Dridex, Software S0384 | MITRE ATT&CK®

Archived: 2026-04-05 12:56:51 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Dridex has used POST requests and HTTPS for C2 communications.[2][4]
Enterprise	T1185		Browser Session Hijacking	Dridex can perform browser attacks via web injects to steal information such as credentials, certificates, and cookies.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Dridex has encrypted traffic with RC4.[2]
		.002	Encrypted Channel: Asymmetric Cryptography	Dridex has encrypted traffic with RSA.[2]
Enterprise	T1574	.001	Hijack Execution Flow: DLL	Dridex can abuse legitimate Windows executables to side-load malicious DLL files.[5]
Enterprise	T1106		Native API	Dridex has used the `OutputDebugStringW` function to avoid malware analysis as part of its anti-debugging technique.[4]
Enterprise	T1027		Obfuscated Files or Information	Dridex's strings are obfuscated using RC4.[4]
Enterprise	T1090		Proxy	Dridex contains a backconnect module for tunneling network traffic through a victim's computer. Infected computers become part of a P2P botnet that can relay C2 traffic to other infected peers.[1][4]

Domain	ID		Name	Use
		.003	Multi-hop Proxy	Dridex can use multiple layers of proxy servers to hide terminal nodes in its infrastructure.[4]
Enterprise	T1219		Remote Access Tools	Dridex contains a module for VNC.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Dridex can maintain persistence via the creation of scheduled tasks within system directories such as `windows\system32\` , `windows\syswow64,` `winnt\system32` , and `winnt\syswow64` .[5]
Enterprise	T1518		Software Discovery	Dridex has collected a list of installed software on the system.[4]
Enterprise	T1218	.010	System Binary Proxy Execution: Regsvr32	Dridex can use `regsvr32.exe` to initiate malicious code.[5]
Enterprise	T1082		System Information Discovery	Dridex has collected the computer name and OS architecture information from the system.[4]
Enterprise	T1204	.002	User Execution: Malicious File	Dridex has relied upon users clicking on a malicious attachment delivered through spearphishing.[4]
