Poseidon Group, Group G0033 | MITRE ATT&CK®

Archived: 2026-04-05 16:15:34 UTC

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	Poseidon Group searches for administrator accounts on both the local victim machine and the network.[1]
		.002	Account Discovery: Domain Account	Poseidon Group searches for administrator accounts on both the local victim machine and the network.[1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	The Poseidon Group's Information Gathering Tool (IGT) includes PowerShell components. [1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	Poseidon Group tools attempt to spoof anti-virus processes as a means of self-defense.[1]
Enterprise	T1003		OS Credential Dumping	Poseidon Group conducts credential dumping on victims, with a focus on obtaining credentials belonging to domain and database servers.[1]
Enterprise	T1057		Process Discovery	After compromising a victim, Poseidon Group lists all running processes.[1]
Enterprise	T1049		System Network Connections Discovery	Poseidon Group obtains and saves information about victim network interfaces and addresses. [1]

Domain	ID	Name	Use
Enterprise	T1007	System Service Discovery	After compromising a victim, Poseidon Group discovers all running services.[1]

Source: https://attack.mitre.org/groups/G0033