ObliqueRAT, Software S0644 | MITRE ATT&CK®

Archived: 2026-04-05 13:05:31 UTC

Domain	ID		Name	Use
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	ObliqueRAT can gain persistence by a creating a shortcut in the infected user's Startup directory.[1]
Enterprise	T1025		Data from Removable Media	ObliqueRAT has the ability to extract data from removable devices connected to the endpoint.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	ObliqueRAT can copy specific files, webcam captures, and screenshots to local directories.[1]
Enterprise	T1030		Data Transfer Size Limits	ObliqueRAT can break large files of interest into smaller chunks to prepare them for exfiltration.[1]
Enterprise	T1083		File and Directory Discovery	ObliqueRAT has the ability to recursively enumerate files on an infected endpoint.[1]
Enterprise	T1027	.003	Obfuscated Files or Information: Steganography	ObliqueRAT can hide its payload in BMP images hosted on compromised websites.[1]
Enterprise	T1120		Peripheral Device Discovery	ObliqueRAT can discover pluggable/removable drives to extract files from.[1]

Domain	ID		Name	Use
Enterprise	T1057		Process Discovery	ObliqueRAT can check for blocklisted process names on a compromised host.[1]
Enterprise	T1113		Screen Capture	ObliqueRAT can capture a screenshot of the current screen.[1]
Enterprise	T1082		System Information Discovery	ObliqueRAT has the ability to check for blocklisted computer names on infected endpoints.[1]
Enterprise	T1033		System Owner/User Discovery	ObliqueRAT can check for blocklisted usernames on infected endpoints.[1]
Enterprise	T1204	.001	User Execution: Malicious Link	ObliqueRAT has gained execution on targeted systems through luring users to click on links to malicious URLs.[1][2]
Enterprise	T1125		Video Capture	ObliqueRAT can capture images from webcams on compromised hosts.[1]
Enterprise	T1497	.001	Virtualization/Sandbox Evasion: System Checks	ObliqueRAT can halt execution if it identifies processes belonging to virtual machine software or analysis tools.[1]