Hacktivist Entity USDoD Claims to Have Leaked CrowdStrike’s Threat Actor List

crowdstrike.com/blog/hacktivist-usdod-claims-to-have-leaked-threat-actor-list/

Counter Adversary Operations July 25, 2024

The threat intel data noted in this report is available to tens of thousands of customers, partners and prospects – and hundreds of thousands of users. Adversaries exploit current events for attention and gain. We remain committed to sharing data with the community.

On July 24, 2024, hacktivist entity *USDoD* claimed on English-language cybercrime forum BreachForums to have leaked CrowdStrike’s “entire threat actor list.”[1] The actor also alleged that they had obtained CrowdStrike’s “entire IOC [indicators of compromise] list” and would release it “soon.” In the announcement, *USDoD* provided a link to download the alleged threat actor list and provided a sample of data fields, likely in an effort to substantiate their claims.

Sample data acquired from the threat actor included a CSV file that contained fields for adversary aliases, adversary status, last active dates for each adversary, region/country of adversary origin, number of targeted industries, number of targeted countries, actor type and motivation. In one example, the adversary alias field contained the same aliases as the Falcon platform but listed in a different order.

The sample data contained data with “LastActive” dates until no later than June 2024; however, the Falcon portal’s last active dates for some of the referenced actors are as recent as July 2024, suggesting when the actor potentially obtained the information.

USDoD also claimed in their post to have “two big dbs from a oil company and a pharmacy industry (not from USA)”. It was unclear whether the post was linking the claims to have breached an oil company and pharmaceutical industry company with their alleged acquisition of CrowdStrike data.

USDoD Background

USDoD has previously exaggerated claims, likely in an attempt to enhance their reputation within both hacktivist and eCrime communities. For example, the actor has previously claimed to have conducted a hack-and-leak operation targeting a professional-networking platform, but industry sources refuted *USDoD*’s claims and asserted the alleged leak was conducted via web scraping rather than via a targeted intrusion.[2]

Since at least 2020, *USDoD* has conducted both hacktivism and financially motivated breaches, primarily using social-engineering tactics to access sensitive data. Over the last two years, the actor has focused on high-profile targeted intrusion campaigns. Additionally, since January 2024, the threat actor has sought to diversify and expand their cyber activities from solely conducting cyber operations into administering eCrime forums.

[1] BreachForums ST Post ID: 781235

[2] https[:]//www.hackread[.]com/hacker-leaks-scraped-linkedin-user-records/