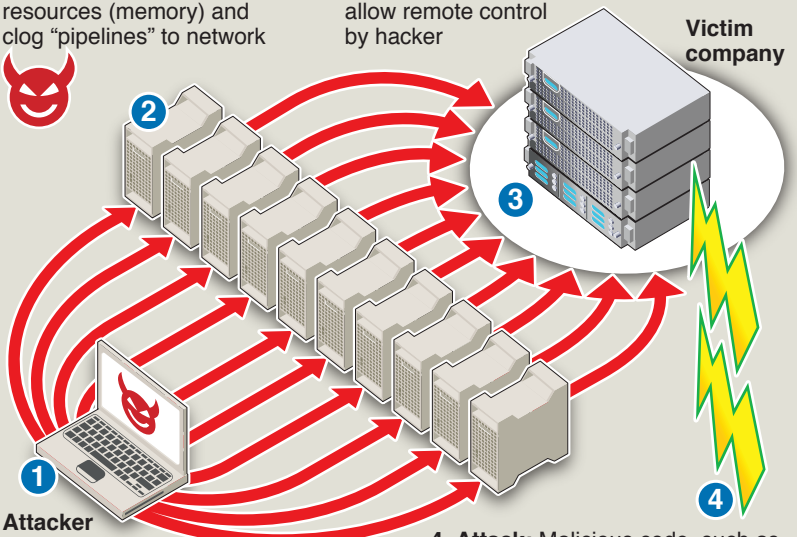
Cyber smokescreen to steal data

Distributed denial-of-service (DDoS) assaults – which overwhelm an online service with fake requests – are increasingly being used to mask attacks to steal sensitive information from a company

1. Attacker: Launches DDoS assault to exhaust server resources (memory) and clog "pipelines" to network

2. Botnets: Large clusters of cellphones, PCs or routers, infected with malware, allow remote control by hacker



3. Firewall: DDoS assault does not breach security perimeter but forces IT team to mitigate damage, masking real attack

4. Attack: Malicious code, such as ***SQL-injection,*** tells database server to bypass authentication and retrieve customers' bank and credit card details

DDoS attacks detected
(Oct 1-7, top five countries affected)

U.S.	**256,212**
Russia	**211,948**
France	**118,670**
India	**34,809**
Germany	**30,732**

652,371 DDoS attacks in seven days

74% of DDoS attacks are smokescreens for other attacks…

482,754 other attacks

126,516

…of which **26%** are sensitive data theft

Source: Kaspersky Lab Denial of Service report