Microsoft says ransomware is fastest growing scam attempt

30 September 2020, by Jefferson Graham, Usa Today

Credit: CC0 Public Domain

Hack attempts are on the rise—as always—with ransomware the most common now, according to Microsoft.

In a new report on "digital defense," Microsoft says it blocked over 13 billion malicious and suspicious emails in the last year, and more than 1 billion of them were URLs set up for to launch phishing credentials attack.

Phishing is when emails or texts are sent to people with normal looking links that in fact are toxic, and let the hacker take over your system.

Attackers often send emails imitating top brands, noted Microsoft. The top spoofed brands used in these attacks were Microsoft, UPS, Amazon, Apple and Zoom.

Hackers "have rapidly increased in sophistication over the past year, using techniques that make them harder to spot and that threaten even the savviest targets," the report says. "For example, nation-state actors are engaging in new reconnaissance techniques that increase their chances of compromising high-value targets, criminal groups targeting businesses have moved their infrastructure to the cloud to hide among legitimate services, and attackers have developed new ways to scour the internet for systems vulnerable to ransomware."

Microsoft sees ransomware, the natural next step for phishing, as a major growing threat. This is when the hacker hijacks your system, and won't let you back in unless you pay the ransom fee.

Attackers have taken advantage of the COVID-19 pandemic to reduce their "dwell time" within a victim's system, the report adds, compromising and exfiltrating data or ransoming quickly. Attackers were under the impression that there would be an increased willingness to pay as a result of the coronavirus outbreak.

Some cybercriminals have gotten so good at what they do that they were able to take over an entire network in 45 minutes, says Microsoft.

What to do?

People need to be diligent about their online security, and take password strength more seriously. "Given the frequency of passwords being guessed, phished, stolen with malware or reused, it's critical for people to pair passwords with some second form of strong credential," Microsoft says.

Organizations need to mandate the use of two-factor authentication for employees, which requires typing in the password twice, the tech giant recommends..