Royal, Software S1073 | MITRE ATT&CK®

Archived: 2026-04-05 17:47:36 UTC

Domain	ID		Name	Use
Enterprise	T1059	.012	Command and Scripting Interpreter: Hypervisor CLI	Royal ransomware uses `esxcli` to gather a list of running VMs and terminate them.[4]
Enterprise	T1486		Data Encrypted for Impact	Royal uses a multi-threaded encryption process that can partially encrypt targeted files with the OpenSSL library and the AES256 algorithm.[2][3][4]
Enterprise	T1083		File and Directory Discovery	Royal can identify specific files and directories to exclude from the encryption process.[2][3][4]
Enterprise	T1490		Inhibit System Recovery	Royal can delete shadow copy backups with vssadmin.exe using the command `delete shadows /all /quiet`.[2][3][5]
Enterprise	T1680		Local Storage Discovery	Royal can use `GetLogicalDrives` to enumerate logical drives.[2][4]
Enterprise	T1106		Native API	Royal can use multiple APIs for discovery, communication, and execution.[2]
Enterprise	T1046		Network Service Discovery	Royal can scan the network interfaces of targeted systems.[2]
Enterprise	T1135		Network Share Discovery	Royal can enumerate the shared resources of a given IP addresses using the API call `NetShareEnum`.[2]

Domain	ID		Name	Use
Enterprise	T1095		Non-Application Layer Protocol	Royal establishes a TCP socket for C2 communication using the API `WSASocketW`.[2]
Enterprise	T1566		Phishing	Royal has been spread through the use of phishing campaigns including "call back phishing" where victims are lured into calling a number provided through email.[2][3][5]
Enterprise	T1057		Process Discovery	Royal can use `GetCurrentProcess` to enumerate processes.[2]
Enterprise	T1021	.002	Remote Services: SMB/Windows Admin Shares	Royal can use SMB to connect to move laterally.[2]
Enterprise	T1489		Service Stop	Royal can use `RmShutDown` to kill applications and services using the resources that are targeted for encryption.[2]
Enterprise	T1082		System Information Discovery	Royal can use `GetNativeSystemInfo` to enumerate system processors.[2][4]
Enterprise	T1016		System Network Configuration Discovery	Royal can enumerate IP addresses using `GetIpAddrTable`.[2]

Source: https://attack.mitre.org/software/S1073