

Serangan DDoS naik 100 kali ganda, catat 3,000 minit pada suku kedua 2022 - Kaspersky

Bernamea

Ogos 5, 2022 20:16 MYT



DDoS ialah jenayah siber yang mana penyerang membanjiri pelayan dengan trafik internet untuk menghalang pengguna daripada mengakses perkhidmatan dalam talian dan laman web. - Gambar hiasan

KUALA LUMPUR: Serangan Penafian Perkhidmatan Teragih (DDoS) mencapai tahap baharu kerana bahagian serangan pintar dan tempoh purata menyaksikan peningkatan mendadak sehingga 100 kali ganda, mencecah 3,000 minit, pada suku kedua tahun ini (S2 2022) berbanding dengan tahun sebelumnya, kata Kaspersky.

DDoS ialah jenayah siber yang mana penyerang membanjiri pelayan dengan trafik internet untuk menghalang pengguna daripada mengakses perkhidmatan dalam talian dan laman web.

Syarikat keselamatan siber global itu dalam laporan DDoS suku tahunannya, berkata bahagian serangan pintar hampir memecahkan rekod empat tahun, menyumbang hampir 50 peratus daripada jumlah itu dan pakar juga menjangkakan peningkatan dalam keseluruhan aktiviti DDoS, terutamanya dengan kejatuhan mata wang kripto baru-baru ini.

Ia berkata, serangan DDoS direka untuk menghalang fungsi normal laman web atau merosakkan sepenuhnya, yang biasanya menasarkannya institusi kerajaan, syarikat runcit atau kewangan, media atau organisasi lain.

"Mangsa akan kehilangan pelanggan kerana laman web telah hilang dan menjejaskan reputasi mereka.

"Berbanding dengan S1 2022, yang tidak pernah berlaku sebelum ini untuk DDoS sebagai hasil daripada aktiviti penggadam, angka S2 juga menunjukkan peningkatan sebanyak tiga kali ganda," katanya.

Ia berkata beberapa serangan pada suku sebelum ini berlangsung selama beberapa hari atau minggu dengan rekod yang dicatatkan ialah 41,441 minit, iaitu kurang sedikit daripada 29 hari.

Pakar Keselamatan Kaspersky, Alexander Gutnikov berkata, adalah sangat mahal untuk meneruskan serangan dalam jangka masa yang lama, terutamanya jika ia tidak berkesan kerana disekat oleh penyelesaian perlindungan.

"Apabila robot internet (bot) yang boleh menjadi perisian hasad (malware) sentiasa aktif, ia boleh meningkatkan risiko kehilangan jaringan robot (botnet), kegagalan alat peranti (node) atau meningkatnya pengesanan dari pusat kawalan.

"Tempoh serangan yang ekstrem ini dan peningkatan bilangan serangan DDoS pintar dan bersasar membuatkan kami tertanya-tanya tentang keupayaan, gabungan profesional dan sumber pembiayaan pelakunya," katanya.

Kaspersky berkata laporan itu menunjukkan bahawa setiap serangan kedua pada S2 2022 yang dikesan oleh produk Kaspersky adalah pintar, bermakna pelakunya melakukan persediaan yang agak canggih.

Ia berkata dari segi jumlah serangan DDoS, S2 menyaksikan lebih rendah daripada S1 yang merupakan fenomena biasa kerana penurunan dalam aktiviti DDoS akan berlaku apabila musim panas semakin hampir.

Bagaimanapun, menurut sistem Perisikan DDoS Kaspersky, dinamik bilangan serangan DDoS dalam suku tersebut tidak sepadan dengan corak biasa tahun ini.

Ia berkata aktiviti botnet terus berkembang sepanjang S2 selepas kelembapan pada penghujung S1, menyebabkan lebih banyak aktiviti pada bulan Jun berbanding April dan ini konsisten dengan penurunan mata wang kripto, yang biasanya merangsang DDoS.

"Kejatuhan mata wang kripto bermula dengan kejatuhan Terra (Luna) dan hanya mendapat momentum sejak itu.

"Pelbagai faktor menunjukkan bahawa kecenderungan itu mungkin berterusan, contohnya, pelombong kripto menjual ladang pada harga rendah kepada pemain," kata Gutnikov.

Beliau menambah bahawa ini boleh membawa kepada lonjakan dalam aktiviti DDoS global.