Unmasking USDoD: The Enigma of the Cyber Realm

socradar.io/unmasking-usdod-the-enigma-of-the-cyber-realm/

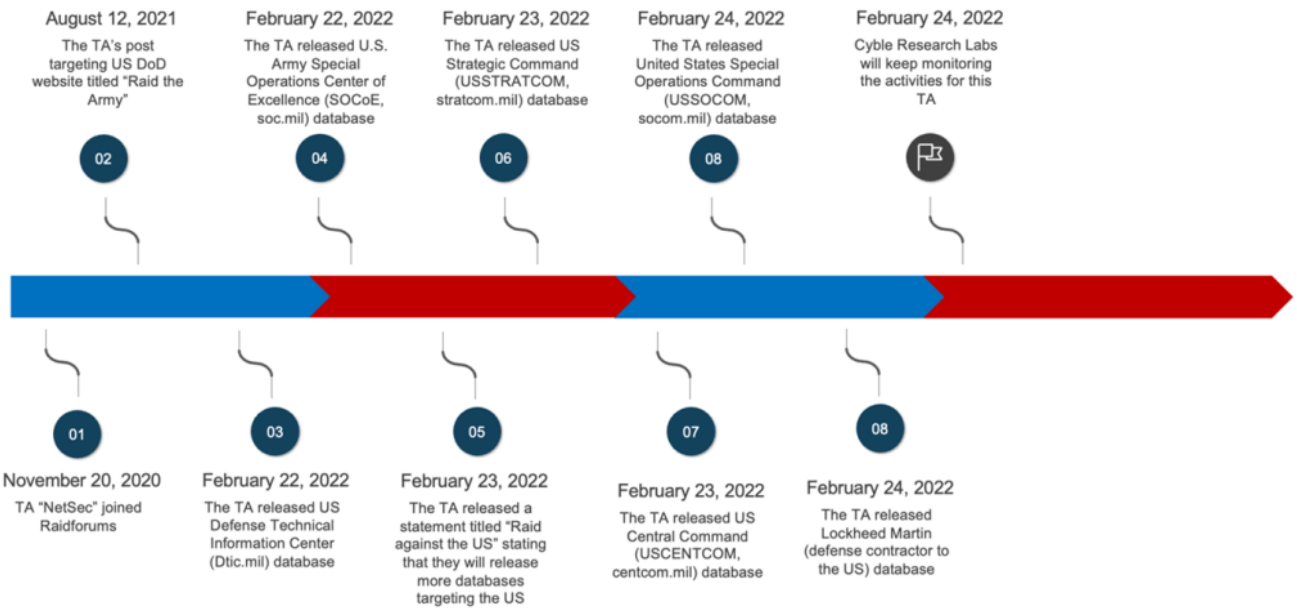
September 20, 2023

[Update] November 7, 2023: See the subheading: "UsDoD Continues Ambitious Claims; Now Its LinkedIn's Turn."

Emerging from the shadows of the cyber realm, "USDoD" first caught attention by exposing the data of **80,000** InfraGard members, revealing significant security lapses within the organization. This audacious act, coupled with a subsequent leak involving **3,200** Airbus vendors, has solidified his reputation in the cybersecurity world. Behind the pseudonym is a man in his mid-30s with roots in South America. Influenced by many, USDoD has been an eyecatcher for some time in the digital landscape.

Early Activities and Background of USDoD

Previously known as **"NetSec"** on RaidForums, USDoD gained notoriety with his **"#RaidAgainstTheUS campaign,"** targeting the U.S. Army and defense contractors. In February 2022, a report highlighted his breaches of multiple U.S. defense databases, painting him as a pro-Russian threat actor. However, USDoD refutes this label, clarifying that his collaborations with Russians were based on personal or business connections, not political motivations. One such collaboration involved an AI project named **"Tulip,"** aimed at collecting military data.



Timeline of the #RaidAgainstTheUS attacks now known as USDoD (Cyble)

His transition to the “USDoD” moniker occurred on Breached.vc in December 2022, where he posted data from InfraGard, a partnership between the FBI and private sector firms. Using social engineering, he impersonated a CEO and successfully gained membership, exposing a significant security lapse within InfraGard.

USDoD’s hacking approach heavily relies on social engineering, particularly **impersonation**. This technique has granted him access to high-profile entities, including NATO Cyber Center Defense and CEPOL. Despite targeting such entities, he remains confident, claiming to have protection in Spain from influential figures. His motivations intertwine personal vendettas with a love for challenging cyber exploits, revealing a multifaceted character behind the hacker alias.

Current Activities and Future of USDoD

Return to BreachForums and Airbus Breach

USDoD marked his return on BreachForums with a significant leak: data from **3,200 Airbus vendors**. He accessed Airbus using an employee’s credentials from a Turkish airline, which he found in infostealer logs. His post also contained a warning for Lockheed Martin and Raytheon, though he later revealed this was a diversion while targeting other entities like Deloitte, NATO, and CEPOL.

Metropolitan Club of the City of Washington Database Breach

Most recently, USDoD has announced a security breach, revealing the database of the Metropolitan Club of the City of Washington. The incident stands apart from an earlier breach linked to the same threat actor and the “Ransomed.vc” ransomware group. He asserts that by obtaining Personal Identifiable Information (PII) about the General Manager, he was able to crack the login details for the organization’s admin panel.

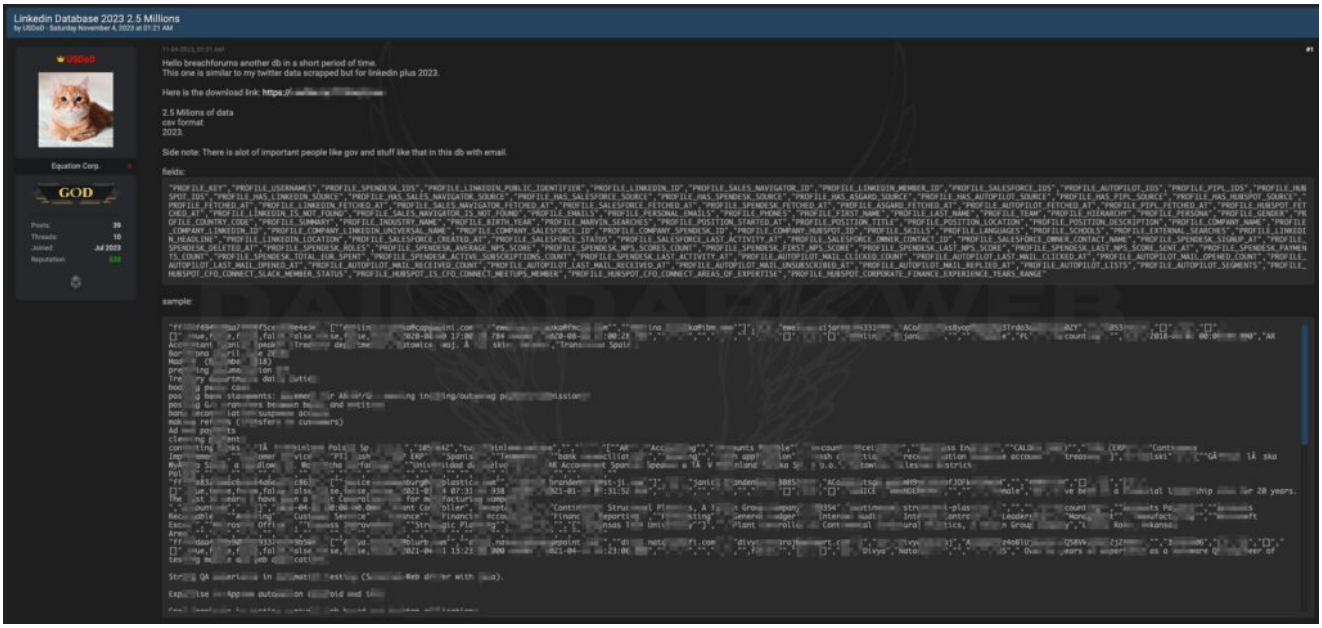
Misunderstandings and Clarifications

Brian Krebs’ report on the Airbus leak, which tied the data release to the 9/11 anniversary, deeply upset USDoD. He clarified that the timing was unintentional and expressed his frustration with Krebs’ insinuations. USDoD emphasized that his actions were neither politically motivated nor terrorist-driven by saying, “I won’t attack Russia, China, South and North Korea, Israel, and Iran. The rest, I don’t care”.

UsDoD Continues Ambitious Claims; Now Its LinkedIn’s Turn

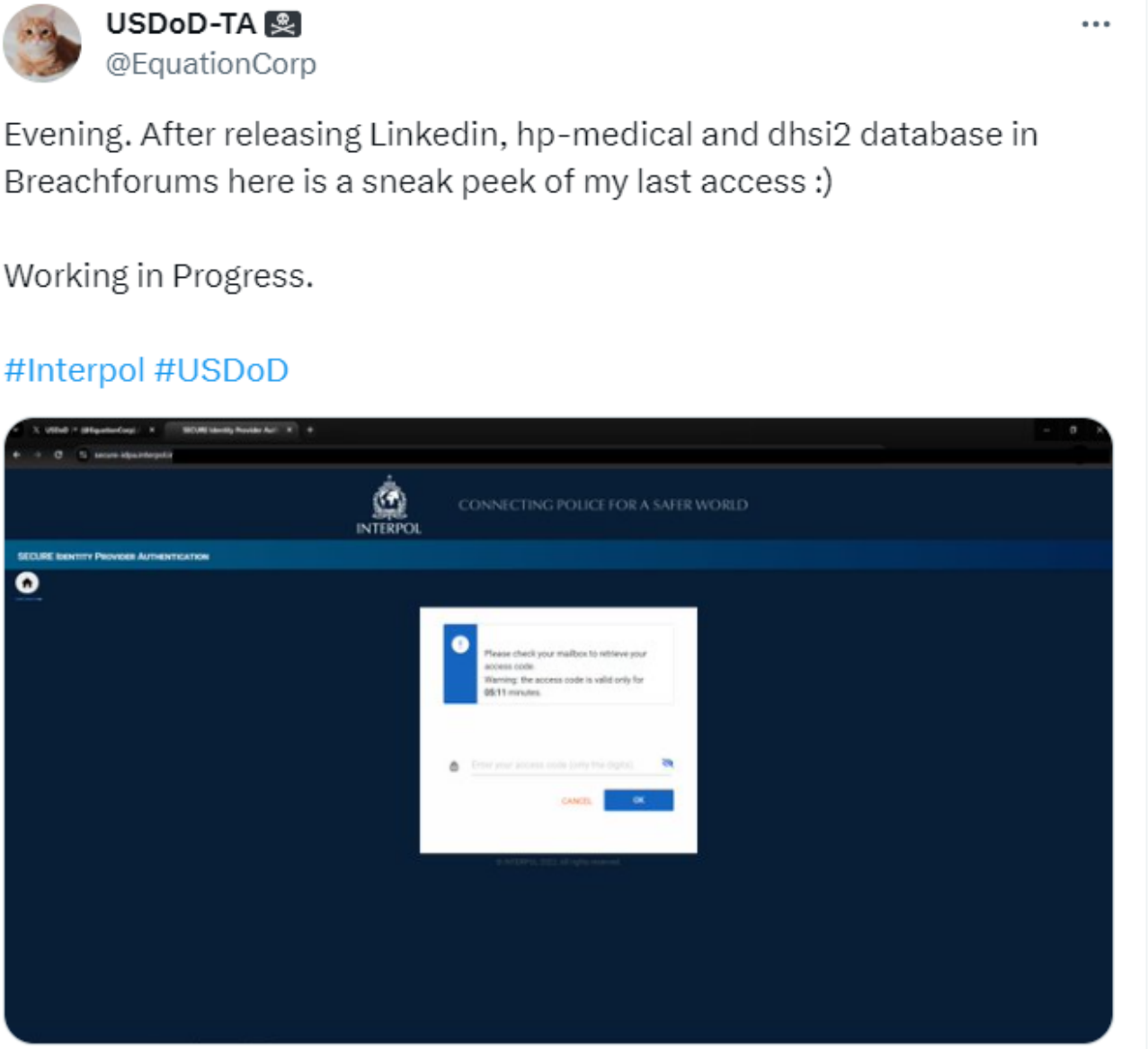
UsDoD, which managed to make a significant impact on its own, continues its operations. He claims to have released 2.5 million records, alleging a breach of the LinkedIn Database.

“haveibeenpwned” founder Troy Hunt made the following comment in his Twitter account, regarding this incident: *“Interesting data. Allegedly 2.5M, but almost 6M unique addresses. One fellow Aussie has 5 addresses across telco, bank, publisher, and 2 e-comm sites. Their LinkedIn reflects this, so this data could tie together identities.”*



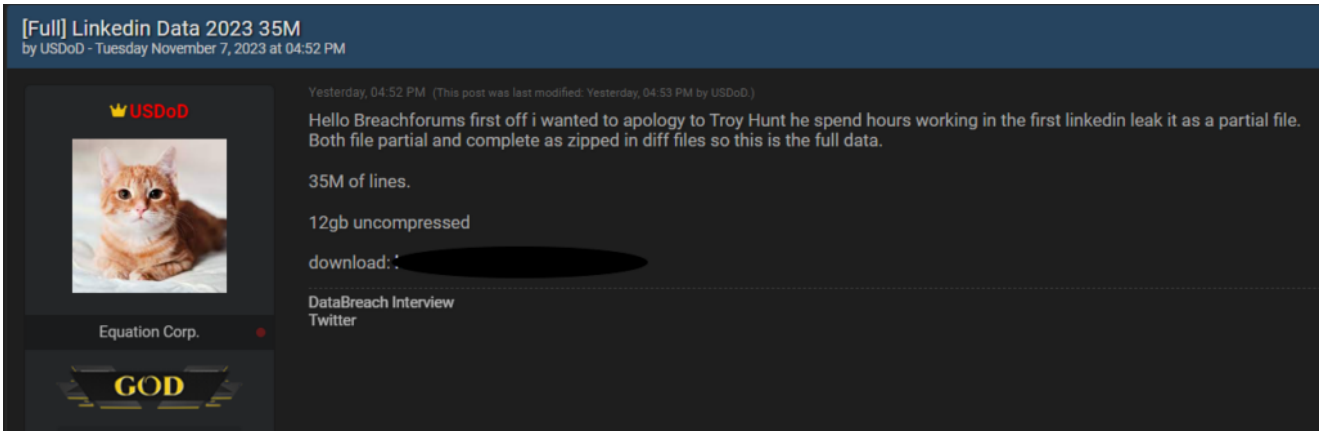
Alleged LinkedIn database leak

According to UsDoD’s statement, the actor shared alleged data breaches of the hp-medical and dhsi2 on “breachforums” recently, also shared a screenshot in his Twitter account from the Interpol website’s interface, labeling it as a preview of his upcoming operation.



UsDoD's tweet

USDoD has expanded the amount of data leaked from LinkedIn. According to his claims, this new dataset comprises **35 million entries and expands to 12 gigabytes when uncompressed. Troy Hunt has shared that the additional collection of scraped and compiled data linked to LinkedIn has now been incorporated into Have I Been Pwned . This inclusion has introduced an extra **14 million unique e-mail addresses**, increasing the total scope of the security breach to nearly 20 million records. It's worth noting that **13%** of these e-mail addresses were already present in Have I Been Pwned.



Furthermore, Troy Hunt published a blog post about the dataset. He stated that the dataset is a blend of data extracted from publicly available LinkedIn profiles, fictitious e-mail addresses, and, to a limited extent, information from other sources listed in the column headings. However, it's important to note that the individuals are real, the companies are legitimate, the domains are authentic, and, in many instances, the e-mail addresses themselves are valid.

Real Targets and Motivations

Despite the public threats against Raytheon and Lockheed, USDoD's real interests lay elsewhere. He targeted and accessed entities like CEPOL and NATO, aiming to understand their security and training methods. His ultimate goal? **Full control and influence.** He plans to establish a private company to sell military intelligence on the dark web, with Constellis being his first target.

USDoD claiming successful access to CEPOL (DataBreaches)

USDoD claiming a successful attempt to register for the NATO portal (DataBreaches)

USDoD's Future Endeavors and BreachForums

USDoD's vision extends beyond hacking. He aims to **revitalize BreachForums**, lamenting the lack of engagement from its current owner, **ShinyHunters**. He believes active participation from influential members can restore the forum's former glory.

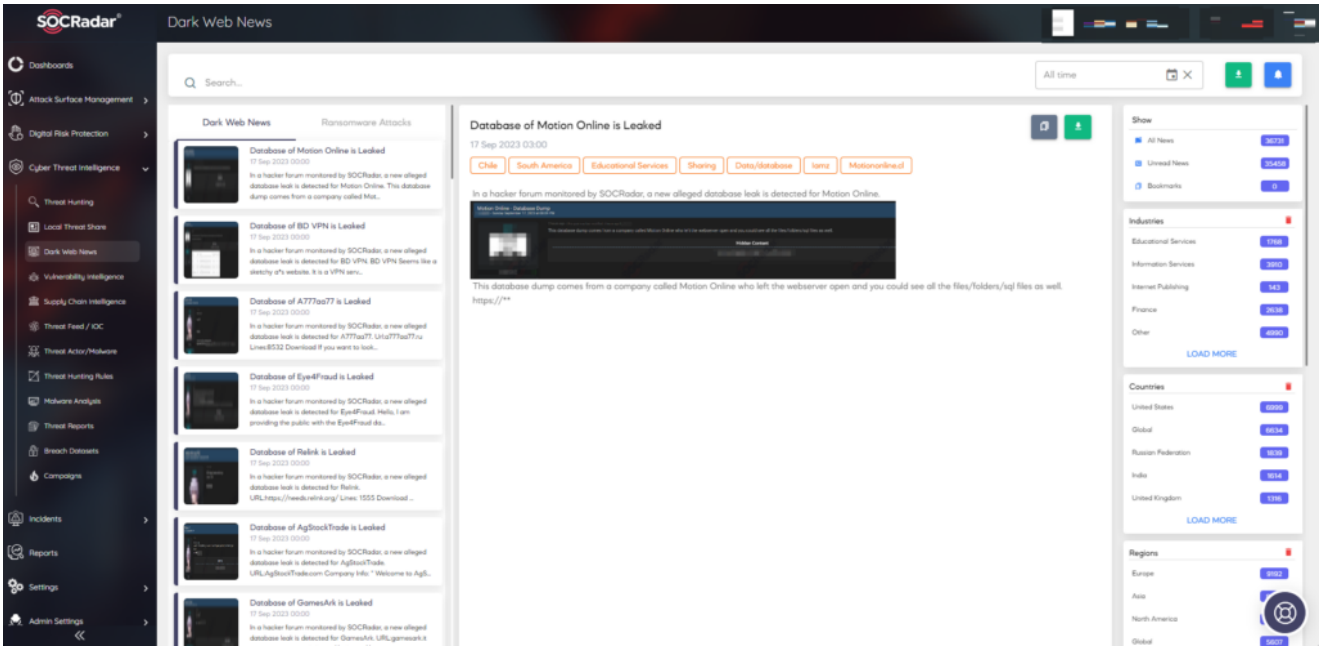
USDoD's activities and plans are multifaceted; as he ventures into selling military intelligence and continues to challenge high-profile targets, **defense entities should remain vigilant**.

Conclusion

The enigmatic figure of **"USDoD"** stands as a testament to the evolving landscape of cybersecurity. From his audacious breaches to his intricate web of motivations, he represents **the new age of hackers** who blend personal vendettas, business ambitions, and sheer love for the challenge. His journey, from exposing significant security lapses in reputed organizations to announcing ambitious future plans, underscores the need for heightened vigilance in the digital realm. As the lines between personal, political, and professional motivations blur, entities worldwide must recognize and prepare for the multifaceted threats posed by individuals like USDoD. In a world where information is power, understanding the motivations and methods of those who seek to control it is paramount.

In today's digital age, the dark web has become a hotbed for illicit activities, including the trade of stolen data and the planning of cyberattacks. SOCRadar's dark web monitoring offers a solution to this growing threat. By continuously scanning the shadowy corners of the dark web, SOCRadar provides **timely alerts** to businesses and individuals when significant

players make a move or when their sensitive information appears in these hidden realms. This system allows for swift action, minimizing potential damage and ensuring that stakeholders remain one step ahead of cyber adversaries.



SOCRadar Dark Web News