CrowdStrike 2024 Global Threat Report

crowdstrike.com/global-threat-report/

34 newly named adversaries in 2023
2 min 7 sec — the fastest recorded eCrime breakout time
75% increase in cloud intrusions

Download report

Uncover the adversaries hiding in plain sight

Tracking 230+ adversaries and noting a record eCrime breakout time, the 2024 Global Threat Report unveils an alarming rise in covert activity and a cyber threat landscape dominated by stealth. Significant threat gains in data theft, cloud breaches, and malware-free attacks, show that despite advancements in detection technology, adversaries continue to adapt.

The must-read cybersecurity report of the year

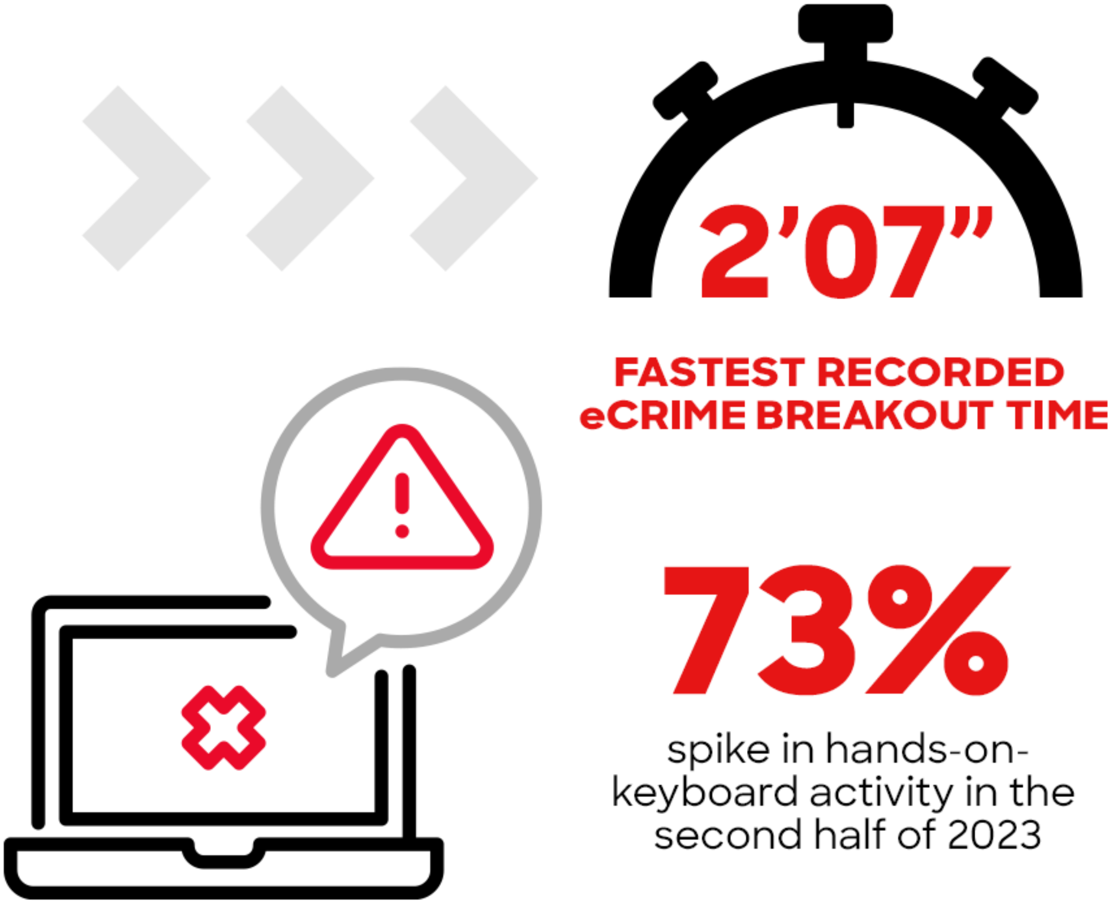
Get your copy of the CrowdStrike 2024
Global Threat Report.

Download report

Key report insights

Speed and stealth result in more successful attacks

Adversaries are operating with unprecedented stealth and today’s attacks take only minutes to succeed. They hide from detection by using valid credentials and legitimate tools, making it harder for defenders to detect a security breach.



2'07"

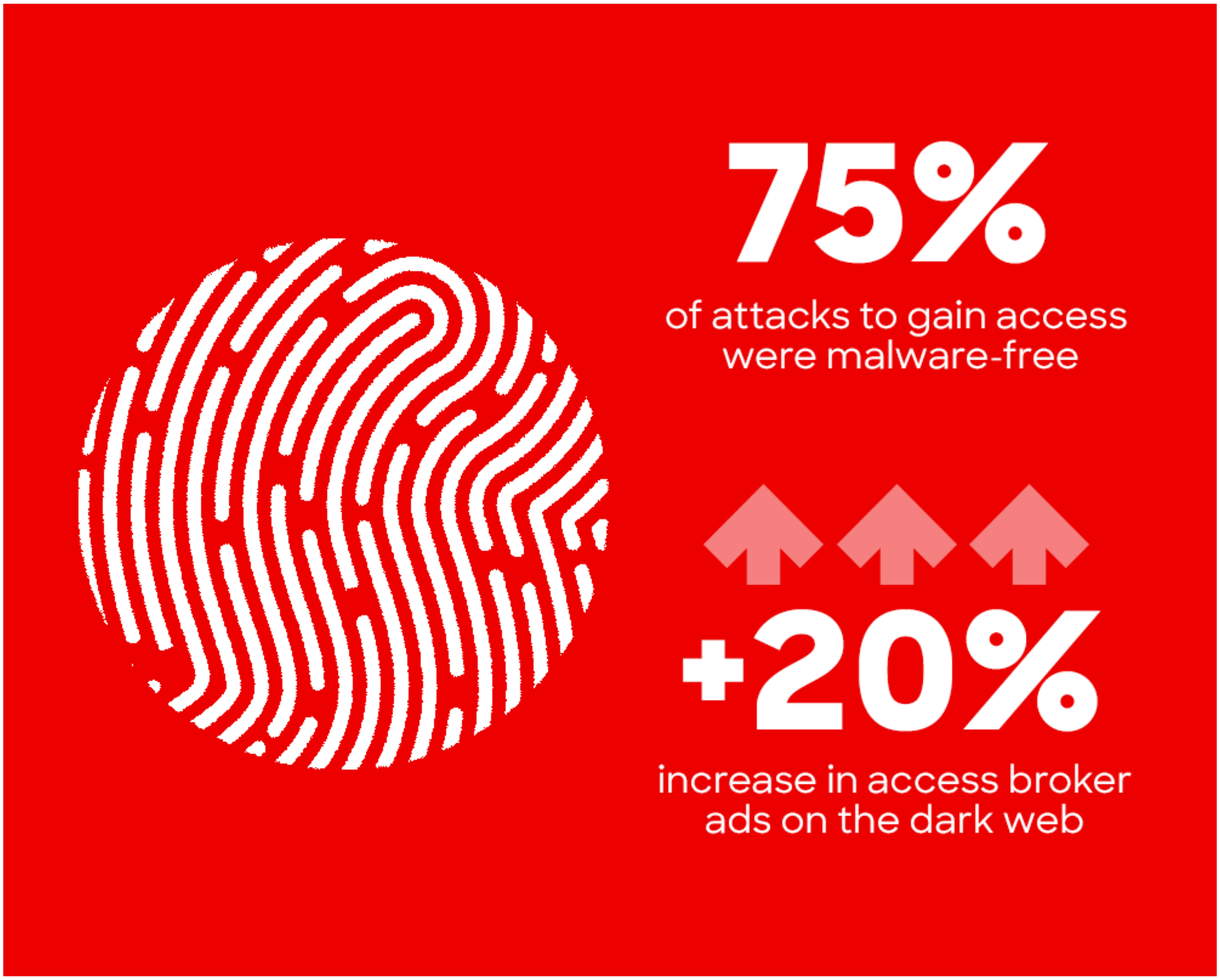
FASTEST RECORDED
eCRIME BREAKOUT TIME

73%

spike in hands-on-keyboard activity in the second half of 2023

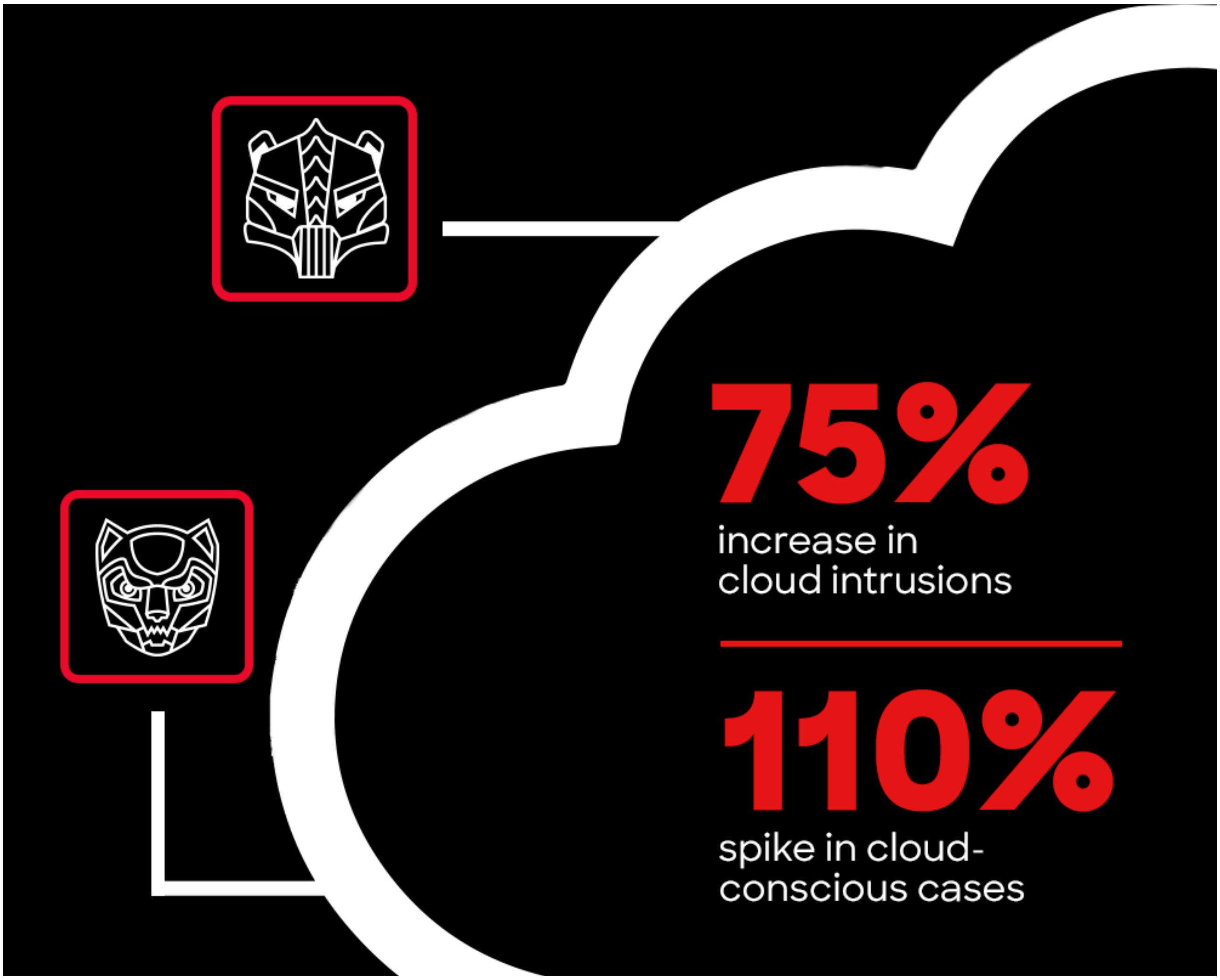
Identity-based attacks continue to surge

Identity threats exploded in 2023. With the help of generative AI, adversaries like SCATTERED SPIDER are using new techniques to break in faster, such as phishing, social engineering, and buying legitimate credentials from access brokers. Tactics like SIM-swapping, MFA bypass, and using stolen API keys to gain initial access are becoming popular.


75%
of attacks to gain access were malware-free
+20%
increase in access broker ads on the dark web

Adversaries are dominating in the cloud

Adversaries are capitalizing on global cloud adoption, making the cloud a prime battleground. Cloud-conscious adversaries, especially eCrime actors, use valid credentials to access victims’ cloud environments, and then use legitimate tools to execute their attack — making it difficult to distinguish between normal user activity and a breach.



Exploiting relationships opens access to multiple victims

Adversaries are maximizing their return on investment (ROI) by targeting vendor-client relationships, creating a single access point to target multiple organizations across verticals and regions. By exploiting access to IT vendors and compromising the software supply chain, they use trusted software to spread malicious tools.

Nearly 100% of relationship exploits originated at commercial software providers

Generative AI drives new adversarial risks

Adversary abuse of generative AI raises concerns about convincing social engineering campaigns and the creation of malicious software, tools, and resources to conduct stronger attacks. 2023 trends already prove AI was often used for social engineering, and the power of AI creates endless possibilities for adversaries to become even more sophisticated.

Inside the Year of Stealth

Get your copy of the CrowdStrike 2024 Global Threat Report.

Download report

Inside the Year of Stealth

Get your copy of the CrowdStrike 2024 Global Threat Report.

Download report