Registry System Threat Analysis

(Last updated: 2014-10-23 by Gavin Brown)

System/Asset	Threat	Source	Severity	Frequency	Score	Mitigation
Authoritative DNS System	Denial of service	Hacktivists, vandals, blackmailers, hostile governments, criminals	3	2	6	Over-provision query handling capacity so that attack traffic doesn't block legitimate traffic Deploy Anycast to provide geographic traffic load balancing and isolation Use third party DDoS mitigation services Filtering at network edge to prevent attack traffic from reaching core infrastructure Surveillance to detect and prevent potential attacks Maintain good communications links with anti-abuse and infrastructure security organisations
Zone File Data	Unauthorized access	Spammers, identity thieves, criminals	1	3	3	Use VPN to secure zone data transfers to prevent tampering Enforce access restrictions on archived zone files to prevent leakage Use NSEC3 on signed zones to prevent enumeration Secure FTP interface for authorised access as normal FTP is insecure and can be intercepted Intrusion detection on servers and network devices to provide early warning and rapid response
	Unauthorized alteration	Hacktivists, vandals, governments, criminals	3	1	3	Use TSIG to sign zone transfers to prevent tampering Perform checks on zone data for consistency among servers to detect tampering Intrusion detection on servers and network devices to provide early warning and rapid response
DNSSEC Key Data	Unauthorized access	Hacktivists, vandals, blackmailers, hostile governments, criminals	3	1	3	Store keys in HSMs to prevent unauthorised access even if attacker has physical access Offline signing rather than online signing using isolated hardware so keys aren't held in "shallow" locations Physical isolation of signing equipment to prevent remote intrusion
	Denial of service	Hacktivists, vandals, blackmailers	3	1	3	Back up key data, store securely at multiple sites to provide multiple backups to restore from Standby signer available if primary system fails or is compromised to ensure continuity
Registry Database	Unauthorized access	Spammers, fraudsters, identity thieves, criminals, hostile governments	2	1	2	Protect Whois server from dictionary attacks by rate limiting and blocking query sources Restrict SRS access SRS access to trusted hosts/networks Secure core registry database Ensure all backups are encrypted before leaving database system Restrict and monitor all access to registrar and administrator consoles

System/Asset	Threat	Source	Severity	Frequency	Score	Mitigation
						Intrusion detection on servers and network devices to provide early warning and rapid response
	Unauthorized alteration	Identity thieves, vandals, domain hijackers	2	1	2	Restrict SRS access to trusted hosts/networks Enforce mutual client/server authentication in EPP using SSL certificates Secure core registry database Ensure all backups are encrypted before leaving database system Restrict and monitor all access to registrar and administrator consoles Intrusion detection on servers and network devices to provide early warning and rapid response
Shared Registry System	Unauthorized access	Identity thieves, vandals, domain hijackers	2	1	2	Restrict SRS access to trusted hosts/networks Enforce mutual client/server authentication in EPP using SSL certificates Intrusion detection on servers and network devices to provide early warning and rapid response
	Denial of service	Hacktivists, vandals	2	1	2	Restrict SRS access to trusted hosts/networks Intrusion detection on servers and network devices to provide early warning and rapid response
Registry Infrastructure	Unauthorized access	Hacktivists, vandals	3	1	3	Global firewall system to cover primary operations centre, all remote sites secured with local firewalls Access policy for remote administration Restrict and monitor access to administrator accounts on servers and network equipment Ensure security-related software updates are applied promptly
	Denial of service	Hacktivists, vandals	3	1	3	Physically separate non-related components to avoid shared fate Filtering at network edge to prevent attack traffic from reaching core infrastructure Redundant network connectivity to provide agility and additional upstream transit Surveillance to detect and prevent potential attacks Intrusion detection on servers and network devices to provide early warning and rapid response