Elon Musk Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever

A new investigation shows nuclear secrets and government servers are dangerously exposed to nation-state hackers.

Cyber-intelligence Brief

Over the past month, an unprecedented number of critical government systems, including those at the nation’s nuclear research labs, have been exposed to the open internet. This exposure jeopardizes both U.S. national security and the privacy of millions of Americans.

Notably, this alarming trend seems to coincide with DOGE’s unrestricted access to federal networks.

Photo by Robs on Unsplash

The Scale of Vulnerability Is Unlike Anything I’ve Ever Seen

Beginning on January 8, 2025, a surge of U.S. government infrastructure began appearing on what’s known as “the search engine of Internet-connected devices,” Shodan.io.

Federal agencies typically secure their systems behind multiple layers of protection, ensuring that critical services – such as mail servers, directory services, VPNs, internal IP addresses, and remote access gateways – remain isolated from public access.

The scope and severity of exposed government networks is unlike anything I've seen. It's hard to even have a baseline to compare it to. But one thing's for sure–adversaries such as Russia and China are dancing for joy.

Essentially, whatever is causing once-private government networks to suddenly be publicly observable is making the lives of Chinese and Russian hackers much easier–we're doing the first stage of hacking campaigns, network reconnaissance, for them. With such easy insights into once-secret U.S. networks, the likelihood of data breaches impacting millions of Americans becomes that much higher.

Mapping federal networks is a crucial first step in cyber-espionage. Hackers identify existing systems, open ports, and running services to exploit vulnerabilities.

Once this information is obtained, attackers can:

- **Identify unpatched vulnerabilities** in exposed services.
- **Crack passwords via brute-force attacks**
- **Harvest credentials** from misconfigured LDAP or mail servers.
- **Pivot into internal networks** through weak remote access configurations (e.g., RDP without multi-factor authentication).
- **Deploy malware or ransomware** targeting government systems.
- **Create backdoors for persistent access**

Adversaries of the U.S. can now easily map out the government's digital landscape, identify unpatched vulnerabilities, launch targeted attacks to crack passwords, and deploy malware or ransomware.

Nuclear Risks

Photo by Dan Meyers on Unsplash

Between January 14 and February 8, servers belonging to Lawrence Livermore National Laboratory, Los Alamos National Laboratory, Thomas Jefferson National Accelerator Facility, and Fermi Accelerator National Laboratory have been found with Remote Desktop Protocol (RDP) services exposed to the public internet. This grants malicious actors the opportunity to hack into servers hosting sensitive nuclear research data, a golden egg for spy agencies across the globe.

Alarmingly, a Department of Energy server allowed anonymous login with **write access,** raising the risk of hackers uploading malicious code or installing backdoors for persistent network access.

Unleashing AI on sensitive government data

My investigation also revealed government servers directly interfacing with AI products, creating yet another disturbing risk to national security that is extremely difficult to reverse or mitigate.

On February 6, the Washington Post reported that DOGE fed sensitive data into AI systems while auditing the Department of Education. The specific AI product used by DOGE was not known to the Post at the time.

However, my investigation reveals that Inventry[.]ai may be one of the AI products in question, with multiple U.S. government IP addresses pointing to its REST API. This indicates a massive flow of government data being sent to the AI company's servers.

Proof: 8 IP addresses on Amazon's GovCloud now point to Inventry.ai's REST API, indicating a massive firehose of data being sent to the AI company's servers. The IP addresses are: 18.253.166.131, 182.30.117.29, 18.253.153.187, 182.30.154.252, 18.254.229.158, 18.253.160.247, 18.254.175.18, 18.254.191.201

This is a stunning breach of Americans' privacy that likely breaks multiple federal laws, including the 1974 Privacy Act, the Federal Information Security Management Act, the E-Government Act, and the Computer Fraud and Abuse Act, among others.

Treasury Department

As early as January 24, Elon Musk and his DOGE entourage may have had partial access to Treasury Department systems, and then obtained full access on February 2. From there, he specifically targeted the Secure Payment System housed under the Bureau of Fiscal Services, which is responsible for disbursing billions of dollars of federal funds totaling **more than 20% of the entire U.S. economy.** (Southern District of NY Complaint, 2025).

That same day, Treasury Department servers linked to the Secure Payment System were observed on Shodan. Reasons for the Secure Payment System's appearance on Shodan could include server configuration changes or new services that were not previously accessible. Ultimately, we're left with more questions than answers–why are our nation's most sensitive systems being exposed on Beyonce's Internet?

Further vulnerable Treasury Department systems discovered include:

1. Comptroller of the Currency's Citrix NetScaler Gateway – enables **remote access to internal applications, desktops, and data**. It acts as a **VPN (Virtual Private Network) or proxy** for

users connecting to a corporate or government network. Exposing this gateway to the Internet makes it **a highly attractive target** for Russia- and China-sponsored hackers.
2. The U.S. Treasury Inspector General for Tax Administration (TIGTA) is responsible for investigating fraud within IRS programs, with divisions fighting cybercrime, fraud, and insider risk. On January 14 and continuing to present, TIGTA's server used for conducting meetings are publicly exposed.
3. The Treasury Department's Office of Inspector General's Outlook Web login page is now publicly exposed. This allows attackers to attempt brute force password attacks. Once inside, hackers could exploit CVE-2024-21413 to send malicious emails that further compromise government systems. Another Treasury mail server is observed here.

Remember your oath

This investigation has been the toughest of my career. I've had many sleepless nights wondering why exactly the DOGE broligarchy thinks they can play games with our nation's most deeply-held secrets. And honestly, as someone who analyzes terrible things for a living, I believe this is the biggest crisis we have ever faced.

The stakes could not be higher. Adversaries like Russia and China now have a roadmap to obtaining our nuclear research, financial systems, and private data of every American.

But we can't just sit back and let our most personal information be held hostage. This isn't just a job for Congress and the courts; we have to organize within our local communities and explain what's at stake to our loved ones.

I know you're tired too. It's a lot easier to not care but here we are. Through all this chaos, with our core values and Constitution under blitzkrieg attack, I've never felt a deeper love for America or more reason to defend her. In the words of Viktor Frankl, "For the world is in a bad state, but everything will become still worse unless each of us does his best."

Citations

1. Shodan Searcpartment of Energy nuclear laboratories [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/search?query=department+of+energy+country%3A%22US%22
2. 24.231.209.106 Department of Energy, anonymous login with write access [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/host/24.231.209.106
3. Natanson H, Gerrit De Vynck, Dwoskin E, Douglas-Gabriel D. Elon Musk's DOGE is feeding sensitive federal data into AI to target cuts [Internet]. Washington Post. The Washington Post; 2025 [cited 2025 Feb 8]. Available

from: https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/
4. 18.253.166.131 [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/host/18.253.166.131
5. 182.30.117.29 [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/host/182.30.117.29
6. 182.30.1.117 [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/host/182.30.1.117
7. 182.30.154.252 [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/host/182.30.154.252
8. 18.254.229.158 [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/host/18.254.229.158
9. 18.253.160.247 [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/host/18.253.160.247
10. 18.254.175.18 [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/host/18.254.175.18
11. 18.254.191.201 [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/host/18.254.191.201
12. Shodan Search Secure Payment System [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/search?query=title%3A%22Secure+Payment+System%22+country%3A%22US%22
13. UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK REQUEST FOR EMERGENCY TEMPORARY RESTRAINING ORDER UNDER FEDERAL RULE OF CIVIL PROCEDURE 65(B) COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF [Internet]. [cited 2025 Feb 9]. Available from: https://www.justsecurity.org/wp-content/uploads/2025/02/new-york-v-trump-doge-treasury-feb-7-2025.pdf
14. Wyden Demands Answers Following Report of Musk Personnel Seeking Access to Highly Sensitive U.S. Treasury Payments System | The United States Senate Committee on Finance [Internet]. Senate.gov. 2025 [cited 2025 Feb 9]. Available from: https://www.finance.senate.gov/chairmans-news/wyden-demands-answers-following-report-of-musk-personnel-seeking-access-to-highly-sensitive-us-treasury-payments-system
15. Shodan Search Treasury email servers [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/search?query=org%3A%22United+States+Department+of+the+Treasury%22+port%3A25
16. 164.95.8.37 Possible Treasury API changes [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/host/164.95.8.37
17. 199.83.35.87 Comptroller of the Currency NetScaler AAA Gateway [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/host/199.83.35.87
18. 164.95.148.5 Treasury Department Citrix Gateway [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/host/164.95.148.5

19.164.95.159.34 TIGTA meetings [Internet]. Shodan.io. 2025 [cited 2025 Feb 9]. Available from: https://www.shodan.io/host/164.95.159.34