New Horizons Computer Learning Centers

THE STATE OF CYBERSECURITY IN 2018

As cyberattacks continue to increase, the threat landscape and defense techniques in IT are constantly shifting to combat issues. Now more than ever, defenders are evolving their own set of technological advances to combat threats.

What you need to know

CYBERATTACKS ARE INCREASING, BUT THE METHODS EMPLOYED REMAIN RELATIVELY STATIC

The number of attacks is rising, and practitioners indicate that the upward trend will continue throughout the near-to intermediate term. Despite an increase in the overall numbers of attacks, techniques employed by attackers remain relatively constant. Some methods of attack (i.e. Phishing) show a slight increase relative to other categories of attacks.

MOTIVATION REMAINS MONETARY, AND RANSOMWARE COUNTERMEASURES ARE NEARING UBIQUITY.

Most attacks are still monetary in nature; they are perpetrated mostly by cybercriminals rather than state actors or politically motivated actors. Enterprises have shifted strongly in favor of better preparation for ransomware relative to last year.

RANSOMWARE IS BEING DISPLACED, MOST LIKELY BY CRYPTOCURRENCY MINING

Ransomware is decreasing as enterprises defend against it more effectively. Alternate strategies, such as cryptocurrency mining, demonstrate effectiveness and better (although different) economic characteristics. This may be, in large part, underpinned by unwillingness to pay the ransom among potential victims.

THREAT INTELLIGENCE IS PREVALENT—ACTIVE DEFENSE IS LESS FAMILIAR BUT EFFECTIVE

Most enterprises employ some threat intelligence capability, often staffed in-house. Active defense strategies, although not understood universally among practitioners or employed in enterprises, demonstrate a high level of success when implemented.

Source: “State of Cybersecurity 2018 Part 2: Threat Landscape and Defense Techniques.” ISACA.com, 2018.