# CrowdStrike observes massive spike in identity-based attacks

techtarget.com/searchsecurity/news/366547445/CrowdStrike-observes-massive-spike-in-identity-based-attacks

Alexander Culafi

By Alexander Culafi, Senior News Writer

Published: 08 Aug 2023

LAS VEGAS -- CrowdStrike observed an alarming rise in identity-based intrusions, including a sixfold increase in Kerberoasting attacks, according to the vendor's 2023 Threat Hunting Report published Tuesday.

The threat report, which is in its sixth year, is CrowdStrike's annual look at attack and threat actor trends based on engagements the cybersecurity vendor observed over the previous year. Published at the start of Black Hat USA 2023, the 40-plus page report covers a number

of attack styles and adversary tactics seen between July 2022 and June 2023, but the clear theme of this year's report was identity-based threat activity.

For example, 62% of interactive intrusions involved the abuse of active accounts, and the report noted a "160% increase in attempts to gather secret keys and other credential materials via cloud instance metadata APIs." In its 2023 Global Threat Report earlier this year, CrowdStrike noted that 80% of all breaches involved compromised identities.

Adam Meyers, head of Counter Adversary Operations at CrowdStrike, told TechTarget Editorial that the focus on identity from threat actors this year came down in part to improvements in endpoint detection and response capabilities. Defenders have made it more difficult for a threat actor to get into a target environment, and as such, "using identity allows [the threat actor] to look more like a legitimate user, avoid detection and have a better chance at accomplishing their goal," he said.

"When a threat actor's ability to use the tactics they have been using becomes more difficult, rather than work harder for the same outcome, they reassess and find another way to accomplish the same goal," Meyers said. "And in this case, using legitimate user credentials that they can either social engineer or get out of a dark forum type of situation gets them the access that they want, and then they can live off the land."

CrowdStrike also noted a 583% increase in Kerberoasting, an attack technique in which threat actors exploit a flaw in the open source authentication protocol Kerberos in order to crack or "roast" user passwords. Although this is an extension to the aforementioned spike in identity-based attacks, CrowdStrike noted in its report that 27% of intrusions involving Kerberoasting came down to a single threat actor, Vice Spider, a ransomware actor active since at least April 2021.

The 2023 Threat Hunting Report also noted that adversary breakout time reached an all-time low, at 79 minutes. Breakout time is the average amount of time a threat actor needs to move laterally from the initial point of compromise to other systems and hosts within the victim environment. Breakout time in the 2022 Threat Hunting Report was 84 minutes.

## CrowdStrike launches Counter Adversary Operations

Also as part of Black Hat, CrowdStrike launched "Counter Adversary Operations," a new team led by Meyers that will bring CrowdStrike's threat intelligence and threat hunting teams under a single banner. The 2023 Threat Hunting Report is the first report under the new team's banner, and the first Counter Adversary Operations product offering, Identity Threat Hunting, was launched at the Las Vegas conference.

Identity Threat Hunting launches immediately as part of CrowdStrike Falcon OverWatch Elite at no additional cost. According to an accompanying press release, the offering "makes it possible to quickly identify and remediate compromised credentials, track lateral movement,

and outpace adversaries with always-on, 24/7 coverage."

"The new mandate is to really use the collective capability of the threat hunting and threat intelligence teams, which I don't think anybody is really doing at this point in the industry," Meyers explained. "We are taking those two teams and colocating them, so we are in a better position to have a more disruptive impact against adversaries and make it harder for them to operate."

*Alexander Culafi is a writer, journalist and podcaster based in Boston.*

### Next Steps

CrowdStrike 'Global Threat Report': Cloud intrusions up 75%

### Related Resources

- XDR and Container Security: A Holistic Approach to Threat Detection and Response – Replay
- EDR, MDR, XDR: What they are, how they work, and how to choose –Replay
- Adapting to a New Paradigm in Security: Implementing Identity Threat Detection ... – Replay
- AI-Powered Security Operations: From Promise to Reality –Replay

### Dig Deeper on Threat detection and response

- 
  CrowdStrike apologises to US government for global mega-outage


By: Alex Scroxton

- 
  CrowdStrike exec apologizes to Congress, shares updates

By: Makenzie Holland

- 
  Risk & Repeat: Cyber Safety Review Board takes Microsoft to task

By: Alexander Culafi

- 
CrowdStrike 'Global Threat Report': Cloud intrusions up 75%


By: Alexander Culafi