Indian Critical Infrastructure Intrusions, Campaign C0043

Archived: 2026-04-02 12:01:55 UTC

Domain	ID		Name	Use
Enterprise	T1583	.001	Acquire Infrastructure: Domains	During Indian Critical Infrastructure Intrusions, RedEcho registered domains spoofing Indian critical infrastructure entities.[1]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	During Indian Critical Infrastructure Intrusions, RedEcho network activity included SSL traffic over TCP 443 and HTTP traffic over non-standard ports.[1]
Enterprise	T1584		Compromise Infrastructure	Indian Critical Infrastructure Intrusions included the use of compromised infrastructure, such as DVR and IP camera devices, for command and control purposes in ShadowPad activity.[2]
Enterprise	T1568		Dynamic Resolution	During Indian Critical Infrastructure Intrusions, RedEcho used dynamic DNS domains associated with malicious infrastructure.[1]
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	During Indian Critical Infrastructure Intrusions, RedEcho used SSL for network communication.[1]
Enterprise	T1599		Network Boundary Bridging	Indian Critical Infrastructure Intrusions involved the use of FRP to bridge network boundaries and overcome NAT.[2] Indian Critical Infrastructure Intrusions also involved the use of VPN tunnels with a potentially compromised MSP entity allowing for direct access to critical infrastructure entity networks.[3]

Domain	ID		Name	Use
Enterprise	T1571		Non-Standard Port	During Indian Critical Infrastructure Intrusions, RedEcho used non-standard ports such as TCP 8080 for HTTP communication.[1]
Enterprise	T1588	.004	Obtain Capabilities: Digital Certificates	Indian Critical Infrastructure Intrusions included the use of digital certificates spoofing Microsoft.[2]

Source: https://attack.mitre.org/campaigns/C0043