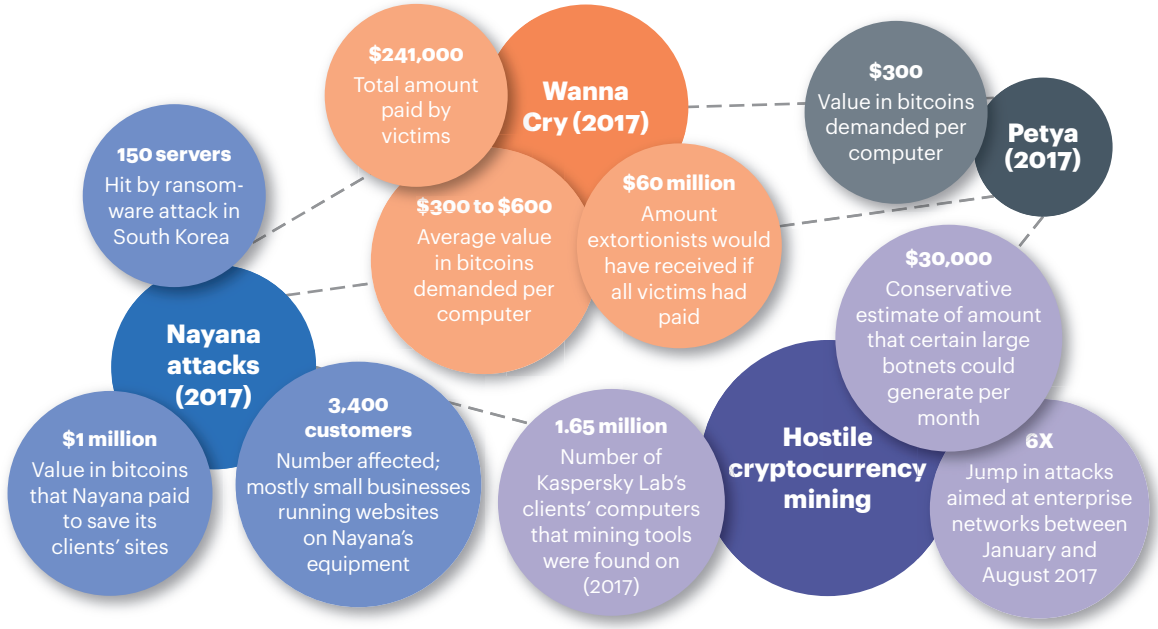
evade detection and to secure their malicious activities. The overall increases in encrypted traffic and attacks render threat recognition difficult and create gaps in traditional, layered-defense systems because intrusion prevention fails to occur.

Encrypted traffic analytics provide insight into threats in encrypted traffic using network analytics.[25] The focus is on identifying malware communications in encrypted traffic through passive monitoring, the extraction of relevant data elements and supervised machine learning with cloud-based global visibility.

The increasing uptake of virtual currency

Since Bitcoin, the first decentralized cryptocurrency, was released in early 2009, similar digital currencies have crept into the worldwide market, including a spin-off called Bitcoin Cash. Abuse of virtual currencies is on the rise (see figure 17).

Figure 17
Virtual currency is increasingly a target for cyberattacks



Source: A.T. Kearney analysis

Security experts have seen a spike in attacks over the past year, aimed at stealing computer power for cryptocurrency mining operations.[26] Researchers have detected several large botnets set up to profit from cryptocurrency mining along with a growing number of attempts to install mining tools on organizations' servers.

Illegal mining operations set up by insiders, which can be much more difficult to detect, are on the rise. These are often carried out by employees with high-level network privileges and the technical skills needed to turn their company's computing infrastructure into a currency mint.

[25] *Encrypted Analytics Traffic*, Cisco

[26] "Hijacking Computers to Mine Cryptocurrency Is All the Rage," *MIT Technology Review*, 5 October 2017