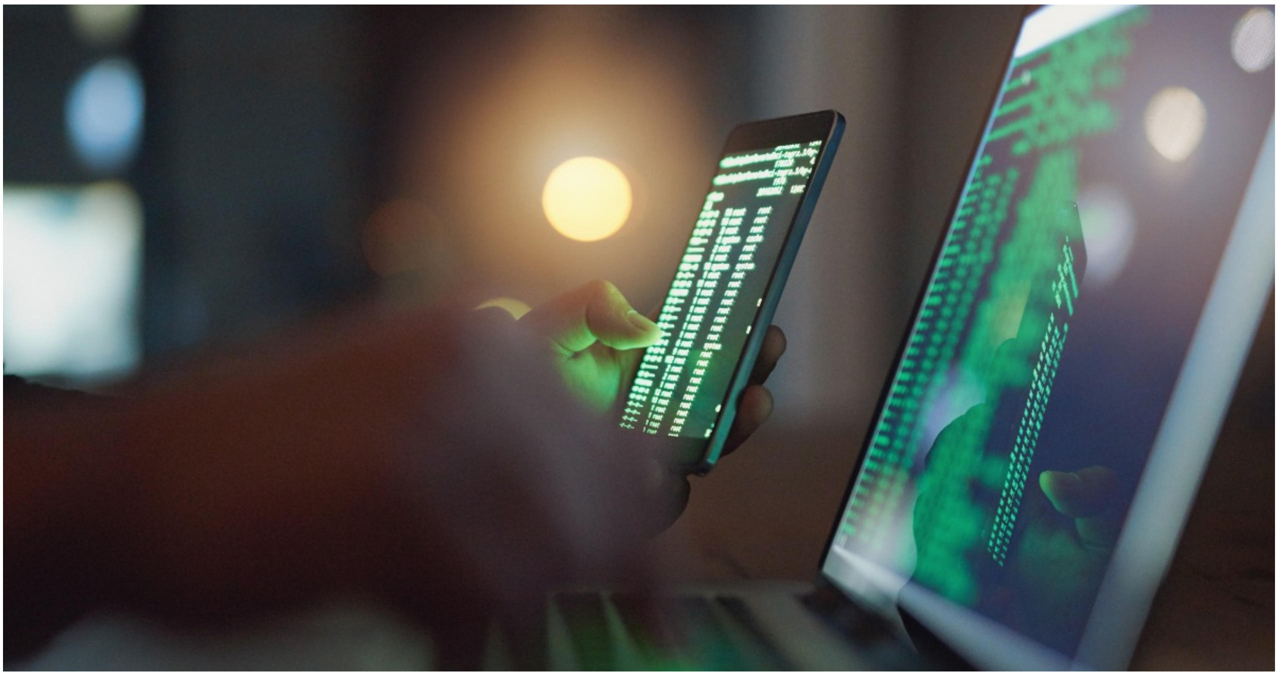
Threat Spotlight: Ransomware trends

blog.barracuda.com/2021/08/12/threat-spotlight-ransomware-trends

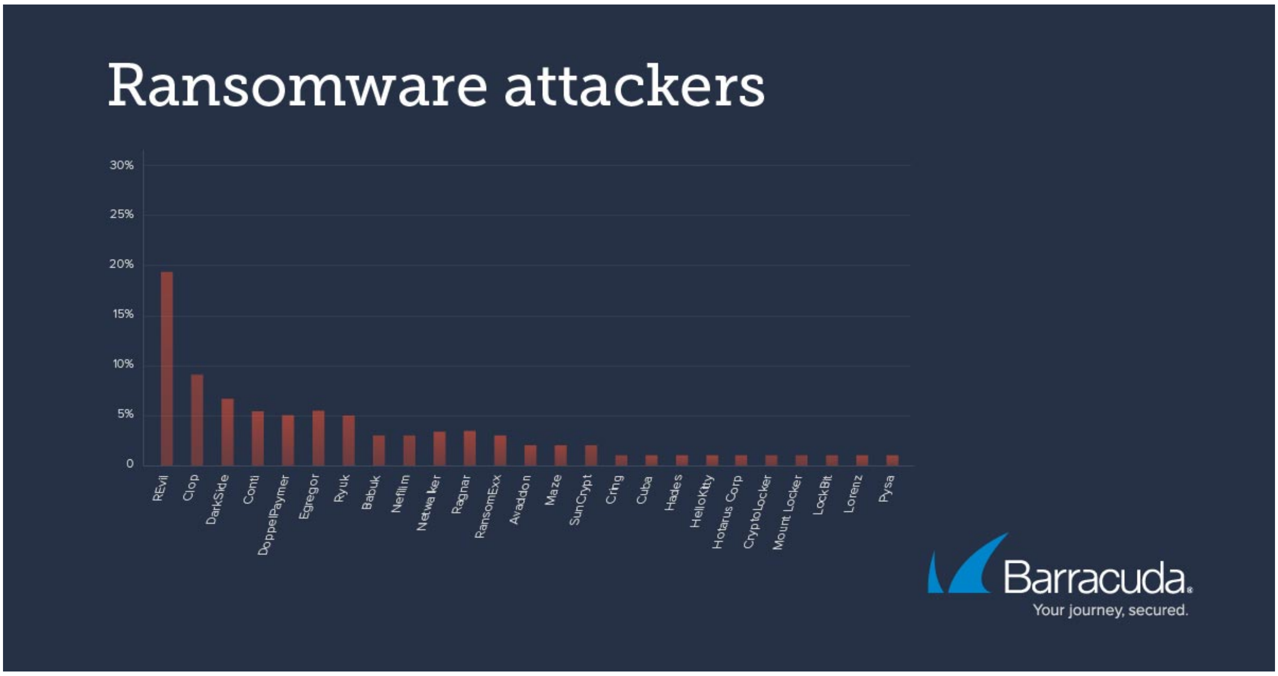
12 augustus 2021



Ransomware attacks have surged in 2021, with the number of attacks increasing dramatically and ransom amounts continuing to skyrocket. Cybercriminals are also expanding their targets, shifting their focus to our critical infrastructure and evolving into deep-rooted software supply chain attack campaigns, which can cause long-lasting devastation.

The grim outlook for the future of ransomware leaves no one spared from financial damage or brand-crushing headlines. Ransomware criminals are penetrating the foundation of our digital economy, from trusted software vendors to IT service providers.

Many of these attacks are being led by a handful of high-profile ransomware gangs. Our analysis of ransomware attacks that occurred between August 2020 and July 2021 showed that REvil accounted for 19% of attacks, and DarkSide is known to be the cause of 8%.



In this Threat Spotlight, we will examine the ransomware attack patterns we identified in our analysis of attacks over the past 12 months and share our insights on prevention and recovery.

Highlighted Threat

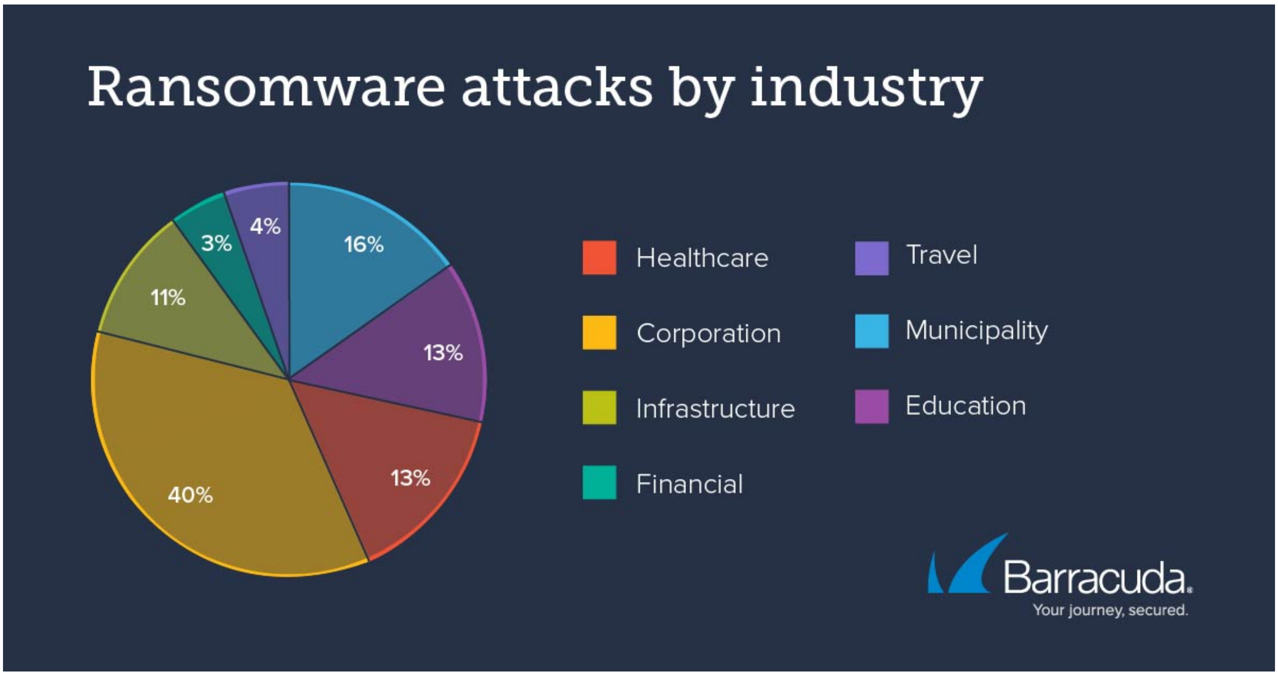
Ransomware — Cybercriminals use malicious software, often delivered as an email attachment or link, to infect the network and lock email, data, and other critical files until a ransom is paid. These evolving and sophisticated attacks are damaging and costly. They can cripple day-to-day operations, cause chaos, and result in financial losses from downtime, ransom payments, recovery costs, and other unbudgeted and unanticipated expenses.

Recently, criminals have refined their tactics to create a double extortion scheme. They base their ransom demands on research they perform ahead of the attack. They steal sensitive data from their victims and demand payment in exchange for a promise to not publish or sell the data to other criminals. Since criminals cannot be trusted, victims who pay are often contacted several months later and asked for another payment to keep the stolen data secret. Some ransomware criminals will accept payment but sell the data anyway.

The Details

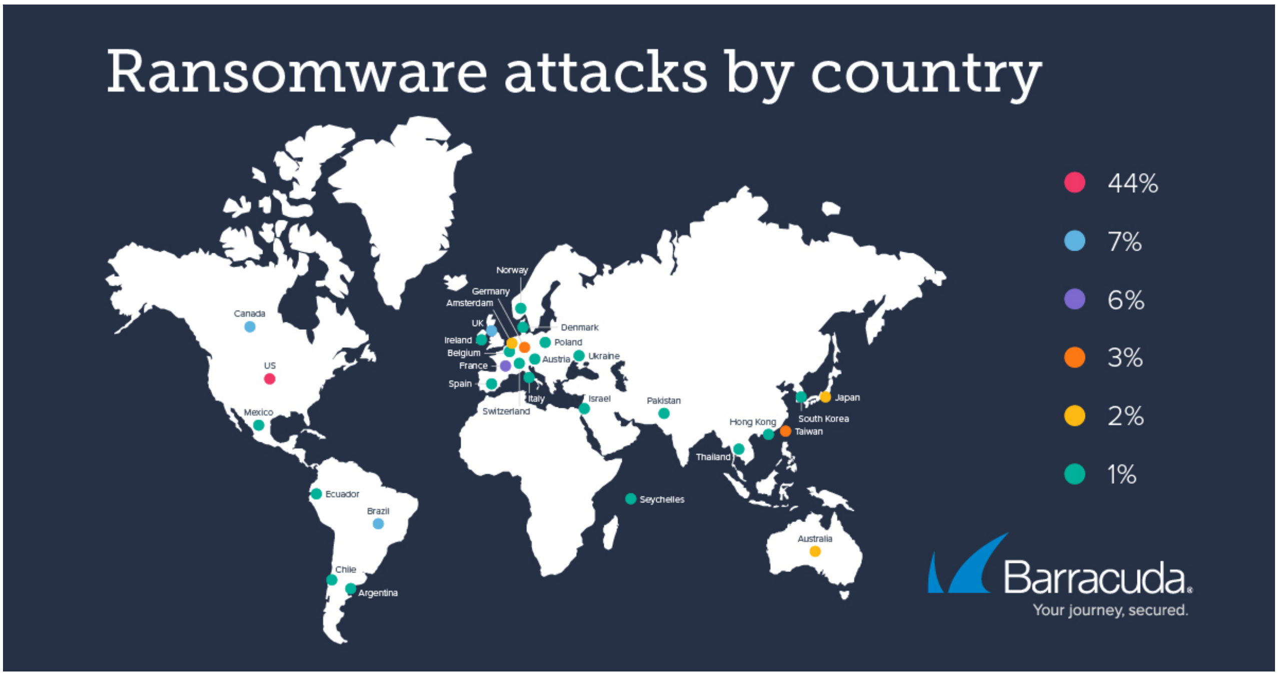
In the past 12 months, Barracuda researchers have identified and analyzed 121 ransomware incidents, a 64% increase in attacks, year over year. Cybercriminals are still heavily targeting municipalities, health care, and education, but attacks on other businesses are surging.

Attacks on corporations, such as infrastructure, travel, financial services, and other businesses, made up 57% of all ransomware attacks between August 2020 and July 2021, up from just 18% in our 2020 study. Infrastructure-related businesses account for 10% of all the attacks we studied. In fact, ransomware attacks are quickly evolving to software supply chain attacks, which reach more businesses in a single attempt.



We previously highlighted how municipalities are not always well-prepared for these types of attacks, often dealing with tight budgets, small IT staffs, and outdated tools. But the problem is much worse than we thought, especially as trusted software vendors have been weaponized against their customers, leading to attacks from unexpected sources at an alarming rate.

While cybercriminals are still heavily focusing ransomware attacks on organizations based in the United States, our research found that ransomware attacks are becoming pervasive across the globe. Just under half of the attacks in the past 12 months hit U.S organizations (44%). In comparison, 30% of the incidents happened in EMEA, 11% were in Asia Pacific countries, 10% were in South America, and 8% were in Canada and Mexico.



Exploiting application vulnerabilities in ransomware attacks

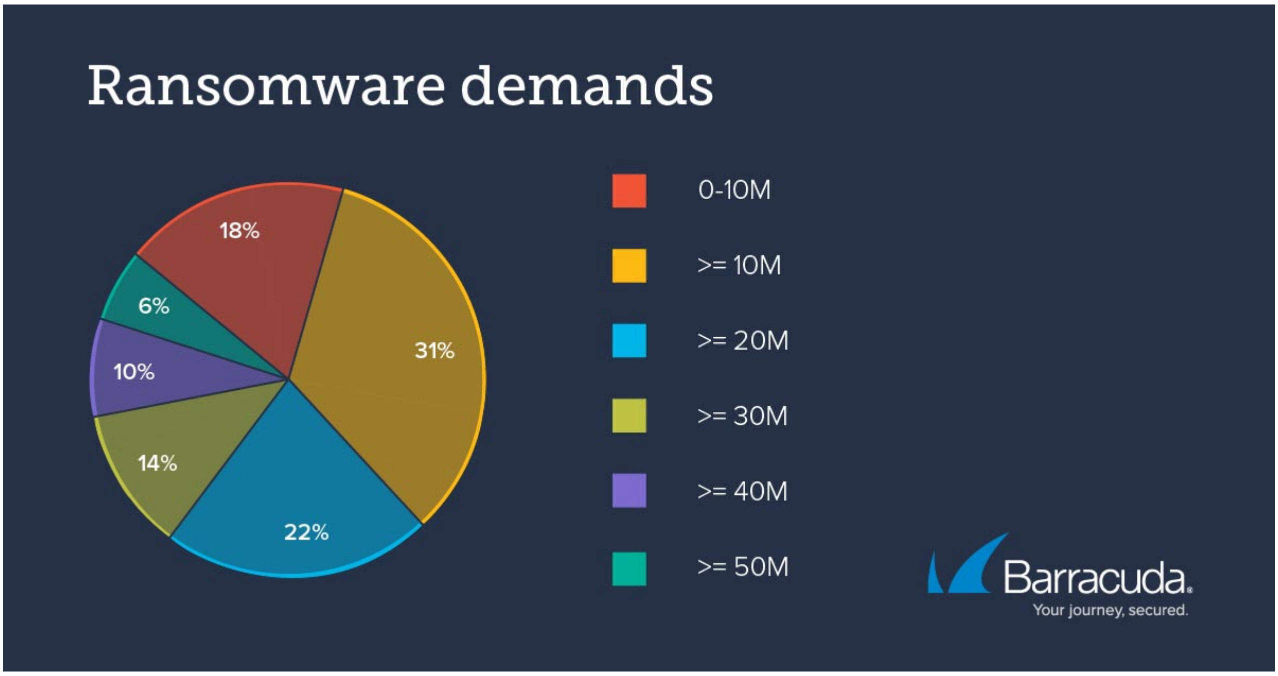
Ransomware attack patterns are evolving as well. Instead of simply relying on malicious links and attachments to deliver ransomware, cybercriminals are leveling up their tactics. First, attackers will find ways to steal credentials through phishing attacks, and then they will use the stolen credentials to challenge the web applications used by the victim. Once the application has been compromised, the attacker can introduce ransomware and other malware into the system. This can go on to infect your network as well as users of your application.

It's important to note that web applications have many forms, including those enabling users to work from home. A web portal for a segment of your IT infrastructure is just as dangerous as a full-blown SaaS application. On multiple occasions in the past year, attackers exploited an application vulnerability to gain control of the application infrastructure and eventually target the most valuable data to encrypt.

OWASP top 10 threats for application security are all potential mechanisms to gain access to an organization's infrastructure. Relying solely on VPN for remote workers also poses significant risk given that many credentials have been exposed on the dark web through leaked passwords. For example, the ransomware attack that led to the extended shutdown of Colonial Pipeline in May started when hackers gained access to the network through a VPN account by using a compromised password found on the dark web.

Ransom payment trends

Just as we have seen in the past years, the ransom amount is increasing dramatically and now the average ransom ask per incident is over $10 million. Only 18% of the incidents had less than $10 million ransom ask, and 30% of the incidents had greater than $30 million ransom asks.



Since the wider adoption of cryptocurrency, we have seen a correlation of increased ransomware attacks and higher ransom amounts. With increased crackdown on bitcoin and successful tracing of transactions, criminals are starting to provide alternative payments methods, such as the REvil ransomware gang asking for Monero instead of bitcoin.

However, in our research we also saw multiple instances of victims reducing ransom payments by deploying negotiation tactics. JBS negotiated a $22.5 million ransom payment down to $11 million, and Brenntag, a chemical distributor in Germany, negotiated a $7.5 million ransom demand down to $4.4 million. The initial ransom ask may not be the final ask, so if they're planning to pay, it is important for ransomware victims to exercise negotiation options. The outcome can be savings in the millions.

We see more organizations refusing to pay the ransom, and that is likely driving up the initial ransom ask. This trend is also followed by more collaboration with the authorities and ransom negotiators. The FBI have recently uncovered the bitcoin wallets of DarkSide and were able to recover some of the ransom payments, and authorities have disrupted payments to the affiliates of the ransomware group.

These are encouraging signs in the fight against these cyberattacks. Beyond legal action, we have also seen the White House speaking directly to world leaders and demanding tough actions against harboring cyber criminals. Given the high-profile, high-impact nature of recent attacks, particularly attacks against critical infrastructure, I believe the U.S. government is no longer just sending warnings. It is ready to take serious actions even against nation states if there is clear evidence of accomplice or negligence in policing cybercriminals.

How to protect against ransomware

The first step in taking on ransomware is assuming that you will be victimized—it's just a matter of when. The next thing you need to do is to set a goal of not paying the ransom. With the goal set, you then need to implement at least the following three procedures to achieve that goal.

- **Do everything you can to prevent credential loss.** Implement anti-phishing capabilities in email and other collaboration tools, and consistently train your users for email security awareness.
- **Secure your applications and access.** Besides using MFA, you should also implement web application security for all your SaaS applications and infrastructure access points. Application vulnerabilities are often hidden in the application code or underlying application infrastructure; therefore, you must protect your applications from the OWASP Top 10 threats. If you have API interactions in your application, you should also make sure you are covered for OWASP API Security Top 10. Along with application protection, try to reduce the amount of access you provide to your users wherever you can. If you can, narrow down to the least amount of access your users need to be productive. It's best to implement Zero Trust Access based on endpoint security postures.
- **Back up your data.** Stay current with a secure data protection solution that can identify your critical data assets and implement disaster and recovery capabilities. That way you can be confident about saying no to ransomware criminals.

As cybercriminals are working towards bigger paydays in the future, the security industry needs to continue to create solutions that are easily consumable for companies of all sizes. Attackers often start with small organizations that are connected to the larger targets and then work their way up. I really hope we can all create products that work well together, and if products are too complicated for a certain segment of the market, we need to turn sophisticated technology and products into services that can be consumed without expensive and scarce security talents.

Webinar: The Three Stages of Ransomware: Threat Spotlight Findings and Analysis