Cybersecurity

The Growth of Ransomware-as-a-Service & Its Effect on Supply Chain Security

Share

Ransomware is the fastest-growing type of cybercrime and a looming threat to supply chain security. In 2021, there was a record total of 292 reported ransomware attacks — a 17% increase from 2020 — and the average ransom demand grew 36% to $6.1 million last year.

As ransomware attacks threaten businesses and infrastructures worldwide, ransomware has become a growing industry in its own right. No longer limited to a few bad actors working independently, ransomware attacks are now largely propagated by attackers and ransomware-as-a-service providers working together to exploit key targets.

So what does this have to do with your supply chain?

One of the primary cyber threats facing organizations today isn't direct cyberattacks but vulnerabilities along their supply chain.

"Basically, high-end terrorists are looking at supply chain and supplier relationships to get into their targets," says Matt Keyes, cybersecurity expert and Commercial Director EMEA at Craft.co.

In other words, supply chain cybersecurity extends beyond your primary organization and its direct suppliers to n-tier suppliers as well, which may be more vulnerable and easier to breach. And with the rise of RaaS, organizations must take steps to strengthen their supply chain security posture amidst an increasingly complex network of vendors.

What is Ransomware-as-a-Service

Ransomware is a type of malware that encrypts data on the targeted device or network so that the owner can't access it. In order for the victim organization to regain access to its data and prevent data from being released or sold on the dark web, it must pay the attacker a ransom-typically to the tune of millions of dollars. Once the ransom is paid, the attacker gives the organization a decryption key. Basically, ransomware holds the victim's data hostage until payment is made.

As cloud infrastructure has grown in the past few years, cybercriminals have a larger "playground" of network environments they can exploit, leading to a rise in ransomware attacks and a growing industry of RaaS.

Basics of Ransomware-as-a-Service (RaaS)

Ransomware-as-Service (RaaS) is a subscription-based model that allows users (also known as affiliates) to pay for out-of-the-box ransomware services.

This includes providing ransomware code and encryption tools, negotiation management, and ransom collection. When the ransom is paid, the RaaS provider and the affiliate split the reward.

How it works:

- Hackers (affiliates) pay for the RaaS services and agree on a service fee for the ransom collected.
- The RaaS provider sets up a dashboard to manage and track the ransomware package.
- The affiliate (or sometimes the RaaS provider) targets the victim and implements the ransomware, communicates demands, and collects the ransom.
- The RaaS provider and affiliate split the reward based on their set terms.

Most ransomware is executed through phishing attacks, which is a method for stealing sensitive data like passwords. Phishing emails are the most common phishing tactic.

Hackers will send an email designed to appear legitimate; when the recipient clicks on the link, it secretly downloads the ransomware, quickly compromising the system without the user even knowing. These are particularly insidious attacks because the ransomware can spread throughout a system beyond the initial endpoint before anyone notices. Once the system is compromised, the hacker can encrypt access to the server and hold the data hostage until the business pays up.

Who Uses RaaS and Why

RaaS customers are hacker groups themselves that search for a RaaS provider to help them hack a company of their choice. Many (if not most) of these hacker groups are located in Russia.

Because RaaS handles the technical know-how, there is a low barrier to entry for would-be hackers. RaaS enables hackers of any experience to execute sophisticated attacks and reap handsome profits. This makes RaaS a popular money-making scheme for bad actors around the world.

Key RaaS industry players include:

- REvil
- DarkSide
- LockBit
- BABUK
- Avaddon
- BlackMatter

The State of Ransomware in 2022

With so many successful hacks, ransomware providers seem unstoppable in the current cyber climate, but in reality, they are worried about competition just like any other startup.

"***What's fascinating about ransomware providers is that they're just like any other entrepreneur," says Keyes.*** Like any other business, RaaS organizations share the same modern business concerns surrounding competition, product differentiation, sustainability, and marketing.

"You would think that being criminals, they wouldn't be concerned with customer service and sustainability. You would be wrong on both counts," Keyes explains. "In fact, DarkSide actually moved their leak site to a solar farm in Iran to make it more sustainable, both from a renewable energy perspective and also from a law enforcement perspective, because they're less likely to be shut down in Iran."

This allows DarkSide to differentiate its service from other RaaS providers on the market as a greener way to hack targets.

The Move Towards Better Compliance

RaaS organizations are also taking steps to ensure compliance and reduce the risk of regulatory restrictions that threaten their business operations.

For example, chief compliance officers are now being employed at RaaS companies to do the exact same thing they would do at a bank-weigh risks. These compliance officers evaluate the risk vs. reward of a crime to determine whether to move forward with an attack.

"What you see happening is they're getting regulated out of existence," says Keyes. "It's just the FBI rather than the SEC that's doing the regulating."

This is what happened to DarkSide after the Colonial Pipeline attack in May 2021. After shutting down the Colonial Pipeline-one of the largest and most important in the U.S.-and securing a ransom of nearly $5 million, DarkSide announced it would close its operations due to pressure from the U.S.

The intense scrutiny from governments and law enforcement following the Colonial Pipeline attack unsettled many RaaS groups, leading two major platforms, REvil and Avaddon to publish strict new rules governing their products and services.

"These RaaS providers are actually facing a crushing regulatory and compliance burden, and they've responded with corporate values pages that would look totally at home on Nike or Starbucks today," says Keyes, quoting one RaaS website:
"We do not attack hospitals, critical infrastructure, oil and gas defense, nonprofits, government sector. We are a team that unites people under one common interest. We provide the best service for our clients and partners compared to our competitors. We rely on honesty and transparency in our dealings, we never attack the same company twice and we always fulfill our obligations."

Increasing Threats to Supply Chain Security

High-profile attacks like the Colonial Pipeline result in unwanted attention globally for RaaS platforms, especially from law enforcement agencies like the FBI. In order to operate more "under the radar" and reduce the risk of regulation, RaaS groups are increasing compliance efforts through risk analysis and limiting the industries and types of organizations they are willing to target. This largely eliminates infrastructure targets like oil and gas and hospitals as well as nonprofits and government entities.

That means private sector companies-and their suppliers-that don't fall under those categories are going to be much bigger targets going forward.

Preventing Ransomware Attacks in Your Supply Chain

A supply chain attack targets victims through their suppliers. As hackers turn their sights on supply chains, organizations will need to mobilize new strategies to combat cyber attacks.

"Traditionally, you think of cybersecurity like a castle," explains Keyes, "You just protect your own estate. But now it's not just about your walls-you have to think of all your partners."

For instance, in July 2021, REvil attached the software company Kaseya, which develops software for managing networks, systems, and information technology infrastructure. The ransomware exploited an authentication bypass vulnerability in the software, enabling the hackers to compromise the system, impacting thousands of Kaseya's direct customers-and millions of customers of the service providers that used Kaseya.

In other words, attacks on n-tier suppliers that organizations don't even know they're affiliated with represent significant vulnerabilities in supply chain security. To protect not only the main business entity but also its suppliers down the supply chain, organizations need to take a more layered mitigation strategy on top of the traditional "castle" approach to security. This means working with your suppliers in a collective effort to reduce risk and strengthen security posture across the board.

Supplier intelligence = intelligent supply chain security

Better supply chain security begins with understanding who your suppliers are and where their strengths and weaknesses lie so you can work together to reduce risk and improve your front-line defense.

Your supplier intelligence platform should help you understand your entire risk landscape, get real-time alerts and actionable insights, and identify key threats, security vulnerabilities, and new opportunities.

Share

View All

Procurement & Supply Chain

Export Controls, Innovation Risks, and the Growing Need for Supplier Visibility

Read Now →