CYBER SECURITY:
HUMAN OPERATED RANSOMWARE ON THE RISE

By: Jack Gerbs
Quanexus

The cost of ransomware attacks in 2021 are projected to reach $20 Billion, almost double the cost impact from 2019. A ransomware attack occurs after a criminal has gained access to a system through a phishing attack or stolen credentials. A typical ransomware attack encrypts data, which stops the company from doing business until the ransom is paid. In a human operated ransomware attack, the criminals gain access to a business network and move around the network to see what they can find.

Microsoft does a good job explaining the difference between the two attack methods:

“Human-operated ransomware attacks are a cut above run-of-the-mill commodity ransomware campaign. Adversaries behind these attacks exhibit extensive knowledge of systems administration and common network security misconfigurations, which are often lower on the list of ‘fix now’ priorities.

Once attackers have infiltrated a network, they perform thorough reconnaissance and adapt privilege escalation and lateral movement activities based on security weaknesses and vulnerable services they discover in the network.”

Hackers can use the business infrastructure to mine bitcoin, run SPAM campaigns, or use company workstations for other criminal activities. Only after they have exploited the private infrastructure do they then execute a typical ransomware attack by encrypting data and asking for money. These criminals can live in a company network for months, using the business infrastructure for their gains.

These ‘hands on keyboard’ attacks are more time consuming for the criminal, but they can also be much more profit-able, which is why we are seeing the increase. While malware attacks are on the decline, ransomware attacks increased 40% last year. Criminals are focusing time and effort on these more elaborate attacks that yield greater gains.

Preventing these targeted attacks starts with education as always. The criminal has to get into the network first. Continued education on phishing campaigns and password management is critical. Additionally, a layered security approach is the best defense along with network monitoring tools. These tools can alarm IT departments to unusual network activity like using workstations to mine bitcoin. road.

Five Cybersecurity Statistics

77% of organizations saw more or the same number of cyberattacks over the past year.

15% of organizations closed their business because of a cyberattack.

62% of organizations anticipate an attack in the next 12 months.

70% of organizations plan to increase their cybersecurity budget

58% of organizations believe they will face an insider security threat over the next year.