Battlecard.

Diamond IP DNS Security Solutions.

Secure your DNS, secure your network.

Defend DNS from attack or misuse.

Attacks on DNS can effectively bring down a network. Attacks that rely on DNS leverage its implicit freedom in traversing firewalls to contact command and control centers or to exfiltrate data.

DNS has proven extremely effective and scalable in practice. Most people take DNS for granted given this and its proven reliability. However, its essential function and decentralized architecture serve to attract attackers seeking to exploit the architecture and rich data store for sinister activities.

Attacks on DNS infrastructure.

Attackers may target DNS servers in and of themselves in order to stifle communications or to steer unwitting end users to imposter web servers or other destinations. The familiar Denial of Service (DOS) or distributed DOS (DDOS) attack is invoked by an attacker to flood the DNS server with bogus DNS requests, overwhelming its ability to process legitimate DNS queries. Pseudo-random subdomain (PRSD) attacks attempt to deny recursive DNS services typically on service provider networks to hamper performance for their subscribers.

Host or server attacks are likewise sometimes attempted in order to disrupt the DNS resolution process or to manipulate DNS data. DNS data could also be manipulated through other means such as resolver attacks, cache poisoning, and authoritative data manipulation.

Network attacks using DNS

DNS may serve as a facilitator for use with the scope of a broader network attack. Just as DNS enables users to connect to websites by resolving text-based destinations to IP addresses, it enables attacker malware to locate command and control centers (CCC) or to tunnel information through firewalls. DNS by its nature also openly publishes potentially useful targeting information about networks, host names and IP addresses for would-be attackers.

Reflector and amplification style attacks are a form of denial of service attack by initiating several queries spoofing the target host's IP address; the host receives several often large DNS response packets which overwhelm it.

Advanced Persistent Threats (APTs) are malware which persist once within a target network by stealthily performing attacks and reprogramming itself based on instructions from its CCC. Such attacks may include denial of service, network disruption, data exfiltration, or other illicit activities.

Why BT Diamond IP?

BT Diamond IP can help you defend your DNS and defend your network. BT Diamond IP was recently ranked number two in DDI (DNS/DHCP/IPAM) market share over the last two years by IDC, a leading analyst firm: "BT Diamond leveraged many years of IP resource management innovation while also being attuned to 3rd Platform trends." We have introduced numerous industry and product innovations over our two decades of DDI experience and offer the following competitive advantages:

- Complete IPAM - BT Diamond IP offers complete IPAM automation from root block to individual IP assignment, DHCP and DNS – for other systems, IPAM is clearly an afterthought
- Hierarchical topology - Our patented container feature provides logical, hierarchical, automated IP allocation – unlike others' smart folders which are merely directory folders
- Automation - We provide site templates support for multi-subnet allocations with one click, e.g., for new branch office – Others only permit multiple same-size block splits from the same parent block (aka network container)
- Less cost and complexity - BT Diamond IP offers a single integrated solution – one GUI, one "master" appliance – for IPAM/DDI, discovery, switch port mapping, reporting, all functions – unlike others who require additional appliances and licenses for discovery, reporting, Microsoft support, DNS firewall, cloud automation, GeoDNS and more
- Flexibility - BT Diamond IP is the only vendor with a comprehensive offering from maximum flexibility with software, appliances, virtual, and managed services
- Inventory assurance - Our unique planned vs. actual discrepancy highlighting with selective import for IPs, blocks, pools and multi-sample based reclaim
- Configurability - BT Diamond IP supports full ISC/BIND configuration including all conf/view/zone options and RRTypes – Others support a rigid subset of options and RRTypes
- Scalability - our solutions manage among the largest IP networks on Earth – other "multi-grid" solutions hinder some features available in a single grid
- Multi- administrator controls - BT Diamond IP offers unmatched administrator policy granularity and tiered delegation (assignable roles)

Battlecard.

Diamond IP DNS Security Solutions.

BT Diamond IP DNS Security Feature Summary

BT Diamond IP offers a comprehensive solution to enable you automate DDI processes and secure your network. The following table summarizes key DNS and network threats along with corresponding mitigation approaches you can implement using the BT Diamond IP solution.

Threat		Threat Summary	Diamond IP Mitigation Approaches
Denial of Service	Denial of service	Attacker transmits a high volume of TCP, UDP, DNS or other packets to the DNS server to inundate its resources	• Inbound rate limiting • Anycast deployment
	Distributed denial of service	Attacker transmits a high volume of TCP, UDP, DNS or other packets from multiple sources to the DNS server to inundate its resources	• Inbound rate limiting • Anycast deployment
	Bogus queries	Attacker transmits a high volume of bogus queries, causing the recursive server to futilely locate authoritative servers	• Limit outstanding queries per client
Cache Poisoning	Packet Interception/ Spoofing	Attacker transmits a DNS response to a recursive DNS server in order to poison its cache, affecting DNS resolution integrity for	• DNSSEC validation on caching servers with automated trust anchor management • Source port and XID randomization • ACLs – allow-query, allow-query-on, allow-query-cache, allow-query-cache-on, allow-recursion, allow-recursion-on • Response integrity verification
	ID Guessing/ Query Prediction	Attacker transmits a DNS response(s) to a predicted query using a predicted or variety of XID values.	• DNSSEC validation on caching servers with automated trust anchor management • Source port and XID randomization • Response integrity verification
	Kaminsky Attack/ Name Chaining	Attacker transmits a DNS response(s) with falsified answers in the DNS message Additional section. The Kaminsky attack produces deterministic queries to facilitate the attack.	• DNSSEC validation on caching servers with automated trust anchor management
Authoritative Poisoning	Illicit dynamic update	Attacker transmits a DNS Update message(s) to a master DNS server to add, modify or delete a resource record in the target zone	• Use ACLs on allow-update, allow-notify, notify-source. • ACLs can also be defined as requiring transaction signatures for added origin authentication
	Server attack/hijack	Attacker hacks into the DNS server which enables manipulation of DNS data among other server capabilities	• Implement host access controls • Use hidden masters • Hardened Sapphire OS • Jailed DNS services • Require SSH authentication • Limit port or console access • Apply security patches
	DNS service misconfiguration	Vulnerability to configuration errors exposes the DNS service to improper configuration	• IPControl DNS error checking • Use checkzone and checkconf utilities • Data backups for reload if needed

Battlecard.

Diamond IP DNS Security Solutions.

	Threat	Threat Summary	Diamond IP Mitigation Approaches
Server/OS Attack	Buffer overflows and OS level attacks	Attacker exploits server operating system vulnerability	• Hardened Sapphire operating system • Apply security patches
	Control channel attack	Attacker accesses the DNS service control channel to disrupt DNS service	• Control channel ACLs • Control channel keyed authentication
	DNS service vulnerabilities	Attacker exploits DNS service vulnerability	• Apply security patches • Do not expose DNS service version to version queries
Resolver/host attacks	Recursive DNS redirection	Attacker misconfigures resolver to point to illicit recursive DNS server	• Configure resolver DNS servers via DHCP • Monitor for rogue DHCP servers • Periodically audit each client for misconfigurations or anomalies
	Resolver Configuration Attack	Attacker hacks into the device which enables manipulation of resolver configuration among other device capabilities	• Implement host access controls • Apply security patches
Network Reconnaissance	Name guessing	Attacker issues legitimate DNS queries for names that, if resolved could serve as further attack target	• Avoid naming hosts with overly “attractive” names
	Illicit zone transfer	Attacker initiates a zone transfer request to an authoritative DNS server to obtain zone resource records to identify potential attack targets	• Use ACLs with TSIG on allow-transfer; and use transfer-source IP address and port to use a non-standard port for zone transfers
Reflector style attacks	Reflector attacks	Attacker spoofs the target’s IP address and issues numerous queries to one or more authoritative DNS servers to inundate the target	• Implement ingress filtering on routers to mitigate spoofing • Use DNS response rate limiting
	Amplification attacks	Attacker amplifies reflector attack by querying for “large” resource records to increase data flow to target per query	• Implement ingress filtering on routers to mitigate spoofing • Use DNS response rate limiting
Data exfiltration	DNS tunneling	Attacker transmits data through firewalls using DNS as the transport protocol	• Monitor DNS queries for frequent queries between a given client and server especially with large query and response payload
	Resource locator	Attacker infects internal device which uses DNS to locate command and control center	• DNS firewall using BT’s DNS firewall subscription feed
APT	Advanced Persistent Threats	Attacker deploys adaptable malware within a network to perform nefarious functions to disrupt communications and/or steal information	• DNS firewall using BT’s DNS firewall subscription feed

Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc’s respective standard conditions of contract. Nothing in this publication forms any part of any contract. Registered office: 81 Newgate Street, London EC1A 7AJ. Registered in England No: 1800000

Find out more at:

1-610-321-9000 www.diamondipam.com