cybersixgill
A BITSIGHT Company

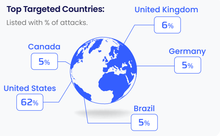
THREAT INTELLIGENCE REPORT

January 2025

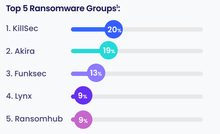
Ransomware Overview January 2025:

Top Targeted Countries:

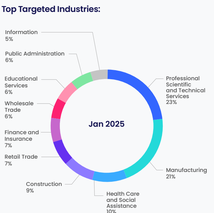
Listed with % of attacks.



Top 5 Ransomware Groups[1]:



Top Targeted Industries:



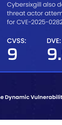
[1]The listed groups above accounted for 70% of all ransomware attacks among the top 10 operations in January 2025. The other five groups in the top 10 consisted of INC (7%), Bbase (7%), Medusa (6%), Qilin (6%), and Cloak (4%).

- The Cybersixgill Investigative Platform detected attacks against 573 organizations in January 2025, in comparison with 619 in December.
- The group KillSec was responsible for the highest number of ransomware attacks this month.
- Juggernaut extortion operation Funksec remained in the top three groups this month, after launching its dedicated leak site (DLS) in December 2024. While Funksec has claimed scores of victims, the group carries out multiple types of attacks, including data breaches, ransomware attacks, and website defacement. Cybersixgill's victimology statistics aggregate all of Funksec's attacks.

Trending Topics of the Month

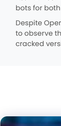
FBI Busts Notorious Underground Forums and Cybercrime Sites in Operation Talent

Two leading cybercrime forums, 'Cracked' and 'Nulled,' were seized by a multinational coalition of law enforcement agencies spearheaded by the FBI. The authorities also took control of three other cybercrime sites, which provided critical services to threat actors. In the wake of the seizure, Cybersixgill detected threat actors discussing migration to other platforms and the fate of those who used the seized forums.



U.S. Treasury Department Attack: Chinese APT Targeted Sanctions Evidence, Leveraged Two Zero-Days

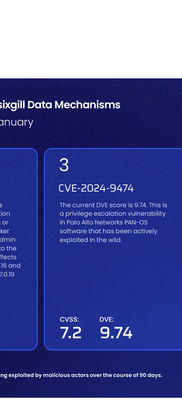
The U.S. Treasury Department revealed details related to a cyber attack perpetrated by a state-sponsored Chinese threat group. The attack zeroed in on systems with evidence related to economic sanctions, exploiting critical vulnerabilities in BeyondTrust security applications. In the immediate aftermath of the attack, Cybersixgill detected a threat actor attempting to sell a proof-of-concept (PoC) for one of the vulnerabilities.



New Ivanti Zero-Day: Attacks Reported as Exploits Circulate on the Underground

Regulators in the US and UK released alerts warning the public about two recently disclosed vulnerabilities affecting Ivanti products (CVE-2025-0282 and CVE-2025-0283), the first of which is being exploited in the wild. Cybersixgill observed multiple PoCs for CVE-2025-0282 on GitHub, which threat actors also spread on underground sources.

A New Interesting Source added to Cybersixgill's Collection Mechanisms:



AKULA Breach Bot:

A new version of the popular Telegram breach bot AKULA was launched, which enables channel subscribers to retrieve credentials for various organizations. Hackers can exploit these credentials to gain initial access to accounts, acting as the first step in broader cyber incidents.

Cybersixgill detected an AKULA subscriber producing credentials for a major media company that was subsequently attacked by an established ransomware operation.

Within two weeks, the channel had close to 7,000 subscribers and had collected tens of billions of records.

Top CVEs of the Month Based on Cybersixgill Data Mechanisms

Top 3 Vulnerabilities in January

1

CVE-2025-0282

The current DVE score is 9.97. This is a stack-based buffer overflow in Ivanti Connect Secure, Ivanti Policy Secure, and Ivanti Neurons for ZTA gateways, which allows unauthenticated attackers to achieve remote code execution. PoCs are available for CVE-2025-0282 which has been actively exploited in the wild. Cybersixgill also detected at least one threat actor attempting to sell a PoC for CVE-2025-0282.

CVSS: 9 DVE: 9.97

2

CVE-2024-55591

The current DVE score is 9.8. This vulnerability allows authentication bypass using an alternate path or channel, which a remote attacker could leverage to gain super-admin privileges via crafted requests to the Node.js websocket module. It affects FortiOS version 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12.

CVSS: 9.8 DVE: 9.8

3

CVE-2024-9474

The current DVE score is 9.74. This is a privilege escalation vulnerability in Palo Alto Networks PAN-OS software that has been actively exploited in the wild.

CVSS: 7.2 DVE: 9.74

*The Dynamic Vulnerability Exploit (DVE) Module score reflects the probability of a vulnerability being exploited by malicious actors over the course of 90 days.

An Analysis of the Top Mentioned Malware in January

Redline Malware

In January 2025, Redline malware had the highest number of mentions in the underground sources collected by the Cybersixgill Investigative Portal, despite an October 2024 sting that seized assets belonging to both the Redline and Meta operations.

Redline and Meta shared infrastructure and ran two of the most popular stealer malware operations on the underground.

The task force that took down Redline and Meta, dubbed Operation Magnus, accessed source code, license servers, REST-API services, panels, stealer binaries, and Telegram bots for both Redline and Meta.

Despite Operation Magnus' success, Cybersixgill continued to observe threat actors on the underground spreading cracked versions of Redline.

The distribution of malware mentions on the underground detected by Cybersixgill during the month of January.

Spotlight on a Threat Actor

b0nd

B0nd is an active member of the leading English-language cybercrime platform BreachForums who does not appear to be part of established ransomware or data extortion groups.

Throughout January 2025, b0nd published 15 posts or replies.

Among b0nd's notable activity was an attempt to sell over 18 million records related to customers of UK telecommunications giant TalkTalk. The threat actor also advertised the data on a Russian forum called XSS.

B0nd demanded $30,000 in cryptocurrency for the data set, and deleted the posts from both BreachForums and XSS, suggesting a buyer may have acquired the TalkTalk content.

APTs During the Month of January

APT Group Silent Crow

A hacktivist collective called Silent Crow attacked a Russian federal agency (Rosreestr), claiming it stole two billion lines of data related to Russian citizens.

While Rosreestr denied it had been breached, Cybersixgill observed Silent Crow leaking sample data and providing proof of the alleged attack on the group's official Telegram channel.

Subsequently, Cybersixgill detected Silent Crow announcing a second breach targeting the Russian subsidiary of Kia Motors.

Silent Crow's statements suggest they are of Ukrainian origin.

Follow us

cybersixgill
A BITSIGHT Company