CYBER UPDATE

WINTERS-OLIVER
INSURANCE AGENCY, INC.

Officials Saw More Professional Cybercriminals and Infrastructure Attacks in 2021

Ransomware attacks on critical infrastructure increased in 2021, hitting 14 of the 16 critical infrastructure sectors in the United States, according to a report from cybersecurity authorities in multiple countries.

Ransomware trends and recommendations were laid out in a Joint Cybersecurity Advisory, coauthored by cybersecurity agencies in the United States, United Kingdom and Australia. The report noted that evolving tactics and techniques of cybercriminals demonstrated their growing sophistication and their increased threat to organizations globally.

Officials cited attacks on critical sectors like the defense industrial base, emergency services, food and agriculture, government facilities and information technology.

Authorities recognized ransomware as the biggest cyberthreat facing the United States, with the education sector being one of the top targets. Other targeted sectors included businesses, charities, legal professionals, and public services in the local government and health sectors.

Cybersecurity authorities observed an increasingly professional field of ransomware actors in 2021.

Along with the increased use of ransomware-as-a-service (RaaS), threat actors employed independent services to negotiate payments, assist victims in making payments and arbitrate payment disputes with other cybercriminals. Criminal groups in Europe and Asia have also shared victim information with each other.

According to the report, authorities observed that "some ransomware threat actors offered their victims the services of a 24/7 help center to expedite ransom payment and restoration of encrypted systems or data."

In the United States, ransomware actors shifted their focus from "big game" organizations to midsize victims halfway through 2021 after they suffered disruptions from cyber authorities. The switch was to reduce scrutiny, officials said.

Most commonly, cybercriminals continued to initiate ransomware attacks via phishing emails, stolen remote desktop protocols (RDP) credentials and exploited software vulnerabilities.

The firm said that increased reliance on digital assets would introduce more vulnerabilities in 2022. Non-fungible tokens (NFTs) experienced significant hype in 2021, and "where value—or perceived value—goes, thieves and bad actors will follow."

These infection vectors likely remain popular because of the increased use of remote work and schooling starting in 2020 and continuing through 2021," the report stated. "This increase expanded the remote attack surface and left network defenders struggling to keep pace with routine software patching."

Cybercriminals increased their impact through a few methods—such as by targeting the cloud, managed service providers (MSPs) and software supply chain entities—and several groups have begun attacking industrial processes. More attacks against U.S. entities occurred on holidays and weekends.

Criminals also expanded methods to extort money from victims. They would threaten to release stolen information publicly, disrupt victims' internet access, and/or inform the victims' partners or shareholders of the incident.

Authorities had several recommendations to reduce the likelihood and impact of ransomware attacks. Organizations should keep all operating systems and software up to date; secure and monitor potentially risky services (e.g., RDP); implement user training programs and phishing exercises; require multifactor authentication (MFA); require strong and unique passwords; protect cloud storage by backing up to multiple locations; and encrypt cloud data.

For more cybersecurity guidance, contact Winters-Oliver Insurance Agency today.