



DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

28 Feb 25

Cyber Threat Roundup

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

Contents

Articles	2
12,000+ API Keys and Passwords Found in Public Datasets Used for LLM Training	2
Sticky Werewolf Uses Undocumented Implant to Deploy Lumma Stealer in Russia and Belarus	2
China-linked Threat Actors Stole 10% of Belgian State Security Service (VSSE)'s Staff Emails	2
Over 49,000 Misconfigured Building Access Systems Exposed Online	2
Silver Fox APT Uses Winos 4.0 Malware in Cyber Attacks Against Taiwanese Organizations.....	3
Sites of Major Orgs Abused in Spam Campaign Exploiting Virtual Tour Software Flaw.....	3

Articles

12,000+ API Keys and Passwords Found in Public Datasets Used for LLM Training

A dataset used to train large language models (LLMs) has been found to contain nearly 12,000 live secrets, which allow for successful authentication. The findings once again highlight how hard-coded credentials pose a severe security risk to users and organizations alike, not to mention compounding the problem when LLMs end up suggesting insecure coding practices to their users. Truffle Security said it downloaded a December 2024 archive from Common Crawl, which maintains a free, open repository of web crawl data. The massive dataset contains over 250 billion pages spanning 18 years. The company's analysis found that there are 219 different secret types in Common Crawl, including Amazon Web Services (AWS) root keys, Slack webhooks, and Mailchimp API keys.

<https://thehackernews.com/2025/02/12000-api-keys-and-passwords-found-in.html>

Sticky Werewolf Uses Undocumented Implant to Deploy Lumma Stealer in Russia and Belarus

The threat actor known as Sticky Werewolf has been linked to targeted attacks primarily in Russia and Belarus with the aim of delivering the Lumma Stealer malware by means of a previously undocumented implant. Cybersecurity company Kaspersky is tracking the activity under the name Angry Likho, which it said bears a "strong resemblance" to Awaken Likho (aka Core Werewolf, GamaCopy, and PseudoGamaredon). However, Angry Likho's attacks tend to be targeted, with a more compact infrastructure, a limited range of implants, and a focus on employees of large organizations, including government agencies and their contractors. The attackers have been found to mainly single out organizations in Russia and Belarus, with hundreds of victims identified in the former.

<https://thehackernews.com/2025/02/sticky-werewolf-uses-undocumented.html>

China-linked Threat Actors Stole 10% of Belgian State Security Service (VSSE)'s Staff Emails

The Belgian federal prosecutor's office is probing a possible security breach on its State Security Service (VSSE) by China-linked threat actors. Chinese hackers gained access to the VSSE's email server between 2021 and May 2023, stealing 10% of staff incoming and outgoing emails. Threat actors exploited a vulnerability, tracked as CVE-2023-2868, in the Barracuda Barracuda Email Security Gateway Appliance (ESG) Vulnerability. The same systems were used by Belgian intelligence and the Belgian Pipeline Organisation, which monitors pipelines in the North Sea. Attackers gained access to VSSE HR's data, including IDs and CVs of staff and applicants.

<https://securityaffairs.com/174743/intelligence/china-linked-threat-actors-stole-10-of-belgian-state-security-service-vsse-emails.html>

Over 49,000 Misconfigured Building Access Systems Exposed Online

Researchers discovered 49,000 misconfigured and exposed Access Management Systems (AMS) across multiple industries and countries, which could compromise privacy and physical security in critical sectors. Access Management Systems are security systems that control employee access to buildings, facilities, and restricted

areas via biometrics, ID cards, or license plates. Security researchers at Modat conducted a comprehensive investigation in early 2025 and discovered tens of thousands of internet-exposed AMS that were not correctly configured for secure authentication, allowing anyone to access them. In some cases, Modat could edit employee records, add fake employees, change access credentials, or manipulate building entry systems to restrict access to legitimate employees or allow unauthorized physical access to malicious actors.

<https://www.bleepingcomputer.com/news/security/over-49-000-misconfigured-building-access-systems-exposed-online/>

Silver Fox APT Uses Winos 4.0 Malware in Cyber Attacks Against Taiwanese Organizations

A new campaign is targeting companies in Taiwan with malware known as Winos 4.0 as part of phishing emails masquerading as the country's National Taxation Bureau. The campaign, detected last month by Fortinet FortiGuard Labs, marks a departure from previous attack chains that have leveraged malicious game-related applications. The attachment mimics an official document from the Ministry of Finance, urging the recipient to download the list of enterprises scheduled for tax inspection. But in reality, the list is a ZIP file containing a malicious DLL ("lastbld2Base.dll") that lays the groundwork for the next attack stage, leading to the execution of shellcode that's responsible for downloading a Winos 4.0 module from a remote server ("206.238.221[.]60") for gathering sensitive data.

<https://thehackernews.com/2025/02/silver-fox-apt-uses-winos-40-malware-in.html>

Sites of Major Orgs Abused in Spam Campaign Exploiting Virtual Tour Software Flaw

The websites of dozens of major private and government organizations have been abused in a massive spam campaign that involves exploitation of a vulnerability affecting widely used virtual tour software known as Krpano. Krpano is a widely used framework for panoramic images, enabling the creation of virtual tours and VR environments. Additional analysis showed that the impacted website hosted a virtual tour powered by software made by Krpano. This software is affected by a reflected cross-site scripting (XSS) vulnerability that has been exploited to lead users to shady websites.

<https://www.securityweek.com/sites-of-major-orgs-abused-in-spam-campaign-exploiting-virtual-tour-software-flaw/>