PeterM🌻 on X: "For IR people #RagnarLocker using https://t.co/KLITtylD8P 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

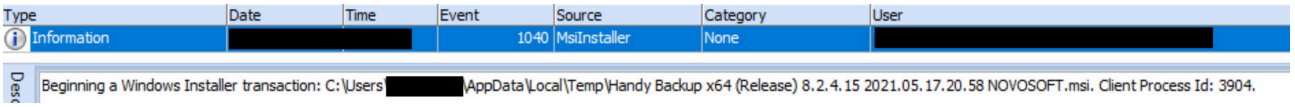
Published: 2021-06-12 · Archived: 2026-04-05 18:32:48 UTC

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



New to X?

Sign up now to get your own personalized timeline!

Something went wrong. Try reloading.
