DRATzarus, Software S0694 | MITRE ATT&CK®

Archived: 2026-04-05 14:03:13 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	DRATzarus can use HTTP or HTTPS for C2 communications.[1]
Enterprise	T1005		Data from Local System	DRATzarus can collect information from a compromised host.[1]
Enterprise	T1622		Debugger Evasion	DRATzarus can use `IsDebuggerPresent` to detect whether a debugger is present on a victim.[1]
Enterprise	T1105		Ingress Tool Transfer	DRATzarus can deploy additional tools onto an infected machine.[1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	DRATzarus has been named `Flash.exe`, and its dropper has been named `IExplorer`.[1]
Enterprise	T1106		Native API	DRATzarus can use various API calls to see if it is running in a sandbox.[1]
Enterprise	T1027		Obfuscated Files or Information	DRATzarus can be partly encrypted with XOR.[1]
		.002	Software Packing	DRATzarus's dropper can be packed with UPX.[1]
Enterprise	T1057		Process Discovery	DRATzarus can enumerate and examine running processes to determine if a debugger is

Domain	ID		Name	Use
				present.[1]
Enterprise	T1018		Remote System Discovery	DRATzarus can search for other machines connected to compromised host and attempt to map the network.[1]
Enterprise	T1033		System Owner/User Discovery	DRATzarus can obtain a list of users from an infected machine.[1]
Enterprise	T1124		System Time Discovery	DRATzarus can use the `GetTickCount` and `GetSystemTimeAsFileTime` API calls to inspect system time.[1]
Enterprise	T1497	.003	Virtualization/Sandbox Evasion: Time Based Checks	DRATzarus can use the `GetTickCount` and `GetSystemTimeAsFileTime` API calls to measure function timing.[1] DRATzarus can also remotely shut down into sleep mode under specific conditions to evade detection.[1]

Source: https://attack.mitre.org/software/S0694