access of many cred.

