Over the last 48 hours, the Check Point Incident Response Team (CPIRT) has seen a marked increase in DDoS attacks against multiple targets globally. This increase has yet to be directly attributed with a specific threat actor, but confidence is high that some activity is related to the COVID-19 pandemic.

**Targets have included:**

- Central Government
- Banking
- Medical
- Energy
- Retail

We have seen DDoS attacks utilized multiple different methods, including:

- SYN Attacks
- Reflection Attacks
- Volumetric Attacks
- DNS – Cache busting Attacks and DNS Volumetric Attacks

It is vital that customer prepare for DDoS attacks before they occur, during an attack it’s too late. Ensuring you have a plan is vital and having a solid IR plan around DDoS and tested before an attack will ensure continued operations.

**Key items to consider**

- Cloud Based Scrubbing

As always, if you need the assistance, IntraSystems and the Check Point Incident Response Team is available 24x7x365 - [https://www.checkpoint.com/support-services/threatcloud-incident-response/](https://www.checkpoint.com/support-services/threatcloud-incident-response/). Please call our Support Team, Monday – Friday, 8:30 AM – 5:30 PM at 781.986.1700 x3 if you have any questions or need assistance.