Civic Commander Mattkse | mattske@mattske.com | (215) 479 - 9543

DOGE.gov Threat Analysis Report

Suspicious & Dangerous Connections Summary

- .gov hosted on private server
- Private server host to 700+ potential botnet sites
- Multiple IP addresses per region
- PITC.gov (Philippine International Trading Corporation) email server
- EOP.gov connection
- WhiteHouse.gov connection
- DoD/.mil connection

These details indicate that DOGE.gov is acting as a cover for foreign adversaries who can access classified information, secure government servers, and read email correspondences within our most important departments including the military. This could lead to adversaries receiving military equipment & troop locations, IP designs for equipment like the Iron Dome proposals, as well as command & control for decentralized cryptocurrencies such as the proposed Treasury system blockchain.

At a minimum, these details describe an incredibly reckless, careless, and vulnerable computer system. At worst, they are the blueprint for the most treasonous coup ever imagined in the modern world, orchestrated by the President of the United States and American businessmen like Elon Musk, Steve Witkoff, and others. Multiple indicators suggest that DOGE.gov is inextricably linked to malicious foreign actors who are using this to gain access to governmental systems, including Americans' private data, financial transaction systems, military secrets, and nearly anything else that passes through between government computers.

Even the Civil War did not pose such an existential threat, because regardless of the horrors involved, the Civil War was a battle between (2) factions that both viewed America as sacrosanct. Donald Trump, Elon Musk, Steve Witkoff, and their associates only view themselves as deserving of protections. They are selling us out to personally gain, while leaving the entire nation wide open to foreign attack on our financial systems, data security, and physical autonomy. It must be stopped immediately, even if interventions are required from allied nations.

Civic Commander Mattkse | mattske@mattske.com | (215) 479 - 9543

DOGE.gov Details About Compromised Network Connectivity

WHOIS

Last Checked: 2/10/25 | **Last Updated: 1/21/25**

CSD/CB: **Cameron Dixon** (Program Manager) - Registry Customer Service

4200 Wilson Blvd.

Arlington, VA 22201

Cybersecurity and Infrastructure Security Agency

CISA – NGR STOP 0645

1110 N. Glebe Rd.

Arlington, VA 20598-0645

(888) 282 - 0870

SecurityTrails

- Cloudflare, Inc. IP Addresses
  - 104.21.3.190
  - 172.67.131.28
- NS Records
  - robert.ns.cloudflare.com
  - ollie.ns.cloudflare.com
- SOA Records
  - Ttl: 10000
  - Email: dns.cloudflare.com
- AAAA Records
  - 2606:4700:3037::6815:3be
  - 2606:4700:3037::ac43:831c
- MX Records: DoD Network Information Center
  - inbound.mail.dmz.pitc.gov

Civic Commander Mattkse | mattske@mattske.com | (215) 479 - 9543

CentralOps

inbound.mail.dmz.pitc.gov

- User: anonymous [47.202.195.201]
- Balance: 43 units
- Addresses
    - 214.3.60.47
        - REGIS10-ARIN: disa.columbus.ns.mbx.arin-registrations@mail.mil
        - MIL-HSTMST-ARIN: disa.columbus.ns.mbx.hostmaster-dod-nic@mail.mil
    - 214.3.60.48
    - 214.3.60.45
    - 214.3.60.46
- Security Email: **dl.eop.cloudadmin@eop.gov**
- Name Server: **dmz01ns01.dns.dmz.pitc.gov**
- Name Server: **dmz01ns02.dns.dmz.pitc.gov**
- Name Server: **dmz02ns01.dns.dmz.pitc.gov**
- Name Server: **dmz02ns02.dns.dmz.pitc.gov**
- DNS Records
    - b399e-adcs001.ede.pitc.gov
    - **postmaster@whitehouse.gov**

CRT. SH

- join.doge.gov (for staffers to submit their applications)

View DNS . info

- 722 Domains On Same Server
- (5) .buzz sites - known for malicious activity like CSAM, extortion, etc.
- Command & Control Nomenclature Evident

Civic Commander Mattkse | mattske@mattske.com | (215) 479 - 9543

DNS Checker

- Previously Known IP Addresses
    - 104.21.3.190
    - 172.67.131.28
- Otherwise Unknown IP Addresses Uncovered
    - 146.112.61.108 (San Francisco)
        - Hostname(s): **hit-phish.opendns.com** - reported for “Russian scammers” over (30) times.
    - 172.64.80.1 (Columbia) - reported as scam under various names:
        - “Red88”
        - “Sv88”