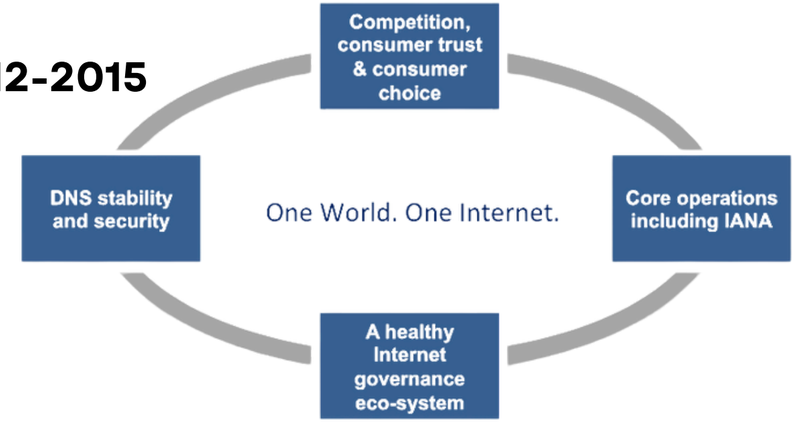
NextGen@ICANN84

Attacks on Network Infrastructure & Threat Intelligence

Shashi Raj - Master's Student, Cybersecurity
National Forensic Sciences University

Why this is Serious?

2012-2015



INTRODUCTION | OVERVIEW OF PLAN STRUCTURE | ICANN'S MISSION & 2030 VISION | STRATEGIC OBJECTIVES | STRATEGIC PLANNING PROCESS

Strategic Objective 4:

Strengthen the Stability and Security of the Internet's Unique Identifier Systems

Given the Internet's pivotal role in communication, commerce, and collaboration, strengthening the security of the Internet's identifier systems is paramount in preserving trust in the DNS. ICANN aims to enhance coordination with DNS stakeholders to raise awareness of threats and promote innovative approaches to address challenges effectively. Taking action requires coordinated efforts to identify and mitigate security threats and combat abuse. Promoting global adoption of open Internet standards and increasing security threat awareness among stakeholders are crucial steps toward strengthening the security and stability of Internet infrastructure. It is a collective responsibility for all stakeholders to ensure the Internet's unique identifier systems remain robust.

The following strategic goals and associated strategies are designed to achieve this strategic objective:

4.1 **Strengthen Partnerships with Relevant Stakeholders to Reinforce the Shared Responsibility of Ensuring Secure and Stable Internet's Unique Identifier Systems.**	4.1.1 Continue to provide and participate in trusted forums that convene relevant stakeholders. 4.1.2 Identify and mitigate security threats to the Internet's unique identifier systems. 4.1.3 Increase ICANN's coordination and collaboration with the numbers community for secure, stable, and resilient numbering and routing systems.
4.2 **Strengthen DNS Root Server System.**	4.2.1 Continue to enhance the governance and technical evolution of DNS root server operations and services. 4.2.2 Increase the robustness of the root zone generation, distribution services, and processes. 4.2.3 Support coordinated plans to address DNS Root Server System attacks.

2026-2030

CURRENT THREAT LANDSCAPE 2025

Critical Statistics - Q1 2025

- 20.5 million DDoS attacks blocked (358% YoY increase)
- 1.5 million DNS-specific attacks in Q1 2024
- 87% of organizations experienced DNS attacks in 2024
- 25.1% of 100.8M new domains classified malicious/suspicious
- $950,000 average cost per DNS attack globally
- 82% of DNS attacks result in application outages
- 29% lead to data theft

Infrastructure Abuse Scale:

- 10,000+ domains renting subdomains via Dynamic DNS
- 45+ malware families using DNS for C2 communications
- 700+ hyper-volumetric attacks exceeding 1 Tbps

What is Happening:

ACTIVE THREAT CAMPAIGNS

These alarming statistics highlight the escalating scale and sophistication of DNS-based threats in 2025, emphasizing the critical need for robust detection and mitigation strategies to protect global internet infrastructure against widespread cyberattacks, application outages, and data breaches. The rapid increase in both volumetric attacks and malicious domain activities underscores the evolving threat landscape that cybersecurity professionals and organizations must urgently address.

01

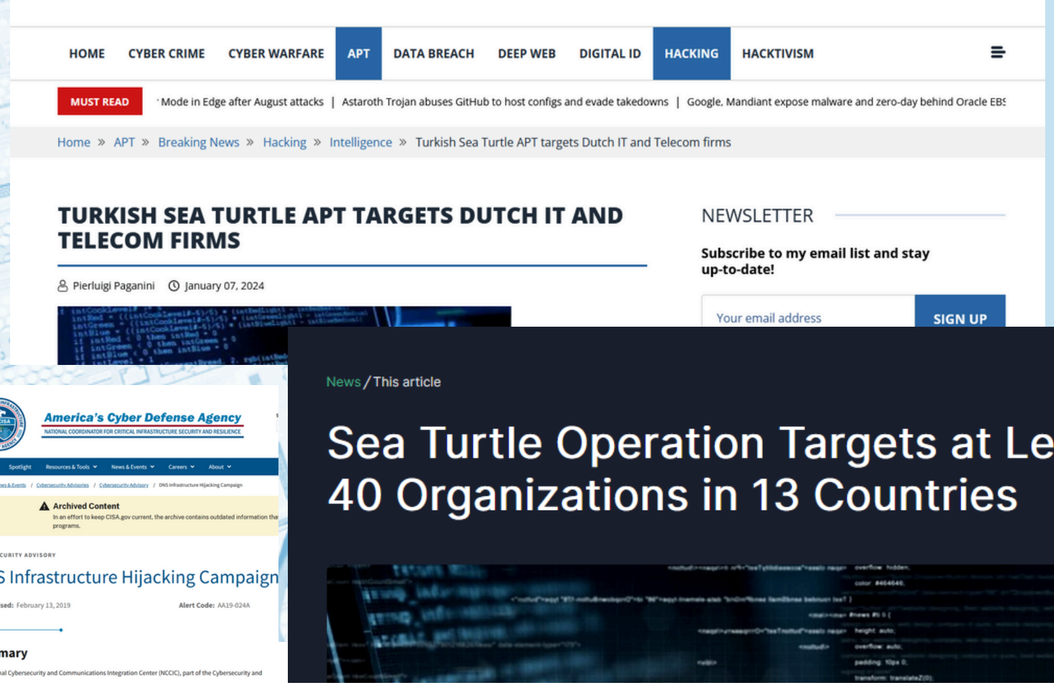
1. Mandiant Global DNS Hijacking Campaign

02

2. Dynamic DNS Provider Exploitation

03

3. DNS Tunneling Operations (8NS Campaign)



APT GROUP INTELLIGENCE

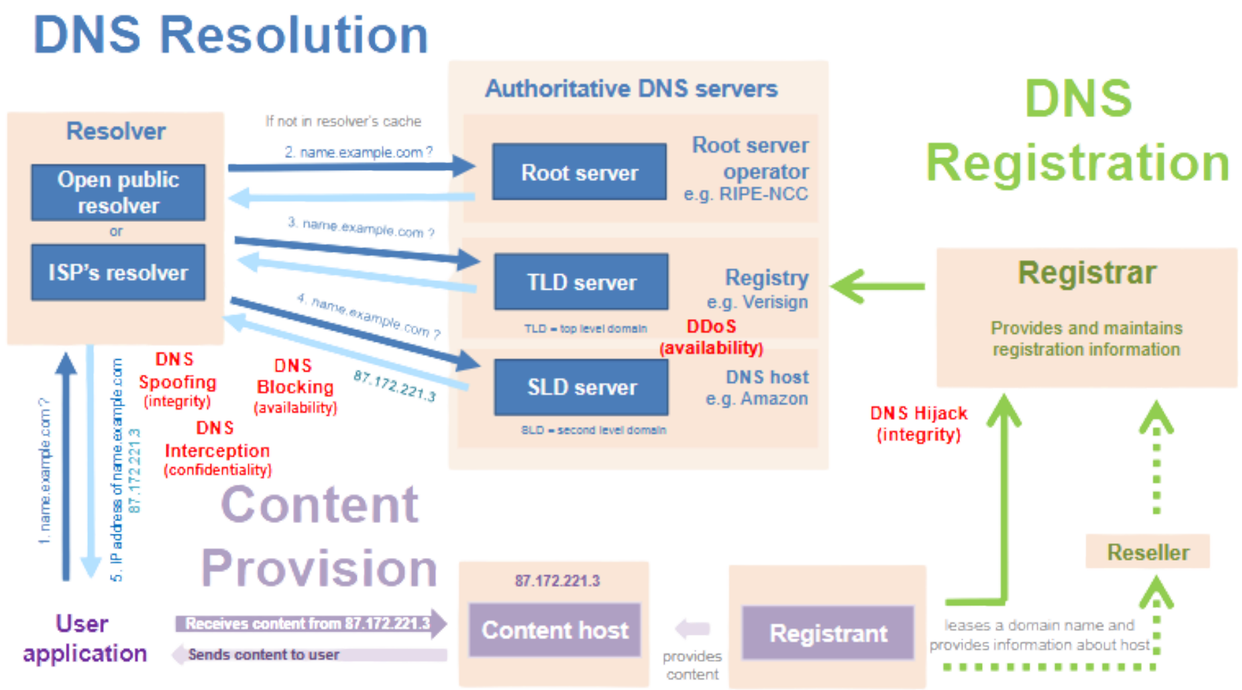
APT29 (Cozy Bear) - Russia
- Activity Level: HIGH
- DNS TTPs: Exclusive Dynamic DNS for QUIETEXIT C2
- Timeline: Active since 2022
- Focus: Government & critical infrastructure

APT28 (Fancy Bear) - Russia
- Activity Level: HIGH
- Evidence: Heavy Dynamic DNS usage (2024 FBI report)
- Recent: Eastern European government targeting

Scattered Spider - Cybercriminal
- Activity Level: HIGH
- Recent: January 2025 operations documented
- TTPs: Social engineering + DNS abuse

Sea Turtle - Turkey
- Activity Level: MODERATE (Evolved)
- Scale: 40+ orgs compromised, 13 countries
- Evolution: Shifted to SnappyTCP reverse shells (2025)

Hows its works



Note: This high-level overview does not intend to be exhaustive, but rather to provide a simplified picture of potential incidents in the DNS ecosystem. In fact, every relationship between DNS actors (represented by an arrow) can be subject to digital security incidents.
Dotted lines represent alternative or optional paths.
Source: OECD

Reference:
[OECD-DNS-2022] OECD report – Security of the Domain Name System (2022, PDF)
[Google-Cloud/Mandiant] Global DNS Hijacking Campaign – Google Cloud blog (Mandiant research)

TECHNICAL ATTACK ANALYSIS

DNS A Record Manipulation

1. Compromise DNS provider credentials
2. Alter A record (mail.victim.com → attacker IP)
3. Deploy proxy with load balancer
4. Generate Let's Encrypt certificates
5. Harvest credentials via MitM

DNS NS Record Hijacking

1. Compromise domain registrar/ccTLD
2. Change nameserver records to attacker-controlled
3. Selective response logic (malicious for targets, legitimate for others)
4. Certificate generation for hijacked domains

DNS Redirector Implementation

1. Deploy custom DNS server
2. Return attacker IPs for victim domains
3. Forward legitimate queries (stealth)
4. Sophisticated filtering to avoid detection

MITRE ATT&CK FRAMEWORK MAPPING

How to Map

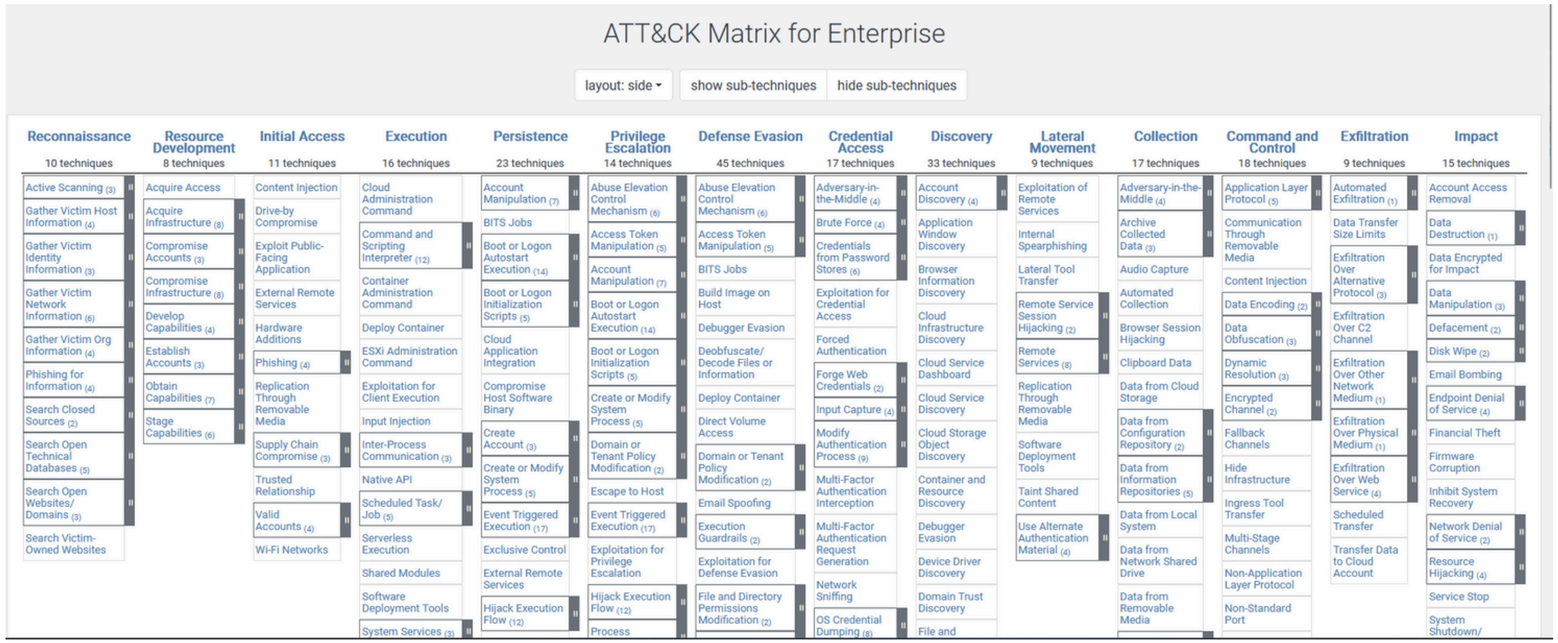
T1071.004 - Application Layer Protocol: DNS
- Usage: 45+ malware families for C2
- Tools: Cobalt Strike, SUNBURST, dnscat2
- Methods: Base64/Hex encoding in subdomains
- Advanced: DNS-over-HTTPS for encrypted C2

T1557 - Adversary-in-the-Middle
- Method: DNS hijacking + SSL generation

Let's Encrypt abuse, certificate impersonation

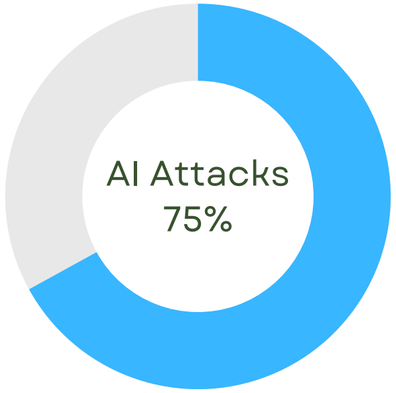
T1583.001/T1584.002 - Infrastructure Acquire/ Compromise
- Sea Turtle: DNS server compromise at registrar level
- Mandiant: DNS provider credential compromise
- APT29: Dynamic DNS service acquisition

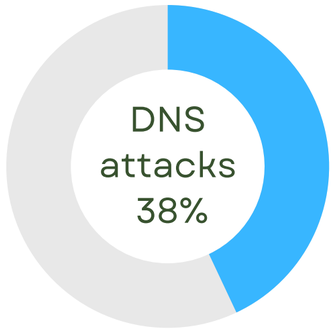
T1572 - Protocol Tunneling
- Usage: Data exfiltration, covert C2 channels
- Detection: Anomaly analysis, payload inspection



AI-POWERED ATTACK

how it's evolving



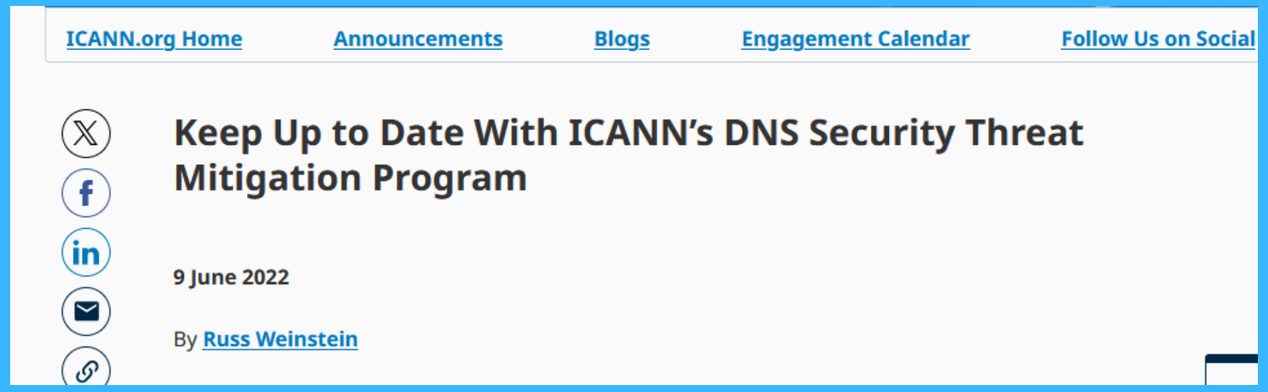


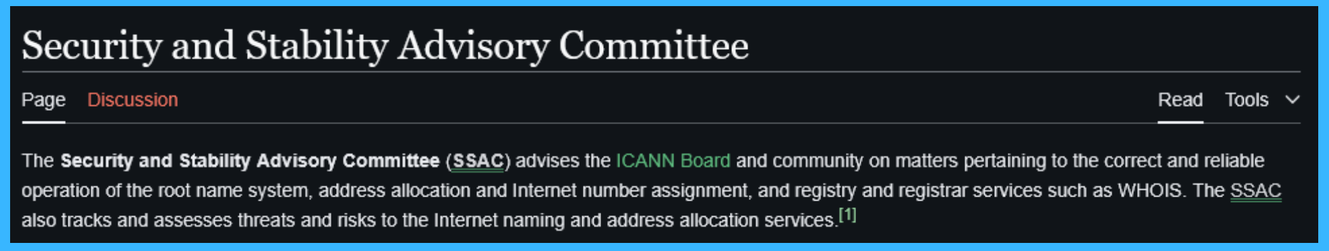
2025 AI Integration Statistics

- 75% of security professionals report AI-enhanced attacks
- 85% attribute attack increase to generative AI usage
- 117% YoY increase in DNS amplification attacks (Q4 2023)
- 38% of DNS attacks involved malware distribution (2023)

Hybrid Attack Combinations

- Spoofing + Tunneling (cache poisoning + covert channels)
- Amplification + Hijacking (DDoS + traffic redirection)
- Fast Flux + Tunneling (resilient infrastructure + covert C2)
- Dynamic DNS + Certificate Abuse (legitimate appearance + flexibility)





DETECTION STRATEGIES & ICANN REPONSE TO IT

How to Prevent

DNS Traffic Analysis

- Baseline Establishment: Normal query patterns & volumes
- Anomaly Detection: Excessive queries, unusual subdomains
- Character Analysis: Encoding detection, distribution analysis
- Timing Analysis: Query frequency, response patterns

Certificate Transparency Monitoring

- Real-time CT log monitoring for unauthorized certificates
- Let's Encrypt abuse pattern detection
- Domain impersonation campaign identification
- Wildcard certificate abuse alerts

Advanced Hunting Techniques for Organizations:

- Behavioral Analytics: Query timing, response patterns
- Statistical Analysis: Character distribution in domains
- Infrastructure Correlation: Cross-campaign analysis
- Intelligence Integration: IOC matching, TTP correlation

Where i learned from

Q&A + REFERENCES

References & Sources

- [CISA-AA19-024A] DNS Infrastructure Hijacking Campaign
- [ICANN-DNS-Abuse-Blog-2024] ICANN – DNS Abuse Mitigation Program (Key updates, Oct 12, 2024)
- [ED19-01-CISA] CISA Emergency Directive ED-19-01 (Mitigate DNS Infrastructure Tampering)
- [ICANN-STRAT-2026-30] ICANN Strategic Plan 2026–2030 (PDF)
- [ICANN-STRAT-2012-15-DRAFT] ICANN Draft Strategic Plan (2012–15 redline PDF)
- [CADE-ICANN-Feedback] CADE – ICANN seeks feedback on DNS abuse mitigation report
- [TechCrunch-ICANN2019] TechCrunch: “ICANN warns …” (Feb 23, 2019)
- [SeaTurtle-SOCPrime] Sea Turtle operation – SOC Prime reporting
- [IMDA-SeaTurtle-SG] IMDA advisory (Singapore): Sea Turtle targets cPanel w/ reverse shell (PDF)
- [SecurityAffairs-SeaTurtle] Security Affairs coverage: Sea Turtle targets Dutch entities
- [Google-Cloud/Mandiant] Global DNS Hijacking Campaign – Google Cloud blog (Mandiant research)
- [MITRE-ATT&CK] MITRE ATT&CK framework (main site)
- [MITRE-T1071.004] MITRE variant page – T1071.004 (Application Layer Protocol: DNS)
- [OECD-DNS-2022] OECD report – Security of the Domain Name System (2022, PDF)
- [Todyl-DNS-Tunneling] What is DNS Tunneling? – Todyl blog
- [Picus-T1071] Picus blog – MITRE ATT&CK T1071 overview

NextGen@ICANN84

Looking Forward

Stable & Secure Network

THANK YOU!

DNS SECURITY