Key insights of the report

- The ransomware threat landscape is seeing a concerning shift in tactics. The rampant abuse of zero-day and one-day vulnerabilities in the past six months led to a 143% increase in victims when comparing Q1 2022 with Q1 2023.
- Ransomware groups now increasingly target the exfiltration of files, which has become the primary source of extortion, as seen with the recent exploitation of GoAnywhere and MOVEit. This underscores the fact that file backup solutions, though effective against file encryption, are no longer a sufficient strategy.
- In some cases, the same victim was attacked twice by different ransomware groups. Akamai research finds victims of multiple ransomware groups are almost 6x more likely to experience a subsequent attack within the first three months of the initial attack. It's a race against time for organizations to close the gaps in their environment because of the likelihood of being attacked by another group.
- Ransomware groups, such as CL0P, are aggressively pursuing the attainment and development of zero-day vulnerabilities in-house. This has proven to be a successful strategy, with CL0P growing its number of victims by 9x from Q1 2022 to Q1 2023.
- LockBit dominates the ransomware scene with 39% of total victims (1,091 victims), more than quadruple the number of the second-highest ranked ransomware group. It has risen significantly in the absence of the previous front-runner, Conti, with its victim count increasing by 92% from Q4 2022 to Q1 2023.
- Attacks against specific verticals grew as well, with the number of manufacturing victims growing by 42% between Q4 2022 and Q4 2021, and the number of healthcare victims growing by 39% between Q4 2022 and Q4 2021.
- Two trends stand out from our analysis: First, a continuous activity from ransomware groups that may be dependent on variables like the group size and its resources; second, significant upticks in activities when critical zero-day vulnerabilities are exploited, such as CL0P's aggressive exploitation of highly targeted security flaws.
- Regulations enforced by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) may make it illegal to pay ransom to certain parties or