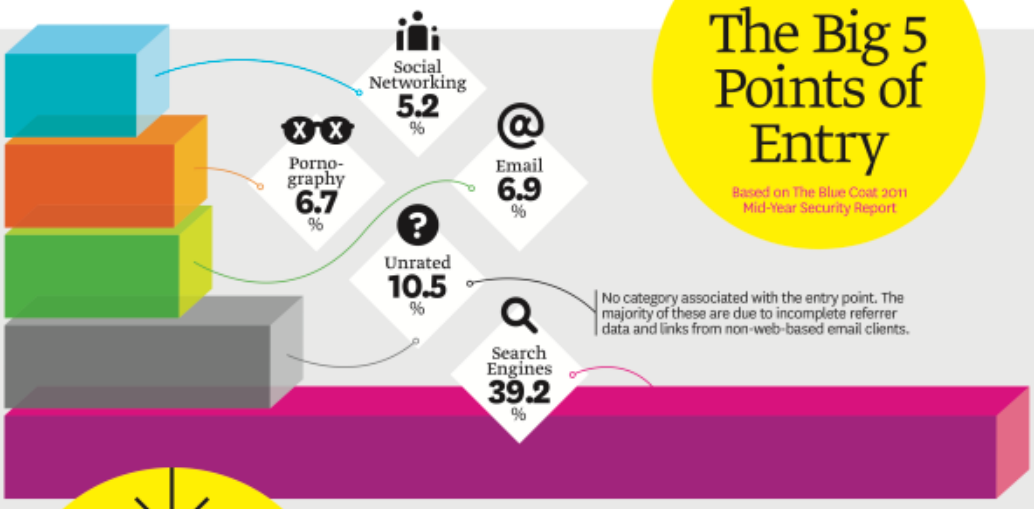
Blue Coat

Malware Networks

A malware delivery network gathers unsuspecting users, usually when they are visiting trusted sites, and routes them to malware, via relay, exploit and payload servers that continually shift to new domains and locations.

The Big 5 Points of Entry

Based on The Blue Coat 2011 Mid-Year Security Report



No category associated with the entry point. The majority of these are due to incomplete referrer data and links from non-web-based email clients.

Largest Malware Networks

SHNAKULE
MAX. HOSTS 4,357
AVG. HOSTS 2,001

ISHABOR
MAX. HOSTS 1,140
AVG. HOSTS 766

CINBRIC
MAX. HOSTS 1,602
AVG. HOSTS 505

NAARGO
MAX. HOSTS 299
AVG. HOSTS 199

VIDZEBAN
MAX. HOSTS 347
AVG. HOSTS 156

4,107 The average number of unique host names per day for the top 10 malware delivery networks

50 The average number of malware delivery networks operating per day

40,180 The average number of user requests per day for the top 10 malware delivery networks

Top 5 Points for Business

1. Image searches are the most dangerous activity users can engage in on the web.
2. Pornography, Placeholders, Phishing, Hacking, Online Games and Illegal/Questionable categories should always be blocked.
3. Malware hosting is often found within categories that are typically allowed in acceptable use policies, such as Online Storage and Software Downloads.
4. A single defense layer, such as a firewall or anti-virus software, will leave users vulnerable to malware.
5. A real-time defense that leverages a collaborative community for intelligence is the best protection against dynamically changing malware.

The Blue Coat 2011 Mid-Year Security Report examines web-based malware ecosystems, including user entry points, the networks that deliver malware and the type of sites where malware is typically hosted.

Blue Coat