2016 Midmarket Threat Summary

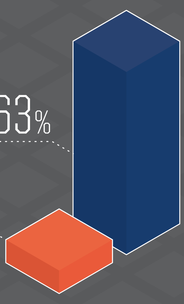
Key Insights

Rudimentary Attacks Pose Greatest Risk to Midsized Organizations

Top Ranking Attacks

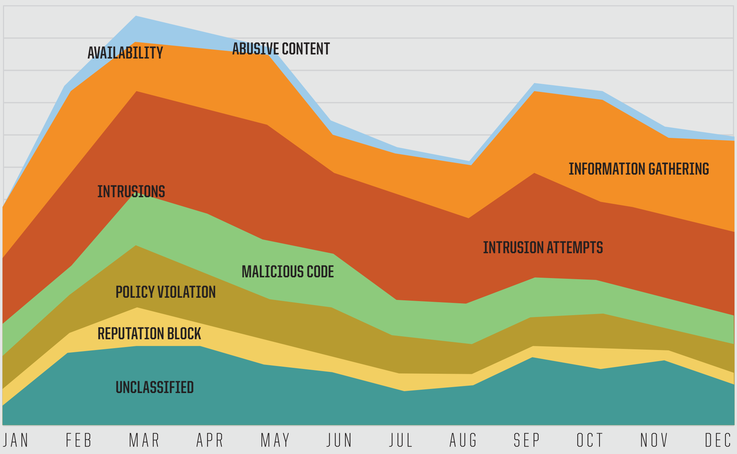
Intrusion Attempts (primarily web attacks), Information Gathering, Policy Violations — 63%

Malicious code related attacks — 12%



Threat Volume Analysis

March to April and September to October were the most intense periods of threat events throughout the year, with March being the most active month, and June to July being the least active.



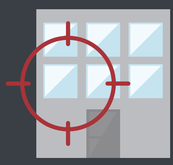
Key Takeaways

Rudimentary attacks pose the greatest risk

Cybercriminals are moving away from sophisticated malicious code attacks, with the majority of attackers preferring inexpensive and automated methods of intrusions, exploiting 'low hanging fruit' (representing almost 30% of all observed events). This trend is expected to continue so long as these techniques are successful.

Every organization is a target

With easier access than ever before to simple and automated tools, cybercriminals can quickly and easily stage attacks against every business. Attacks, such as ransomware, can reap financial gains without the painstaking effort required to identify and extract high value information from an organization's network.



Detecting and disrupting the common methods and tools used will make attacks less effective

Take steps to minimize the attack surface and tailor security controls. Doing so directly impacts cybercriminal rationale when choosing attack targets.

Organizations can use seasonal threat trends to align security efforts to their advantage

For example, security awareness training is most effective when applied between December to March, ahead of the busiest time for threat activity, which is March to April.

READ THE COMPLETE REPORT