Data from Network Shared Drive, Technique T1039 - Enterprise

Archived: 2026-04-02 12:02:45 UTC

ID	Name	Description
G0007	APT28	APT28 has collected files from network shared drives.[1]
S0128	BADNEWS	When it first starts, BADNEWS crawls the victim's mapped drives and collects documents with the following extensions: .doc, .docx, .pdf, .ppt, .pptx, and .txt.[2]
G0060	BRONZE BUTLER	BRONZE BUTLER has exfiltrated files stolen from file shares.[3]
C0015	C0015	During C0015, the threat actors collected files from network shared drives prior to network encryption.[4]
G0114	Chimera	Chimera has collected data of interest from network shares.[5]
S0050	CosmicDuke	CosmicDuke steals user files from network shared drives with file extensions and keywords that match a predefined list.[6]
S0554	Egregor	Egregor can collect any files found in the enumerated drivers before sending it to its C2 channel.[7]
G0117	Fox Kitten	Fox Kitten has searched network shares to access sensitive documents.[8]
G0047	Gamaredon Group	Gamaredon Group malware has collected Microsoft Office documents from mapped network drives.[9][10]

ID	Name	Description
G0045	menuPass	menuPass has collected data from remote systems by mounting network shares with `net use` and using Robocopy to transfer data.[11]
S0458	Ramsay	Ramsay can collect data from network drives and stage it for exfiltration.[12]
G1039	RedCurl	RedCurl has collected data about network drives.[13][14]
G0054	Sowbug	Sowbug extracted Word documents from a file server on a victim network.[15]

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Source: https://attack.mitre.org/techniques/T1039