Issued 8/1/18

Starting at $40, Hackers can Attack your Business with Services Bought on the Dark Web

A study by Positive Technologies [link] identified major cyber incidents have increased by 32% between Q1 2017 and Q1 2018. Through their analysis, the organization found that the rise in attacks can be attributed to ready-made malware. Positive Technologies then analyzed 25 dark web sites to examine the costs of cybercrime services across the darkweb. With remote desktop protocol (RDP) access to businesses being sold on the dark web for 10 bucks [link], users have already seen how easily they can be compromised. However, the inexpensive hacking tacts don't stop at RDP—and some of them are shockingly low. Here are the costs of different cybercrime services, according to Positive Technologies:

- Hacking email: $40
- DDoS attack: $50
- Hacking website: $150
- Stealing payment data $270
- Infecting with Trojan for mining: $300
- Infecting with ransomware Trojan: $750
- Stealing from ATM: $1,500
- Targeted attack: $4,500

Starting at $40, hackers can infiltrate a business' email and steal sensitive information. With the price of attacks starting so low, cybercrime isn't directed only at big business. Some 71% of SMBs are not prepared for cybersecurity risks, and with how cheap it is to attack, they need to shore up their defenses.

SMBs can begin by conducting detailed digital risk assessments—check out this article for more tips on how SMBs can protect themselves.