CROWDSTRIKE

Sector Under Attack: Healthcare

Big game hunting (BGH) and targeted intrusions remain key threats to the healthcare sector.

84 out of 245+

adversaries currently tracked by CrowdStrike target healthcare[1]

Attack Advancements in Healthcare

↑75%

year-over-year increase in eCrime intrusions in 2023[2]

↑142%

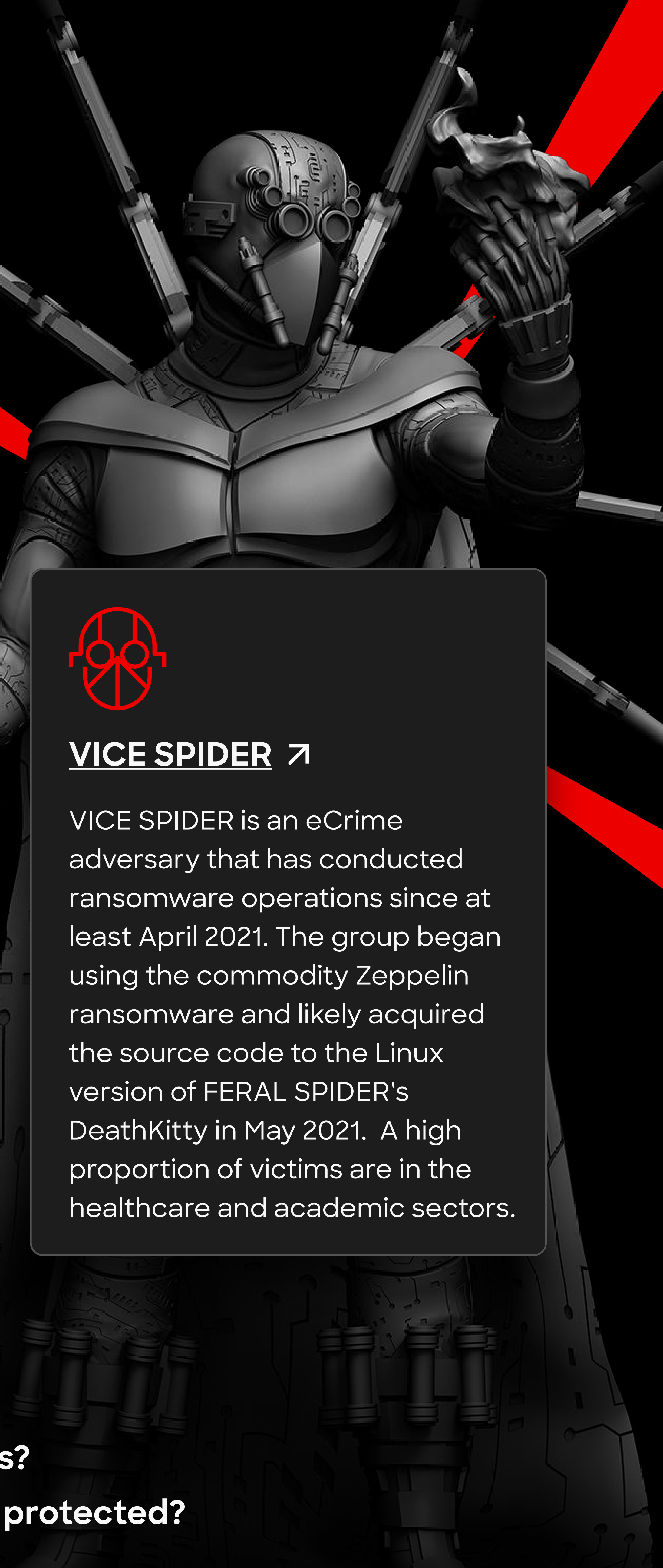
increase in access broker advertisements[3]

↑176%

increase in data leakage exfiltration activity[4]

How Adversaries Achieve Their Objectives

- **Exploit** legitimate credentials to gain access and extend presence without raising alarms
- **Adapt** sophisticated hands-on-keyboard attacks to evade detection
- **Focus** on cross-domain tradecraft to maintain persistence, move laterally and exfiltrate data



Key Adversaries Targeting Healthcare Institutions

GRACEFUL SPIDER ↗

Active since 2016, GRACEFUL SPIDER develops and operates Clop ransomware, focusing on BGH and point-of-sale malware for payment card theft. In 2023, the group exploited zero-day vulnerabilities in file transfer applications targeting U.S.-based healthcare entities for data theft.

BITWISE SPIDER ↗

This eCrime adversary is responsible for the development of LockBit ransomware and the StealBIT information stealer. BITWISE SPIDER relies on credential brute-forcing and software supply chain compromises to gain initial access.

VICE SPIDER ↗

VICE SPIDER is an eCrime adversary that has conducted ransomware operations since at least April 2021. The group began using the commodity Zeppelin ransomware and likely acquired the source code to the Linux version of FERAL SPIDER's DeathKitty in May 2021. A high proportion of victims are in the healthcare and academic sectors.

Questions for Defenders

- **Do you know who is targeting you?**
- **Are you prepared for the latest adversarial tactics and techniques?**
- **Are all of your user credentials, cloud assets and endpoint assets protected?**

Visit the Adversary Universe or download the CrowdStrike 2024 Threat Hunting Report

[1] Adversaries tracked by CrowdStrike Counter Adversary Operations as of 12/2/2024

[2] CrowdStrike 2024 Threat Hunting Report

[3] CrowdStrike 2024 Threat Hunting Report

[4] Falcon Advesary Intelligence Premium report CSECR-24025

November 2024