Olympic Destroyer, Software S0365 | MITRE ATT&CK®

Archived: 2026-04-05 17:00:52 UTC

Domain	ID		Name	Use
Enterprise	T1555	.003	Credentials from Password Stores: Credentials from Web Browsers	Olympic Destroyer contains a module that tries to obtain stored credentials from web browsers.[1]
Enterprise	T1485		Data Destruction	Olympic Destroyer overwrites files locally and on remote shares.[1][2]
Enterprise	T1070	.001	Indicator Removal: Clear Windows Event Logs	Olympic Destroyer will attempt to clear the System and Security event logs using `wevtutil`. [1]
Enterprise	T1490		Inhibit System Recovery	Olympic Destroyer uses the native Windows utilities `vssadmin`, `wbadmin`, and `bcdedit` to delete and disable operating system recovery features such as the Windows backup catalog and Windows Automatic Repair.[1]
Enterprise	T1570		Lateral Tool Transfer	Olympic Destroyer attempts to copy itself to remote machines on the network.[1]
Enterprise	T1135		Network Share Discovery	Olympic Destroyer will attempt to enumerate mapped network shares to later attempt to wipe all files on those shares.[1]
Enterprise	T1003	.001	OS Credential Dumping: LSASS Memory	Olympic Destroyer contains a module that tries to obtain credentials from LSASS, similar to Mimikatz. These credentials are used with PsExec and Windows Management Instrumentation to

Domain	ID		Name	Use
				help the malware propagate itself across a network.[1]
Enterprise	T1021	.002	Remote Services: SMB/Windows Admin Shares	Olympic Destroyer uses PsExec to interact with the `ADMIN$` network share to execute commands on remote systems.[1][3]
Enterprise	T1018		Remote System Discovery	Olympic Destroyer uses Windows Management Instrumentation to enumerate all systems in the network.[1]
Enterprise	T1489		Service Stop	Olympic Destroyer uses the API call `ChangeServiceConfigW` to disable all services on the affected system.[1]
Enterprise	T1016		System Network Configuration Discovery	Olympic Destroyer uses API calls to enumerate the infected system's ARP table.[1]
Enterprise	T1569	.002	System Services: Service Execution	Olympic Destroyer utilizes PsExec to help propagate itself across a network.[1]
Enterprise	T1529		System Shutdown/Reboot	Olympic Destroyer will shut down the compromised system after it is done modifying system configuration settings.[1][2]
Enterprise	T1047		Windows Management Instrumentation	Olympic Destroyer uses WMI to help propagate itself across a network.[1]

Source: https://attack.mitre.org/software/S0365/