Corero SmartWall® *Threat Advisory*

DDOS Cyberattack risks rise as Russia aggression continues against Ukraine

Advisory ID: 022422-1
Published: 1 March 2022

Summary

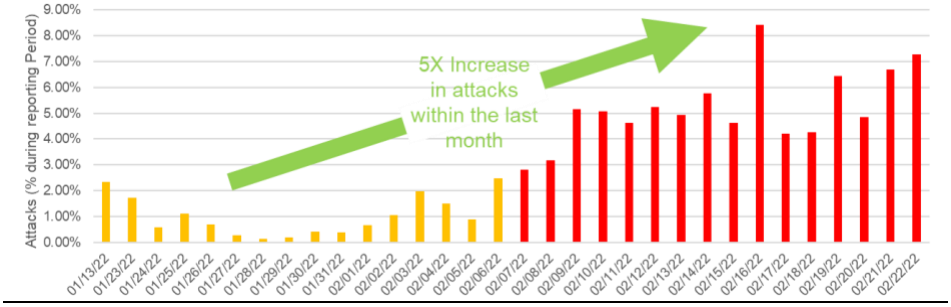
The Corero SecureWatch DDoS Threat Intelligence team has observed an increase in DDoS attacks against customers in the Eastern European region over the recent weeks, which is consistent with news reports of DDoS attacks targeting several Ukrainian banks and government agencies.

Although we have yet to register a statistically significant increase in DDoS activity in other global regions, Corero is predicting that the increasing global sanctions against Russia will trigger state-sponsored DDoS attacks towards the countries imposing them.

All the attacks detected by Corero, so far, have been successfully and automatically mitigated by our SmartWall® Solution, ensuring business continuity was preserved.

Threat Vector

The DDoS vectors being used are numerous and varied but have not changed significantly. However, there is a notable fivefold (5x) increase in attacks against customers in the Eastern European region:



Recommended Action: SecureWatch Customers

SmartWall DDoS protection solutions mitigate a wide range of known and zero-day attacks, all while maintaining the availability of applications and services being protected and without disrupting the delivery of legitimate traffic. They are designed to handle large DDoS floods, reflective amplified spoof attacks, as well as attacks that are typically too low, or short, to be mitigated manually, or by traditional out-of-band solutions.

Corero customers using the latest software releases and recommended SmartWall protection settings are comprehensively defended from this increase in DDoS activity.

Please contact Corero Support if you have any questions.