Axiom, Group 72, Group G0001

Archived: 2026-04-05 16:49:53 UTC

Domain	ID		Name	Use
Enterprise	T1583	.002	Acquire Infrastructure: DNS Server	Axiom has acquired dynamic DNS services for use in the targeting of intended victims.[5]
		.003	Acquire Infrastructure: Virtual Private Server	Axiom has used VPS hosting providers in targeting of intended victims.[5]
Enterprise	T1560		Archive Collected Data	Axiom has compressed and encrypted data prior to exfiltration.[5]
Enterprise	T1584	.005	Compromise Infrastructure: Botnet	Axiom has used large groups of compromised machines for use as proxy nodes.[5]
Enterprise	T1005		Data from Local System	Axiom has collected data from a compromised network.[5]
Enterprise	T1001	.002	Data Obfuscation: Steganography	Axiom has used steganography to hide its C2 communications.[5]
Enterprise	T1189		Drive-by Compromise	Axiom has used watering hole attacks to gain access.[4]
Enterprise	T1546	.008	Event Triggered Execution: Accessibility Features	Axiom actors have been known to use the Sticky Keys replacement within RDP sessions to obtain persistence.[5]

Domain	ID		Name	Use
Enterprise	T1190		Exploit Public-Facing Application	Axiom has been observed using SQL injection to gain access to systems.[5][4]
Enterprise	T1203		Exploitation for Client Execution	Axiom has used exploits for multiple vulnerabilities including CVE-2014-0322, CVE-2012-4792, CVE-2012-1889, and CVE-2013-3893.[4]
Enterprise	T1003		OS Credential Dumping	Axiom has been known to dump credentials.[5]
Enterprise	T1566		Phishing	Axiom has used spear phishing to initially compromise victims.[4][5]
Enterprise	T1563	.002	Remote Service Session Hijacking: RDP Hijacking	Axiom has targeted victims with remote administration tools including RDP.[5]
Enterprise	T1021	.001	Remote Services: Remote Desktop Protocol	Axiom has used RDP during operations.[5]
Enterprise	T1553		Subvert Trust Controls	Axiom has used digital certificates to deliver malware.[5]
Enterprise	T1078		Valid Accounts	Axiom has used previously compromised administrative accounts to escalate privileges.[5]