



DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

16 June 25

Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

Articles	2
Anubis Ransomware Packs a Wiper to Permanently Delete Files	2
New Predator Spyware Infrastructure Revealed Activity in Mozambique for the First Time	2
WestJet Investigates Cyberattack Disrupting Internal Systems	2
Apple Zero-Click Flaw in Messages Exploited to Spy on Journalists Using Paragon Spyware	2
Paraguay Suffered Data Breach: 7.4 Million Citizen Records Leaked on Dark Web	3
A Cyberattack on United Natural Foods Caused Bread Shortages and Bare Shelves	3
SinoTrack GPS Devices Vulnerable to Remote Vehicle Control via Default Passwords	3

Articles

Anubis Ransomware Packs a Wiper to Permanently Delete Files

Active since late 2024 and operating under the ransomware-as-a-service (RaaS) model, Anubis was first detailed in February this year, when threat intelligence firm Kela observed it mainly focusing on data extortion, without the encryption component. A fresh Trend Micro report, however, puts things in a different perspective: not only does Anubis encrypt victims' data, but it also has a wiper module that destroys it. Affiliates are promised negotiable revenue-share structures for long-term cooperation, as well as access to programs beyond the typical RaaS and double extortion for monetization, namely a data ransomware affiliate and an access monetization affiliate program. To date, the group has targeted construction, engineering, and healthcare organizations in Australia, Canada, Peru, and the United States, with seven victims listed on Anubis' Tor-based leak site. Anubis' operators rely on spear phishing emails for initial access. Once in, they rely on various commands and scripts to check for administrative privileges, attempt to elevate them to System, and then proceed to file and directory discovery.

<https://www.securityweek.com/anubis-ransomware-packs-a-wiper-to-permanently-delete-files/>

New Predator Spyware Infrastructure Revealed Activity in Mozambique for the First Time

Insikt Group analyzed the new Predator spyware infrastructure and discovered it's still gaining users despite U.S. sanctions since July 2023. Despite earlier declines in activity due to U.S. sanctions and public exposure, Predator spyware has resurged. Insikt Group analyzed a renewed infrastructure linked to the commercial spyware company and identified a new customer in Mozambique, highlighting continued use of the surveillance tools, especially in Africa. Over half of Predator's identified clients are on the continent, and links to a Czech entity suggest the Intellexa Consortium remains active behind the scenes. Insikt Group uncovered a new Predator spyware infrastructure, including evasive updates and high-tier components. The new Predator spyware infrastructure includes domains likely used for delivering payloads and exploiting victims. While earlier Predator domains mimicked legitimate sites like news outlets, recent ones feature random English or Portuguese words, some hinting at specific target regions, like the Badinan area in Iraqi Kurdistan.

<https://securityaffairs.com/179036/hacking/new-predator-spyware-infrastructure-revealed-activity-in-mozambique-for-first-time.html>

WestJet Investigates Cyberattack Disrupting Internal Systems

WestJet, Canada's second-largest airline, is investigating a cyberattack that has disrupted access to some internal systems as it responds to the breach. The attack prevented users from logging into the website and mobile app, with those services now restored. A Saturday morning update says the company's operation continues to run safely, but the attack has impacted access to some of its software and services. It is unclear if the loss of access to its systems is caused by a ransomware attack that encrypted those devices or if they shut them to prevent the spread of the breach.

<https://www.bleepingcomputer.com/news/security/westjet-investigates-cyberattack-disrupting-internal-systems/>

Apple Zero-Click Flaw in Messages Exploited to Spy on Journalists Using Paragon Spyware

Apple has disclosed that a now-patched security flaw present in its Messages app was actively exploited in the wild

to target civil society members in sophisticated cyber attacks. The vulnerability, tracked as CVE-2025-43200, was addressed on February 10, 2025, as part of iOS 18.3.1, iPadOS 18.3.1, iPadOS 17.7.5, macOS Sequoia 15.3.1, macOS Sonoma 14.7.4, macOS Ventura 13.7.4, watchOS 11.3.1, and visionOS 2.3.1. "A logic issue existed when processing a maliciously crafted photo or video shared via an iCloud Link," the company said in an advisory, adding the vulnerability was addressed with improved checks. The iPhone maker also acknowledged that it's aware the vulnerability "may have been exploited in an extremely sophisticated attack against specifically targeted individuals." While Apple did not share any further details of the nature of the attacks weaponizing CVE-2025-43200, the Citizen Lab said it unearthed forensic evidence that the shortcoming was leveraged to target Italian journalist *Ciro Pellegrino* and an unnamed prominent European journalist and infect them with Paragon's Graphite mercenary spyware.

<https://thehackernews.com/2025/06/apple-zero-click-flaw-in-messages.html>

Paraguay Suffered Data Breach: 7.4 Million Citizen Records Leaked on Dark Web

Resecurity has identified 7.4 million records containing personally identifiable information (PII) of Paraguayan citizens leaked on the dark web today. Last week, cybercriminals have offered information about all citizens of Paraguay for sale, demanding \$7.4 million in ransom payments, \$1 per citizen. A ransomware group was extorting the entire country in what is probably one of the most significant cybersecurity incidents in the nation's history, with a symbolic deadline – Friday, June 13, 2025. The stolen data has been published on multiple underground forums. Interestingly, besides ZIP files containing databases, the actors also published a torrent file, enabling other Internet users to freely download citizens' records using P2P networks. Notably, in the ransom demand, the actors accuse the country's leadership of corruption and a lack of attention to citizens' data protection. Government of Paraguay declined to pay the ransom in the official statement, and did not share any insights on how the information about 7.5 million citizens has been stolen, bringing only vague statements.

<https://securityaffairs.com/178970/data-breach/paraguay-suffered-data-breach-7-4-million-citizen-records-leaked-on-dark-web.html>

A Cyberattack on United Natural Foods Caused Bread Shortages and Bare Shelves

United Natural Foods, Inc. (UNFI) is a Providence, Rhode Island–based natural and organic food company. The largest publicly traded wholesale distributor of health and specialty food in the United States and Canada, it is Whole Foods Market's main supplier, with their traffic making up over a third of its revenue in 2018. On June 5, United Natural Foods Inc. (UNFI) suffered a cyberattack that disrupted its systems and caused product shortages at Whole Foods stores nationwide. United Natural didn't disclose details about the attack, but similar disruptions in the past have often been tied to ransomware attacks. The impact of the UNFI cyberattack has extended beyond Whole Foods, affecting smaller retailers as well. The Community Food Co-Op in Bellingham, Washington, informed customers that due to UNFI being its main supplier, some shelves may look bare.

<https://securityaffairs.com/178991/hacking/a-cyberattack-on-united-natural-foods-caused-bread-shortages-and-bare-shelves.html>

SinoTrack GPS Devices Vulnerable to Remote Vehicle Control via Default Passwords

Two security vulnerabilities have been disclosed in SinoTrack GPS devices that could be exploited to control certain remote functions on connected vehicles and even track their locations. The vulnerabilities, per the agency, affect all versions of the SinoTrack IoT PC Platform. A brief description of the flaws: CVE-2025-5484 (CVSS score: 8.3) A weak authentication to the central SinoTrack device management interface stems from the use of a default password and a username that's an identifier printed on the receiver. CVE-2025-5485 (CVSS score: 8.6) The

username used to authenticate to the web management interface, i.e., the identifier, is a numerical value of no more than 10 digits. An attacker could retrieve device identifiers with either physical access or by capturing identifiers from pictures of the devices posted on publicly accessible websites such as eBay. Furthermore, the adversary could enumerate potential targets by incrementing or decrementing from known identifiers or through enumerating random digit sequences. There are currently no fixes that address the vulnerabilities.

<https://thehackernews.com/2025/06/sinotrack-gps-devices-vulnerable-to.html>