New Horizons
Computer Learning Centers

3 Cyber Trends That Are Still Relevant in 2019

As new threats emerge from the changing landscape, three cyber threats from 2018 are still relevant today.

Targeted ransomware
This approach gained popularity in 2018 and has proven effective in 2019; not a week goes by without some kind of tailored destructive ransomware attack hitting the headlines. One such prominent attack vector utilizes Emotet's vast distribution and victim base to select lucrative targets. Emotet is used to spread TrickBot within the compromised corporate network which, in turn, deploys Ryuk or another ransomware as the final payload.

Cryptomining and cryptominers
They remain a prevalent malware type in the first half of 2019's threat landscape. Despite the shut-down of the notorious drive-by mining service 'CoinHive' this March, which led to a decrease in the popularity of cryptominers among threat actors, it resulted in threat actors adopting a new approach regarding cryptominers, aiming at more rewarding targets than consumer PC's and designing more robust operations.

DNS Attacks
Targeting one of the most important mechanisms that govern the internet, the Domain Name System (DNS), such attacks target DNS providers, name registrars, and local DNS servers belonging to the targeted organization and are based on the manipulation of DNS records. DNS takeovers can compromise the whole network and enable multiple attack vectors: control of email communications, redirection of victims to a phishing site, and more. One of the biggest advantages DNS attacks provide is the option to issue legitimate looking certificates by Certificate Authorities which rely on DNS to verify that you are the legitimate holder of the domain in question.

Source: "Cyber Attack Trends: 2019 Mid-Year Report," Check Point Research, August 2019.