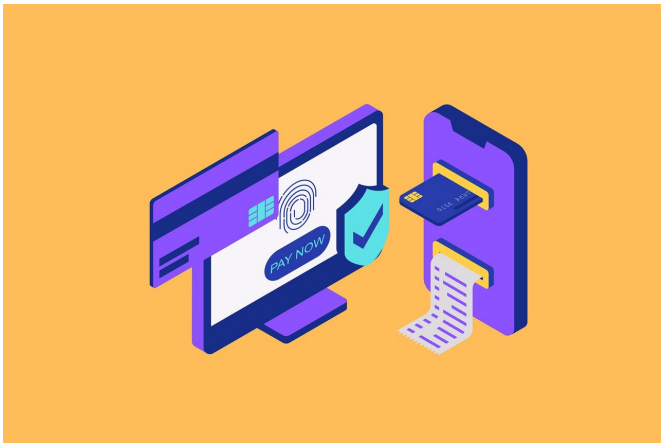
EXPLAINER: Ransomware and its role in supply chain attacks

4 July 2021



Credit: Pixabay/CC0 Public Domain

Another holiday weekend in the U.S., another ransomware attack that has paralyzed businesses around the world.

This time it's affecting an untold number of small and big companies that use IT software from a company called Kaseya.

High-profile ransomware attacks in May hit the world's largest meat-packing company and the biggest U.S. fuel pipeline, underscoring how gangs of extortionist hackers can disrupt the economy and put lives and livelihoods at risk.

WHAT IS RANSOMWARE? HOW DOES IT WORK?

Ransomware scrambles the target organization's data with encryption. The criminals leave instructions on infected computers for negotiating ransom payments. Once paid, they provide decryption keys for unlocking those files.

Ransomware crooks have also expanded into data-theft blackmail. Before triggering encryption, they sometimes quietly copy sensitive files and threaten to post them publicly unless they get their ransom payments.

WHAT'S A SUPPLY-CHAIN ATTACK?

The latest attack affecting Kaseya customers combines a ransomware operation with what's known as a supply-chain attack, which typically involves sneaking malicious code into a software update automatically pushed out to thousands of organizations.

Kaseya says the ransomware affected its product for remotely monitoring networks; but because many of its clients are providers of broader IT management services, a large number of organizations is likely to be affected.

"What makes this attack stand out is the trickle-down effect, from the managed service provider to the small business," said John Hammond of the security firm Huntress Labs. "Kaseya handles large enterprise all the way to small businesses globally, so ultimately, it has the potential to spread to any size or scale business."

Until now, the best-known recent supply-chain attack was attributed to elite Russian hackers and targeted software provider SolarWinds. But the motive was different; it was a massive intelligence operation targeting government agencies and others, not an attempt to extort money.

HOW DO RANSOMWARE GANGS OPERATE?

The criminal syndicates that dominate the ransomware business are mostly Russian-speaking and operate with near impunity out of Russia and allied countries. Though barely a blip three years ago, the syndicates have grown in sophistication and skill. They leverage dark web forums to organize and recruit while hiding their identities and movements with sophisticated tools and

cryptocurrencies like Bitcoin that make payments—and their laundering—harder to track.

Most experts have tied the Kaseya attack to a group known as REvil, the same ransomware provider that the FBI linked to an attack on JBS SA, a major global meat processor, amid the Memorial Day holiday weekend.

Active since April 2019, the group provides ransomware-as-a-service, meaning it develops the network-paralyzing software and leases it to so-called affiliates who infect targets and earn the lion's share of ransoms.

WHO IS AFFECTED?

The scale of the attack affecting Kaseya is not yet clear, but it's already been blamed for closing stores across a grocery chain in Sweden because their cash registers weren't working.

Last year alone in the U.S., ransomware gangs hit more than 100 federal, state and municipal agencies, upwards of 500 health care centers, 1,680 educational institutions and untold thousands of businesses, according to the cybersecurity firm Emsisoft. Dollar losses are in the tens of billions. Accurate numbers are elusive. Many victims shun reporting, fearing the reputational blight.