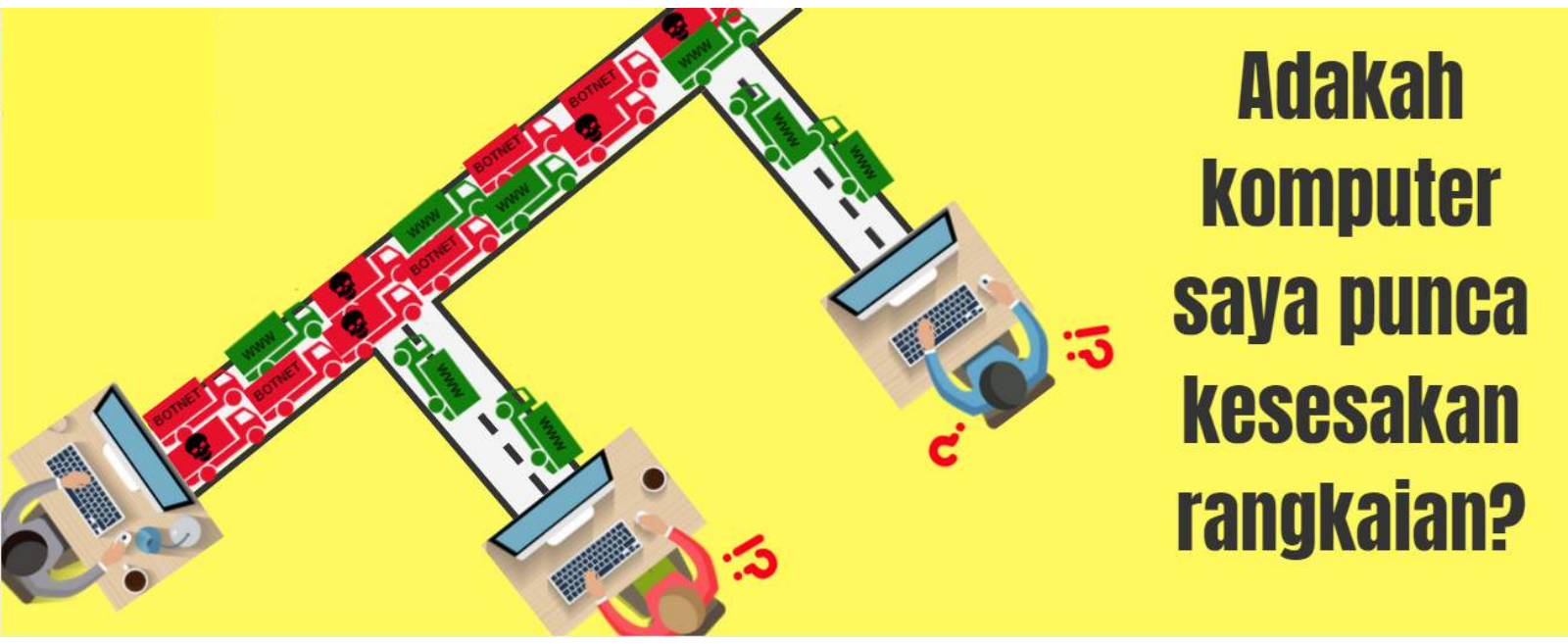


Kesesakan rangkaian Universiti boleh menjejaskan capaian pengguna ke internet dan Sistem Maklumat Universiti (SMU). Pengguna akan mendapati transaksi atas talian yang dilakukan mengambil masa yang lama atau sentiasa terputus. Kesesakan rangkaian boleh disebabkan oleh serangan *Distributed Denial of Service* (DDoS) yang berpunca daripada komputer yang dijangkiti Botnet.

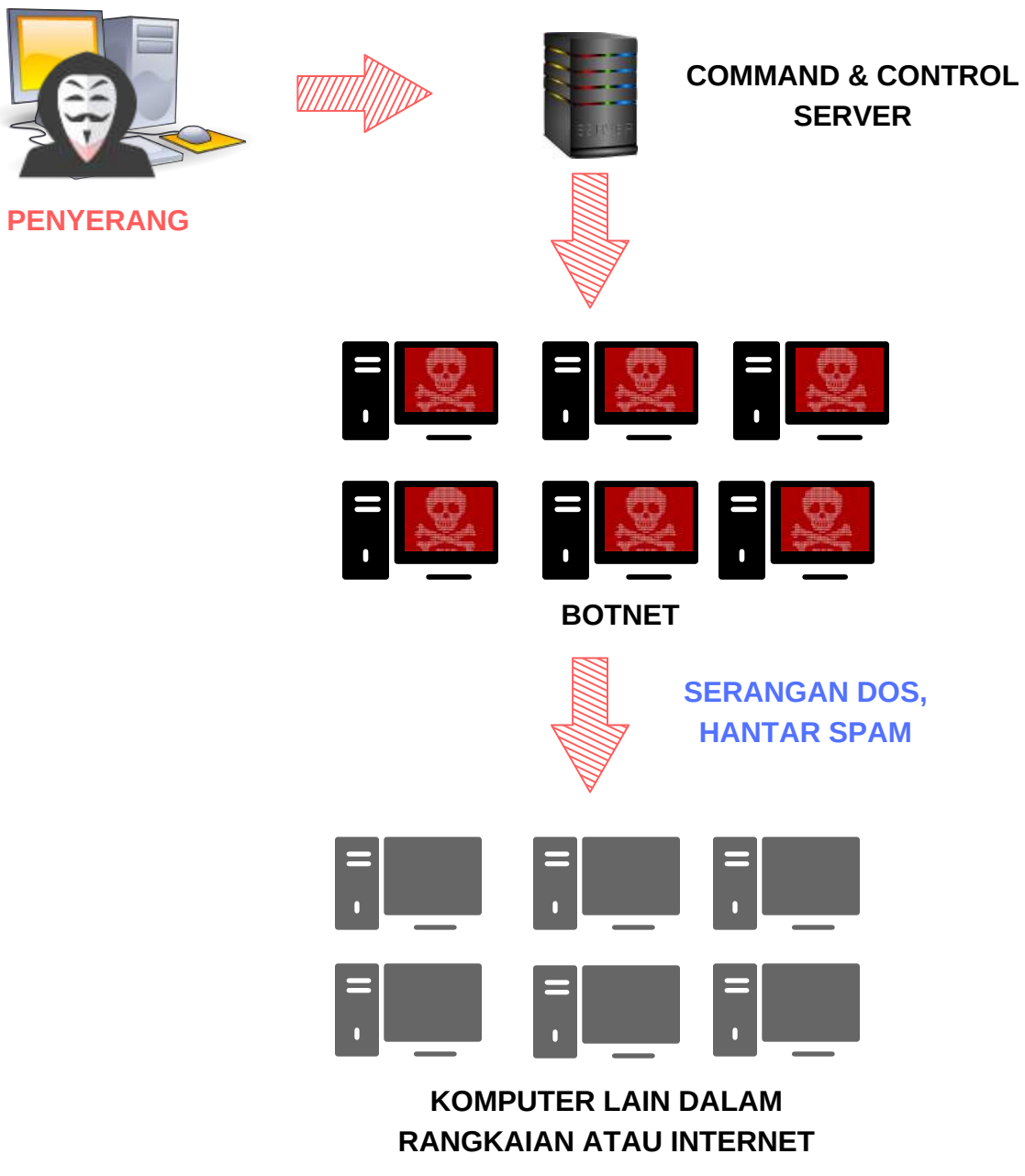
APA ITU BOTNET?

Botnet adalah satu rangkaian komputer dikenali sebagai 'bots' yang dikawal secara jauh oleh pihak tertentu dengan niat jahat. Sebelum komputer menjadi 'bots', ia sebenarnya telah dijangkiti oleh malware (perisian jahat) yang membolehkan pihak lain mengawalnya secara jauh dengan tujuan untuk mencuri maklumat atau melancarkan serangan kepada komputer lain.

APA ITU DDOS?

Serangan Distributed denial-of-service (DDoS) atau serangan DDoS berlaku apabila komputer yang telah dijangkiti Botnet digunakan untuk mensabotaj laman web atau server.

Penyerang memberi arahan kepada komputer-komputer ini untuk menghubungi laman web atau server yang disasarkan secara berterusan atau menghantar data yang banyak (spam) sehingga jumlah trafik meningkat. Situasi ini akan memberi bebanan kepada laman web atau server serta menyebabkan capaian yang perlahan kepadanya dan boleh juga melumpuhkan keseluruhan operasi.



ADAKAH KOMPUTER ANDA SALAH SATU DARIPADA 'BOTS'?

Kebanyakan pengguna tidak menyedari komputer mereka telah dikompromi. Berikut adalah beberapa perkara yang memberi petunjuk komputer anda mungkin telah dijangkiti:

- Capaian ke internet menjadi sangat perlahan.
- Banyak iklan atau 'pop-up windows' yang muncul semasa menggunakan pelayar web (web browser).
- Terdapat komponen pada pelayar web (web browser) yang tidak dimuat turun oleh anda.
- Komputer gagal berfungsi secara tiba-tiba.
- Program-program dalam komputer berfungsi dengan perlahan.
- Komputer mengambil masa yang lama untuk 'shutdown' atau terdapat ralat semasa 'shutdown'.
- 'Setting' pada komputer telah diubah tetapi anda tidak dapat kembalikan 'setting' yang asal.
- Kenalan atau keluarga anda menerima e-mel daripada anda, tetapi anda tidak pernah menghantar e-mel tersebut.

BAGAIMANA CARA UNTUK MELINDUNGI KOMPUTER DARIPADA BOTNET?

- Lindungi kata laluan anda
- Pasang perisian antivirus/antimalware yang berkualiti dan pastikan ia terkemaskini (updated)
- Pastikan semua perisian dalam komputer sentiasa dikemaskini.
- Jangan klik pautan yang mencurigakan.
- Berhati-hati semasa memuat turun fail yang dilampirkan pada e-mel.
- Elakkan melakukan perkongsian fail dalam rangkaian atau memuat turun fail melalui P2P.
- Jangan guna 'thumb drive' pada komputer yang telah dijangkiti.

KOMPUTER SAYA DIJANGKITI 'BOTNET'. APA YANG PERLU SAYA LAKUKAN?

- Jika komputer anda tiada perisian antivirus, pasang perisian antivirus yang disediakan oleh PTM (untuk komputer hakmilik UKM) atau perisian antivirus yang lain (untuk komputer persendirian) dan laksanakan proses imbasan (scanning).
- Sekiranya perisian antivirus tidak dapat menghapuskan malware yang menjangkiti komputer anda, mohon hubungi Pusat Teknologi Maklumat (PTM) untuk bantuan lanjut melalui:
  a) sistem aduan eFACt atau
  b) talian hotline PTM - 7070