FBI Hacker Dropped Stolen Airbus Data on 9/11

Published: 2023-09-14 · Archived: 2026-04-02 10:34:14 UTC

In December 2022, KrebsOnSecurity broke the news that a cybercriminal using the handle "**USDoD**" had infiltrated the **FBI**'s vetted information sharing network **InfraGard**, and was selling the contact information for all 80,000 members. The FBI responded by reverifying InfraGard members and by seizing the cybercrime forum where the data was being sold. But on Sept. 11, 2023, USDoD resurfaced after a lengthy absence to leak sensitive employee data stolen from the aerospace giant **Airbus**, while promising to visit the same treatment on top U.S. defense contractors.

USDoD's avatar used to be the seal of the U.S. Department of Defense. Now it's a charming kitten.

In a post on the English language cybercrime forum **BreachForums**, USDoD leaked information on roughly 3,200 Airbus vendors, including names, addresses, phone numbers, and email addresses. USDoD claimed they grabbed the data by using passwords stolen from a Turkish airline employee who had third-party access to Airbus' systems.

USDoD didn't say why they decided to leak the data on the 22nd anniversary of the 9/11 attacks, but there was definitely an aircraft theme to the message that accompanied the leak, which concluded with the words, "Lockheed martin, Raytheon and the entire defense contractos [sic], I'm coming for you [expletive]."

Airbus has apparently confirmed the cybercriminal's account to the threat intelligence firm **Hudson Rock**, which determined that the Airbus credentials were stolen after a Turkish airline employee infected their computer with a prevalent and powerful info-stealing trojan called **RedLine**.

Info-stealers like RedLine typically are deployed via opportunistic email malware campaigns, and by secretly bundling the trojans with cracked versions of popular software titles made available online. Credentials stolen by info-stealers often end up for sale on cybercrime shops that peddle purloined passwords and authentication cookies (these logs also often show up in the malware scanning service VirusTotal).

Hudson Rock said it recovered the log files created by a RedLine infection on the Turkish airline employee's system, and found the employee likely infected their machine after downloading pirated and secretly backdoored software for Microsoft Windows.

Hudson Rock says info-stealer infections from RedLine and a host of similar trojans have surged in recent years, and that they remain "a primary initial attack vector used by threat actors to infiltrate organizations and execute cyberattacks, including ransomware, data breaches, account overtakes, and corporate espionage."

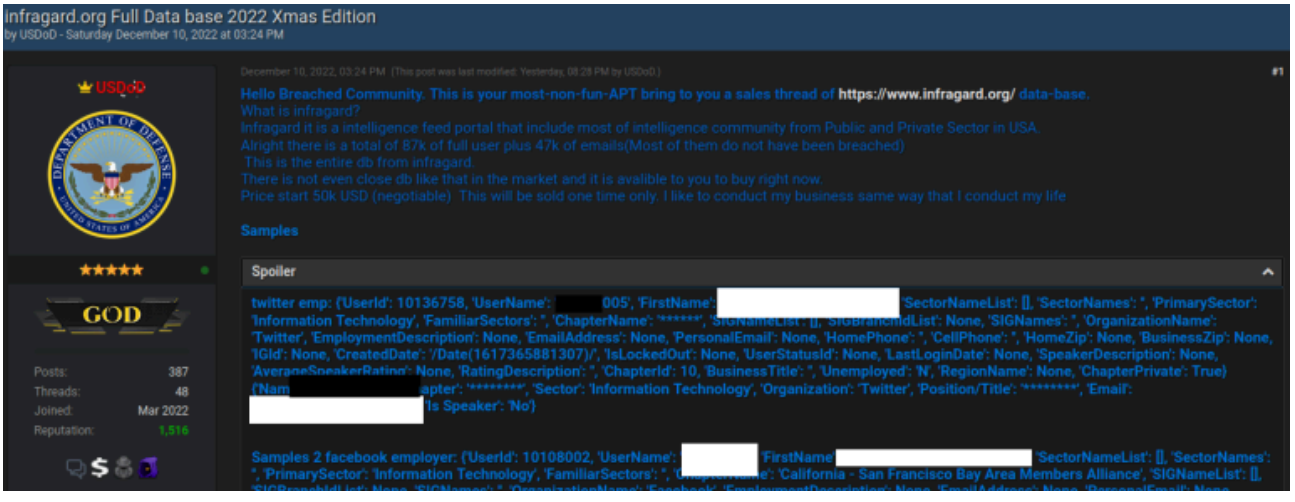
The prevalence of RedLine and other info-stealers means that a great many consequential security breaches begin with cybercriminals abusing stolen employee credentials. In this scenario, the attacker temporarily assumes the identity and online privileges assigned to a hacked employee, and the onus is on the employer to tell the difference.

In addition to snarfing any passwords stored on or transmitted through an infected system, info-stealers also siphon authentication cookies or tokens that allow one to remain signed-in to online services for long periods of time without having to resupply one's password and multi-factor authentication code. By stealing these tokens, attackers can often reuse them in their own web browser, and bypass any authentication normally required for that account.

Microsoft Corp. this week acknowledged that a China-backed hacking group was able to steal one of the keys to its email kingdom that granted near-unfettered access to U.S. government inboxes. Microsoft's detailed post-mortem cum mea culpa explained that a secret signing key was stolen from an employee in an unlucky series of unfortunate events, and thanks to TechCrunch we now know that the culprit once again was "token-stealing malware" on the employee's system.

In April 2023, the FBI seized Genesis Market, a bustling, fully automated cybercrime store that was continuously restocked with freshly hacked passwords and authentication tokens stolen by a network of contractors who deployed RedLine and other info-stealer malware.

In March 2023, the FBI arrested and charged the alleged administrator of BreachForums (aka Breached), the same cybercrime community where USDoD leaked the Airbus data. In June 2023, the FBI seized the BreachForums domain name, but the forum has since migrated to a new domain.



USDoD's InfraGard sales thread on Breached.

Unsolicited email continues to be a huge vector for info-stealing malware, but lately the crooks behind these schemes have been gaming the search engines so that their malicious sites impersonating popular software vendors actually appear before the legitimate vendor's website. So take special care when downloading software to ensure that you are in fact getting the program from the original, legitimate source whenever possible.

Also, unless you *really* know what you're doing, please don't download and install pirated software. Sure, the cracked program might do exactly what you expect it to do, but the chances are good that it is also laced with something nasty. And when all of your passwords are stolen and your important accounts have been hijacked or sold, you will wish you had simply paid for the real thing.
