

PeterM 🌻 on X: "For IR people #RagnarLocker using <https://t.co/KLITtyID8P> for exfiltration. Persistence: Cobalt/ScreenConnect, Lateral Movement: Cobalt/RDP, Discovery: Advanced IP Scanner, Collection: Winrar. Large amounts of data taken (TB's) in exfil. Ransom notes include links to screenshots. <https://t.co/2Irg4dUq3E>" / X

Published: 2021-06-12 · Archived: 2026-04-05 18:32:48 UTC

Don't miss what's happening

People on X are the first to know.

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly.

Post

Conversation

For IR people [#RagnarLocker](#) using handybackup.net for exfiltration. Persistence: Cobalt/ScreenConnect, Lateral Movement: Cobalt/RDP, Discovery: Advanced IP Scanner, Collection: Winrar. Large amounts of data taken (TB's) in exfil. Ransom notes include links to screenshots.

C:\Users**<REDACTED>**\Downloads\backup.exe

C:\Program Files\Handy Backup 8\HandyBackupNetworkCoordinator8.exe

C:\Program Files\Handy Backup 8\HandyBackupNotifyService8.exe

C:\Program Files\Handy Backup 8\HandyBackupServer8.exe

C:\Program Files\Handy Backup 8\HandyBackup8.exe

C:\Program Files\Handy Backup 8\ws64\HandyBackupWorkstation8.exe

Type	Date	Time	Event	Source	Category	User
Information			1040	MsiInstaller	None	

Desktop Beginning a Windows Installer transaction: C:\Users**<REDACTED>**\AppData\Local\Temp\Handy Backup x64 (Release) 8.2.4.15 2021.05.17.20.58 NOVOSOFT.msi. Client Process Id: 3904.

New to X?

Sign up now to get your own personalized timeline!

Something went wrong. Try reloading.

Source: <https://twitter.com/AltShiftPrtScn/status/1403707430765273095>