BlackByte 2.0 Ransomware, Software S1181

Archived: 2026-04-05 13:00:48 UTC

Domain	ID		Name	Use
Enterprise	T1486		Data Encrypted for Impact	BlackByte 2.0 Ransomware is a ransomware variant associated with BlackByte operations.[1]
Enterprise	T1068		Exploitation for Privilege Escalation	BlackByte 2.0 Ransomware exploits a vulnerability in the RTCore64.sys driver (CVE-2019-16098) to enable privilege escalation and defense evasion when run as a service.[1]
Enterprise	T1562	.004	Impair Defenses: Disable or Modify System Firewall	BlackByte 2.0 Ransomware modifies the Windows firewall during execution.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	BlackByte 2.0 Ransomware deletes itself following device encryption.[1]
		.006	Indicator Removal: Timestomp	BlackByte 2.0 Ransomware can timestomp files for defense evasion and anti-forensics purposes.[1]
Enterprise	T1490		Inhibit System Recovery	BlackByte 2.0 Ransomware modifies volume shadow copies during execution in a way that destroys them on the victim machine.[1]
Enterprise	T1112		Modify Registry	BlackByte 2.0 Ransomware modifies the victim Registry to allow for elevated execution.[1]
Enterprise	T1135		Network Share Discovery	BlackByte 2.0 Ransomware can identify network shares connected to the victim machine.[1]

Domain	ID		Name	Use
Enterprise	T1055		Process Injection	BlackByte 2.0 Ransomware injects into a newly-created `svchost.exe` process prior to device encryption.[1]
Enterprise	T1489		Service Stop	BlackByte 2.0 Ransomware can terminate running services.[1]
Enterprise	T1569	.002	System Services: Service Execution	BlackByte 2.0 Ransomware executes as a service when deployed.[1]

Source: https://attack.mitre.org/software/S1181