Dire Wolf Ransomware: Summary of TTPs

Tactic / Technique	Description	MITRE ATT&CK IDs
Double Extortion Model	Encrypts files and exfiltrates sensitive data; threatens public leak site exposure if ransom not paid.	T1486 – Data Encrypted for Impact, T1657 – Exfiltration to Threaten/Leak
Advanced Encryption	Uses Curve25519 and ChaCha20 algorithms for robust encryption, complicating recovery.	T1486 – Data Encrypted for Impact
Malware Development	Written in Golang, packed with UPX to hinder reverse engineering and static analysis.	T1027.002 – Software Packing
Anti-Forensics: Disable Logs/Backups	Disables Windows event logs, deletes backups and shadow copies.	T1562.002 – Impair Defenses: Disable Windows Event Logging, T1490 – Inhibit System Recovery
Anti-Forensics: Process Termination	Terminates security, admin, and productivity processes to disrupt response.	T1562.001 – Impair Defenses: Disable or Modify Tools, T1489 – Service Stop
Anti-Forensics: Mutex & Self-Delete	Uses mutexes to prevent multiple execution; self-deletes to reduce forensic footprint.	T1070.004 – Indicator Removal: File Deletion, T1480 – Execution Guardrails
Negotiation & Communication	Custom ransom notes with qTox IDs for chat; proof of exfiltration shown to victims.	T1491.001 – Internal Defacement: Ransom Notes, T1071.003 – Application Layer Protocol: qTox, T1041 – Exfiltration Over C2 Channel
Infrastructure: Tor Leak Site	Data leak site hosted on Tor; onion routing for anonymity and resilience.	T1048.003 – Exfiltration Over Unencrypted Non-C2 Protocol, T1090.003 – Proxy: Tor

Initial Access: Phishing	Likely phishing campaigns with malicious attachments or links.	T1566 – Phishing
Initial Access: VPN Exploits	Exploitation of public-facing vulnerabilities (e.g., Ivanti Connect Secure).	T1190 – Exploit Public-Facing Application
Initial Access: Credential Theft	Use of stolen credentials for access.	T1078 – Valid Accounts
Initial Access: Remote Services	Remote lateral movement using RDP, SMB, PsExec.	T1021 – Remote Services, T1021.002 – SMB/Service Execution (PsExec)
Initial Access: Living-off-the-Land	PowerShell, WMI, PsExec for lateral movement and execution.	T1059.001 – PowerShell, T1047 – Windows Management Instrumentation
Initial Access: Social Engineering	Malicious domains (e.g., tor-browser.io), possible AI-enhanced phishing/vishing.	T1598 – Phishing for Information, T1598.004 – Voice Phishing
Credential Dumping	Use of Mimikatz for privilege escalation and lateral movement.	T1003.001 – LSASS Memory
Living-off-the-Land	Abuse of legitimate system tools to evade detection.	T1059 – Command and Scripting Interpreter, T1078 – Valid Accounts
Process Termination	Aggressive termination of processes to maximize impact.	T1489 – Service Stop
Triple Extortion (Potential)	Possible escalation to DDoS or regulatory/media pressure beyond encryption and leaks.	T1498 – Network Denial of Service, T1657 – Exfiltration to Threaten/Leak