FLASHFLOOD, Software S0036 | MITRE ATT&CK®

Archived: 2026-04-05 15:03:03 UTC

Domain	ID		Name	Use
Enterprise	T1560	.003	Archive Collected Data: Archive via Custom Method	FLASHFLOOD employs the same encoding scheme as SPACESHIP for data it stages. Data is compressed with zlib, and bytes are rotated four times before being XOR'ed with 0x23.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	FLASHFLOOD achieves persistence by making an entry in the Registry's Run key.[1]
Enterprise	T1005		Data from Local System	FLASHFLOOD searches for interesting files (either a default or customized set of file extensions) on the local system. FLASHFLOOD will scan the My Recent Documents, Desktop, Temporary Internet Files, and TEMP directories. FLASHFLOOD also collects information stored in the Windows Address Book.[1]
Enterprise	T1025		Data from Removable Media	FLASHFLOOD searches for interesting files (either a default or customized set of file extensions) on removable media and copies them to a staging area. The default file types copied would include data copied to the drive by SPACESHIP.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	FLASHFLOOD stages data it copies from the local system or removable drives in the "%WINDIR%\$NtUninstallKB885884$\" directory.[1]

Domain	ID	Name	Use
Enterprise	T1083	File and Directory Discovery	FLASHFLOOD searches for interesting files (either a default or customized set of file extensions) on the local system and removable media.[1]

Source: https://attack.mitre.org/software/S0036/