## 1.1 ASEAN countries have emerged as launchpads for cyberattacks

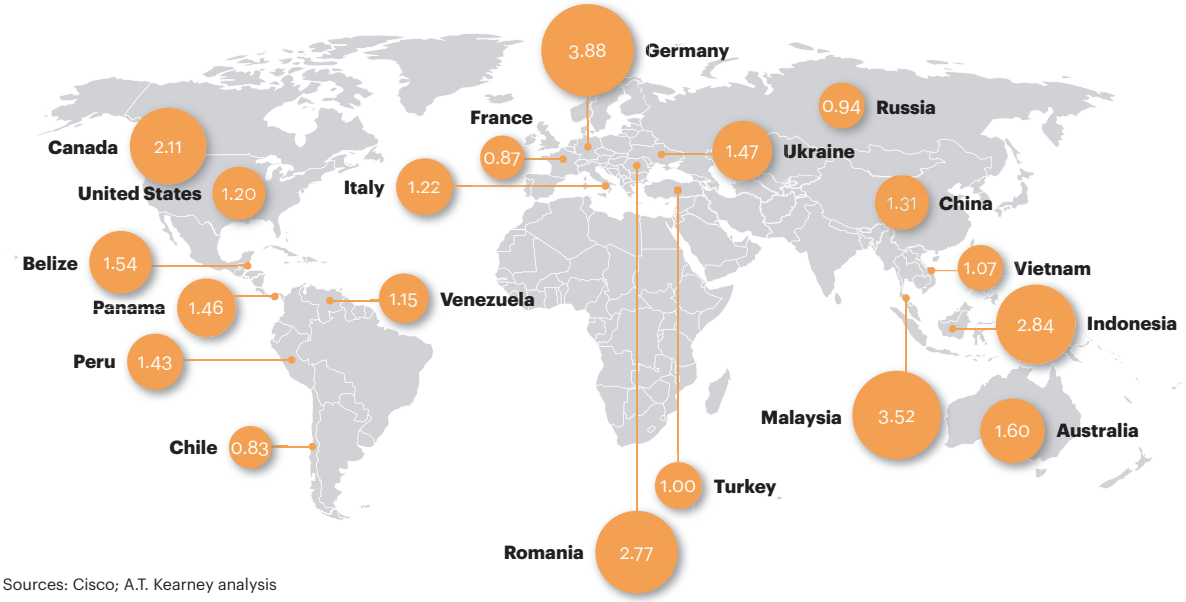
ASEAN countries are being used as launchpads for cyberattacks—either as vulnerable hotbeds of unsecured infrastructure where numerous computers can be infected easily for large-scale attacks or as hubs for a single point of attack to gain access to the hubs' global connections.

Malaysia, Indonesia, and Vietnam are global hotspots for major blocked suspicious Web activities—up to 3.5 times the standard ratio, indicating that these countries are being used to launch malware attacks (see figure 3). Spam botnets are also finding ASEAN countries to be attractive hosts for their attacks. For example, Vietnam registered 1.68 million IP blocks from December 2015 to November 2016, and the country is number five in the world's top countries from which attacks against IoT devices originated in 2016.[7, 8]

> "In our country, there are still many weaknesses in information security, including lack of awareness and action plans at leadership levels, lack of policies to promote human resource development and nurture talent in information security, and a lack of cohesiveness amongst information security stakeholders in general."
>
> **—ASEAN national CERT**

Figure 3

**Blocked suspicious Web activity, by country of origin (expected ratio = 1.0)**




Sources: Cisco; A.T. Kearney analysis

[7] IP blocks are spam messages that are blocked immediately by spam-detecting technology because the sender has a bad reputation score. Examples include messages that originate from known spam-sending botnets or compromised networks.

[8] *Internet Security Threat Report Volume 22*, Symantec, April 2017