Report

on

Recent Ransomware Trends 2021

Dilpreet Singh Bajwa

According to the U.S. Government's Cybersecurity and Infrastructure Assurance Agency(CISA): "Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid."

Today's attackers are not only holding data ransom, but stealing it to sell on the Internet. This shows a trend where attackers aren't just executing ransomware, they are persisting on the network, successfully exfiltrating data, and then finally deploying ransomware.

Some of the latest survey reports related to Ransomware attacks:

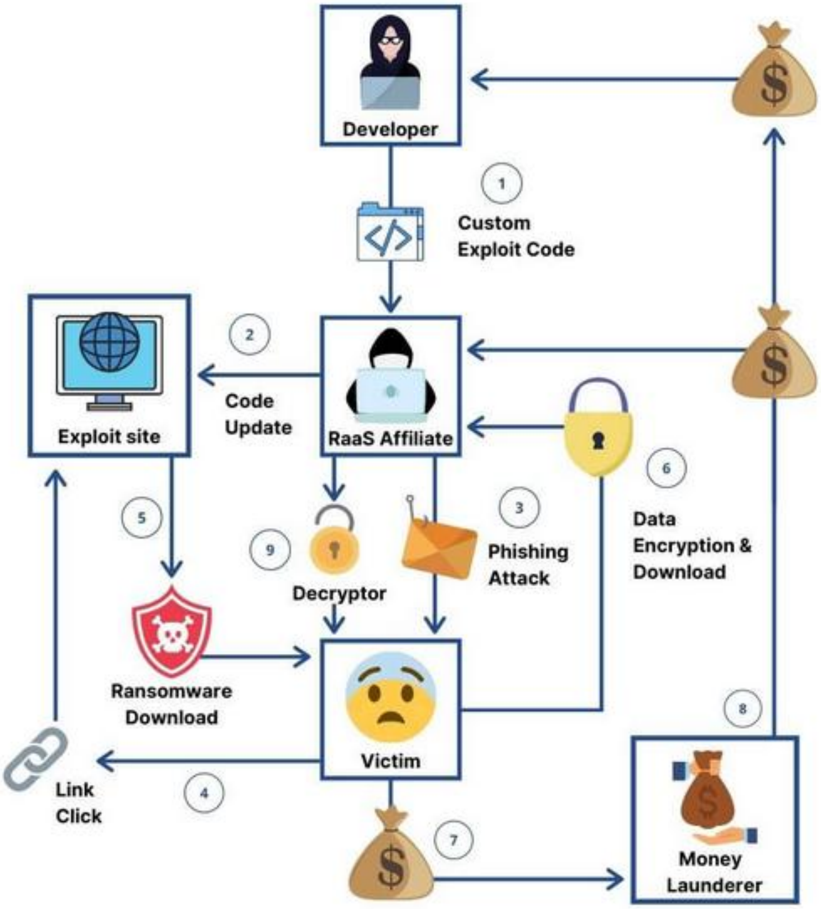
- Ransomware remains the most prominent malware threat for 2021. (Datto).
- The volume of ransomware around the world hit just over 304 million attempts in the first six months of this year-2021 and that was equal to the number of attempts for all of 2020. (SonicWall)
- India has seen the most number of attacks attempts per organization, with an average of 213 weekly attacks since the beginning of the year. This is followed by Argentina with 104 per organization, Chile with 103, France 61 and Taiwan 50. (Checkpoint)
- Malicious emails are up 600% due to COVID-19. (ABC News, 2021)
- 37% of respondents' organizations were affected by ransomware attacks in the last year. (Sophos, 2021)
- In 2021, the largest ransomware payout was made by an insurance company at $40 million, setting a world record. (Business Insider, 2021)
- The average ransom fee requested has increased from $5,000 in 2018 to around $200,000 in 2020. (National Security Institute, 2021)
- The average downtime a company experiences after a ransomware attack is 21 days. (Coveware, 2021)
- The most common tactics hackers use to carry out ransomware attacks are email phishing campaigns, RDP vulnerabilities, and software vulnerabilities. (Cybersecurity & Infrastructure Security Agency, 2021)
- From a survey conducted with 1,263 companies, 80% of victims who submitted a ransom payment experienced another attack soon after, and 46% got access to their data but most of it was corrupted. (Cybereason, 2021)
- Additionally, 60% of survey respondents experienced revenue loss and 53% stated their brands were damaged as a result. (Cybereason, 2021)

Recent Trends in Ransomware:

1. Ransomware as a Service (RaaS) is increasing.
2. The Exploitation of IT outsourcing services or Managed Service Providers (MSPs).
3. More focused towards Vulnerable Industries.
4. Healthcare industry victimization by Ransomware.
5. Triple Extortion Ransomware Technique.

1. Ransomware as a Service (RaaS) is increasing.

Ransomware-as-a-service, or RaaS, is a subscription that allows affiliates to use ransomware tools that are already developed to carry out ransomware attacks. One reason for the growth in Ransomware attacks is due to appearance of ransomware as a service and ransomware kits on the dark web, which can be purchased for as low as $175 and require little to no technical knowledge to deploy.



General Ransomware Infection workflow through RaaS Model

Some of the groups providing Ransomware as a Service:

- **DopplePaymer** – provided ransomware for attacks on Pemex in Mexico, Bretagne Télécom in France, and both Newcastle and Düsseldorf University.
- **Egregor** – provided ransomware for attacks on Crytek in Germany, Ubisoft in France, and Barnes & Noble in the U.S.
- **Netwalker/Mailto** – provided ransomware for attacks on Toll Group in Australia as well as Equinix, UCSF, and Michigan State University in the U.S.
- **REvil/Sodinokibi** – provided ransomware for attacks on Britain's Travelex, as well as airports and local governments in the U.S.
- **Ryuk** – the biggest RaaS gang was responsible for almost 33% of all attacks in 2019, including Sopra Steria in Europe and Seyfarth Shaw Law Firm, Universal Health Systems, and several other individual hospitals in the U.S

2. The Exploitation of IT outsourcing services or Managed Service Providers (MSPs):

Ransomware gangs have been shifting their focus to managed service providers (MSPs), a platform that serves many clients at once. This means that if a hacker gains access to one MSP, it could also reach the clients it's serving as well.

The business of MSPs has boomed during the coronavirus pandemic alongside the rapid increase in remote work. Managed service providers include companies such as IBM and Accenture offering cloud versions of popular software and specialist firms devoted to specific industries. They typically serve small and medium-sized firms that lack in-house technology capabilities and often boost security. But MSPs also make an efficient vehicle for ransomware because they have wide access inside many of their customers' networks.

One recent example is Kaseya, Kaseya's software serves many MSPs, so the attacks multiplied before Kaseya could warn everyone, rapidly encrypting data and demanding ransoms of as much as $5 million per victim. Kaseya ransomware attack paralyzed as many as 1,500 organizations. An affiliate of a top Russian-speaking ransomware gang known as REvil was behind the attack.

With REvil extortionists asking for a record $70 million to reverse all the Kaseya damage, but their aspirations are clearly bigger now, and their approach is more measured. It's unclear how much ransom was ultimately paid or how many businesses were affected.

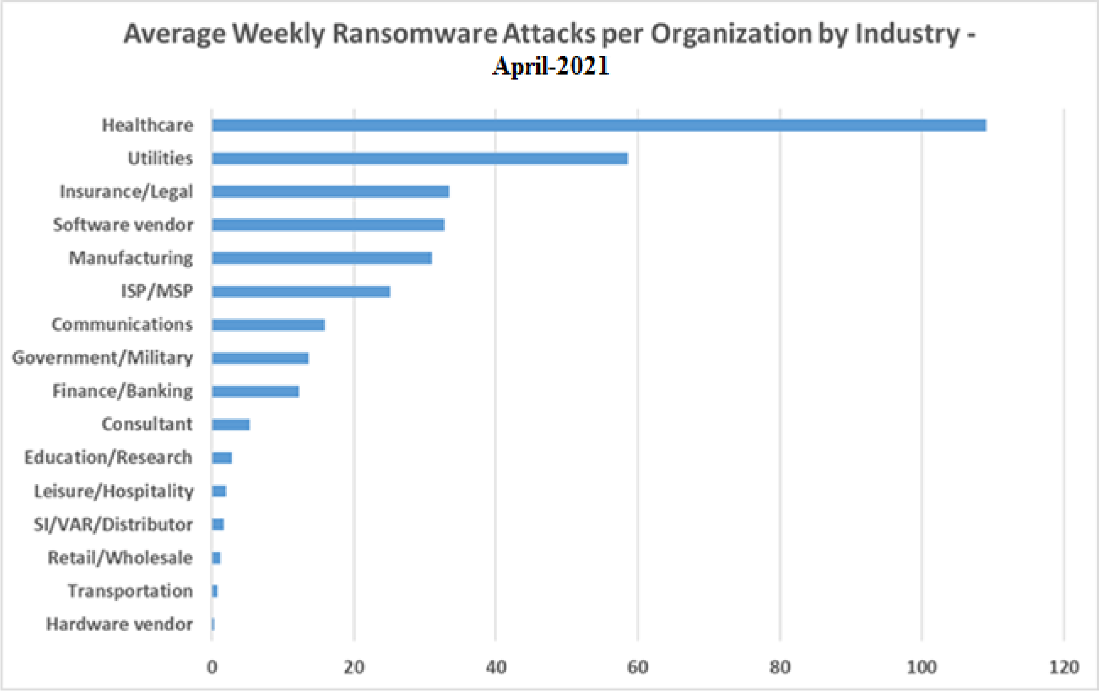
Less than two weeks after the July 2 Kaseya attack, CISA issued guidelines for best practices on both sides of the equation. CISA also offers free risk assessments, penetration testing and analyses of network architecture.

3. Healthcare industry victimization by Ransomware:

Cybercriminals often focus their attacks on the most vulnerable targets, and unfortunately health systems tend to be high on that list. Digital transformation in health systems accelerated even further over the pandemic. However, rapid change sometimes creates conflicting priorities leading to divergent and fragmented technologies within a single health system. This makes it easier for attackers to focus their attention and attacks.

Additionally, a lot of healthcare platforms have focused on data portability and interoperability which has meant that security was not necessarily a top priority. All of these factors make healthcare an appealing target, and when you consider that health systems are likely to succumb to ransom-based attacks to protect data, it just encourages the attackers even more.

Following figure shows average number of ransomware attacks per week by industry in April-2021 and the healthcare industry was on top i.e. it is one of the most attractive target for attackers.



Average number of ransomware attacks per organization per week by industry – April 2021

Key findings(from sophos Report "The State of Ransomware in Healthcare 2021"):

- 34% of healthcare organizations were hit by ransomware in the last year.
- 65% that were hit by ransomware in the last year said the cybercriminals succeeded in encrypting their data in the most significant attack.
- 44% of those whose data was encrypted used backups to restore data.

- 34% of those whose data was encrypted paid the ransom to get their data back in the most significant ransomware attack.
- However, on average, only 69% of the encrypted data was restored after the ransom was paid.
- 89% of healthcare organizations have a malware incident recovery plan.
- The average bill for rectifying a ransomware attack, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc. was US$1.27 million. While this is a huge sum, it's also the lowest among all sectors surveyed.

For a healthcare organization, the ramifications of a cyberattack expand beyond financial harm. Cyber-attacks have the potential to inhibit the organization's ability to provide care. These attacks also have regulatory compliance, and legal impact as they may constitute a breach under HIPAA or result in medical malpractice. This may result in additional audits, fines, and other burdens on the organization.

4. More focused towards Vulnerable Industries:

These cybercriminals are focusing their efforts on businesses that store a large amount of personal and confidential data.

They're also looking for industries where they can cause the most disruption and turmoil (since downtime is significantly more expensive than the ransom), such as the ones listed below:

- In June, a cyberattack on JBS S.A., a multinational meat producer, shut down a quarter of American beef production for two days as the company shut down its computer systems to contain the incident.
- Colonial Pipeline was forced to shut off gasoline delivery to much of the Eastern Seaboard in May due to a cyberattack, resulting in shortages across the South. In the same month, a hacker took down the databases of a San Diego medical system for two weeks.
- Hackers claimed to have stolen 500 gigabytes of data, including contracts and non-disclosure agreements, from the Houston Rockets in April.
- In March, CNA Financial Corp, one of the top insurance companies, was locked out of its network for about two weeks due to a security compromise.
- In February, hackers gained access to an Oldsmar, Florida, water-treatment plant, temporarily boosting lye levels in drinking water to unsafe levels.

5. Triple Extortion Ransomware Technique:

Cybercriminals who specialize in ransomware have already been using double extortion tactics in which they not only decrypt stolen data but also threaten to leak it publicly unless the ransom is paid.

Now, some attackers have progressed to a triple extortion tactic with the intent of squeezing out even more money from their malicious activities. The surge in attacks has been fuelled by the rise of the "triple extortion" ransomware technique whereby attackers, in addition to stealing sensitive data from organisations and threatening to release it publicly unless a payment is made, are also targeting the organisations customers, vendors or business partners in the same way.

To make matters worse, we now see an added complication to ransomware – a triple extortion threat – exemplified by ransomware group Avaddon. Not only does your data get encrypted and exfiltrated, but if you do not respond to the original threat for payment or the threat of a data leak, attackers may then launch a DDoS attack against your services as a way to bring you back to the negotiation table.

DDoS has traditionally been associated with only one form of extortion, Ransom Denial of Service (RDoS). This is a type of attack where threat actors launch a DoS attack against a victim's network and then demand a payment in Bitcoin to stop. But piggybacking this with ransomware, as with Avaddon, is relatively novel. It confirms the growing underground economy in that threat actors can now inexpensively rent attack services or keep affiliates on the payroll for additional pressure when required.

Modern Ransomware Capabilities:

Traditional ransomware was all about coming in with a big splash and causing immediate damage. The goal was to get on the machine and ransom data, and that was it but ransomware is continuously evolving; currently many types of malware silently persist on the network, move laterally, communicate with their C2, or obfuscate their behaviors to prevent detection.

Combined with obfuscation techniques and vulnerabilities that allow remote code execution, ransomware is able to evade legacy prevention solutions to achieve its goal. Modern ransomware is taking a slightly different approach. Instead of limiting themselves to leveraging ransomware to exclusively collect a ransom, attackers are now deploying malware that steals credentials and persists in the network for an extended period of time before deploying ransomware. This method has the potential for much greater bang for the buck, as attackers can sell off stolen credentials, move to infect other machines on the network, and ultimately deploy the actual ransomware.

Further, in addition to that, ransomware used hybrid techniques like triple extortion and RDOS in combination to exploit the victim.

Ryuk Ransomware(Feat. Emotet & Trickbot): The Cybereason Nocturnus team researched a campaign that used a multi-stage attack to stealthily deliver the Ryuk ransomware. This spanned from Emotet’s delivery of TrickBot, to TrickBot’s information stealing capabilities, lateral movement, and use as a downloader for Ryuk, and finally to Ryuk’s ransomware capabilities. With Ryuk, the attacker is able to encrypt the machine and ransom data back to the victim, with the potential to cost victims significant sums of money due to downtime, recovery costs, and damage to reputation.

Note : Many companies impacted by Ryuk weren’t just hit by ransomware, but also additional malware that collects credentials and persists on the network. This is further confirmation that ransomware attacks are evolving to damage organizations as much as possible.

GandCrab: GandCrab was one of the most prevalent ransomwares in the threat landscape and was constantly evolving and perfecting its delivery methods to evade detection.

Bitdefender estimates that GandCrab is responsible for 40% of all ransomware infections globally, which demonstrates exactly how effective it has become. The authors are known to iteratively and quickly update GandCrab with stealthy new delivery mechanisms and other adaptations.

Note : Before being retired, GandCrab had many variants and continues to evolve. The only way to reliably prevent this ransomware is through security tools that can identify and correlate behaviors, and not just signatures.

Sodinokibi: Sodinokibi, a highly evasive ransomware that takes many measures to prevent its detection by antivirus and other means. The authors of Sodinokibi have previously been connected to the same authors of the prolific GandCrab ransomware, which was recently retired. When Sodinokibi first emerged, it exploited vulnerabilities in servers and other critical assets. As time went by, it also leveraged other infection vectors such as phishing and exploit kits. There were several instances where the Sodinokibi ransomware purposefully searched for an AV made by South Korean security vendor Ahnlab in an attempt to inject its malicious payload into the trusted AV vendor.

Note : Sodinokibi is another ransomware that uses a suite of tricks, including obfuscated PowerShell commands, to evade existing defenses. This highlights the need to have comprehensive prevention and detection on the endpoint.

Prominent Ransomware Attacks in 2021:

Kaseya: A ransomware attack in July-21 that paralyzed as many as 1,500 organizations by compromising tech-management software from a company called Kaseya. An affiliate of a top Russian-speaking ransomware gang known as REvil used two gaping flaws in software from Florida-based Kaseya to break into about 50 managed services providers (MSPs) that used its products, investigators said. REvil extortionists asking for a record $70 million to reverse all the Kaseya damage.

Colonial Pipeline: The breach of Colonial Pipeline in late April had the most news coverage. The Colonial Pipeline attack made such an impact because the pipeline is an important part of the US national critical infrastructure system. Taking the system down disrupted gas supplies all along the East Coast of the United States, causing chaos and panic.

The DarkSide gang was behind the attack and targeted the firm’s billing system and internal business network, leading to widespread shortages in multiple states. To avoid further disruption, Colonial Pipeline eventually gave in to the demands and paid the group $4.4 million dollars in bitcoin.

Brenntag: In early May 2021, the same notorious hacker group (Dark Side) that targeted Colonial Pipeline, also targeted Brenntag, a chemical distribution company. After stealing 150 GB worth of data, DarkSide demanded the equivalent of $7.5 million dollars in bitcoin.

Brenntag soon caved to the demands and ended up paying $4.4 million. Although it was a little more than half of the original demand, it still stands as one of the highest ransomware payments in history.

Acer: Also in May this year, the computer manufacturer Acer_was attacked by the REvil hacker group, the same group responsible for an attack on London foreign exchange firm Travelex. The $50 million ransom stood out as the largest known to date. REvil hackers exploited a vulnerability in a Microsoft Exchange server to get access to Acer's files and leaked images of sensitive financial documents and spreadsheets.

JBS Foods*:* Another high-profile ransomware attack took place this May on JBS Foods, one of the biggest meat processing companies in the world. The same Russia-based hacking group that attacked Acer, REvil, is thought to be behind the attack.

On June 10th, it was confirmed that JSB paid the $11 million ransom demand after consulting with cybersecurity experts. This massive payment in bitcoin is one of the largest ransomware payments of all time.

Quanta: As with the Acer attack, the REvil gang also demanded a $50 million ransom from computer manufacturer Quanta in April. The company is one of Apple's major business partners. After the firm refused negotiations with the hacker group, REvil targeted Apple instead. After leaking Apple product blueprints obtained from Quanta, they threatened to release more sensitive documents and data. As of now, however, REvil seems to have called off the attack, and Apple has not mentioned the cyber attack.

National Basketball Association (NBA): In mid-April of this year, the hacker group Babuk claimed to have stolen 500 GB of confidential data concerning the Houston Rockets. Babuk warns that these confidential documents, including financial info and contracts, will be made public if their demands are not met. As of now, no ransom payments have been made.

AXA: In May, the European insurance company AXA was attacked by the Avaddon gang. The attack happened soon after the company announced important changes to their insurance policy. This attack on a cyber-insurance firm made headlines and the hacker group gained access to a massive 3 TB of data.

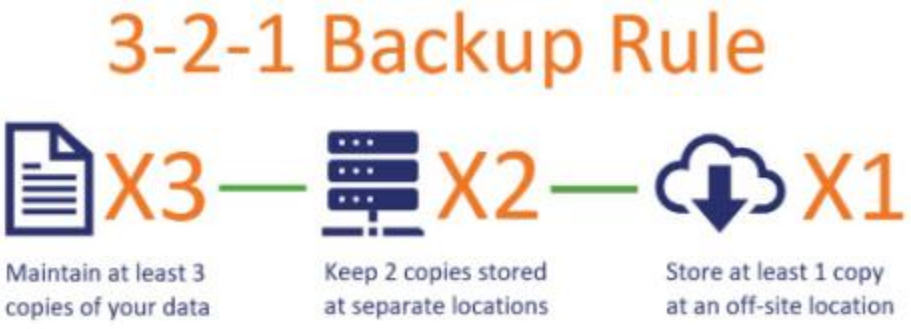
CNA: Earlier this year in March, another large insurance firm fell victim to a ransomware attack. CNA's network was attacked on March 21 and the hacker group encrypted 15,000 devices, including many computers of employees working remotely. The attack is supposedly linked to the hacker group Evil Corp and uses a new type of malware called Phoenix CryptoLocker.

CD Projekt: CDProjekt Red is a popular videogame development firm based in Poland. In February of this year, the firm was hacked by the HelloKitty gang. The hacker group accessed source code to game projects in development and encrypted devices. However, CDProjekt has no plans to pay the ransom money, and has backups in place to restore the lost data.

Kia Motors: This February, Kia Motors, a subsidiary of Hyundai, was reportedly hacked with ransomware. Although Kia reported a widespread IT and systems outage, they did not confirm the hack. Still, many experts believe the claims by the DoppelPaymer gang demanding a $20 million ransom. The gang has released some stolen data, but updates on the hack have not surfaced in the news for the past few months.

Mitigation Techniques:

- Implement multi-factor authentication and complex password policy.
- Enable strong spam filters to prevent phishing emails from reaching end users.
- Implement a user training program and simulated attacks for spear phishing to discourage users from visiting malicious websites or opening malicious attachments, and re-enforce the appropriate user responses to spear phishing emails.
- Filter network traffic to prohibit ingress and egress communications with known malicious IP addresses. Prevent users from accessing malicious websites by implementing URL block lists and/or allow lists.
- Update software, including operating systems, applications, and firmware on IT network assets, in a timely manner.
- Implement 3-2-1 Backup Rule as follows:


3-2-1 Backup Rule
X3
X2
X1
Maintain at least 3 copies of your data
Keep 2 copies stored at separate locations
Store at least 1 copy at an off-site location

- Limit access to resources over networks, especially by restricting RDP.
- Set anti-virus/anti-malware programs to conduct regular scans of IT network assets using up-to-date signatures.
- Combine human experts and anti-ransomware technology. Key to stopping ransomware is defense in depth that combines dedicated anti-ransomware technology and human-led threat hunting.
- Implement unauthorized execution prevention by:
  1. Disabling macro scripts from Microsoft Office files transmitted via email. Consider using Office viewer software to open Microsoft Office files transmitted via email instead of full Microsoft Office suite applications.
  2. Implementing application allow-listing, which only allows systems to execute programs known and permitted by security policy.
  3. Monitor and/or block inbound connections from Tor exit nodes and other anonymization services.

    4. Deploy signatures to detect and/or block inbound connection from Cobalt Strike servers and other post exploitation tools.

- If your organization is impacted by a ransomware incident:
    1. Isolate the infected system.
    2. Turn off other computers and devices. Power-off and segregate any other computers or devices that shared a network with the infected computer(s) that have not been fully encrypted by ransomware.
    3. Secure your backups. Ensure that your backup data is offline, secure, and free of malware.

Conclusion:

In 2021, We expect a massive surge in the number of ransomware threats, the reasons for which could be both the acceleration of digital transformation in all industries and the widespread transition to remote work. During the course of the year, the number of ransomware attacks will grow, their complexity will increase, and it will become increasingly difficult to counter them.

References:

- https://securityboulevard.com/2021/04/2021-malware-trends-what-we-should-expect/
- https://www.varonis.com/blog/ransomware-statistics-2021/
- https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php
- https://www.kaspersky.com/resource-center/threats/ransomware
- https://www.cybereason.com/blog/five-things-you-need-to-know-about-ransomware-attacks
- https://www.cybereason.com/hubfs/2020_05_Ransomware_Decoded.pdf
- https://monstercloud.com/surveys/monstercloud-reviews-top-ransomware-threats-for-2021/
- https://www.forbes.com/sites/servicenow/2021/08/06/the-art-of-being-human-in-the-new-world-of-work/?sh=4626b5071a5b
- https://www.upguard.com/blog/what-is-ransomware-as-a-service
- https://unfoldlabs.medium.com/2021-the-rise-of-ransomware-as-a-service-raas-49205254077b
- https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php
- https://www.varonis.com/blog/ransomware-statistics-2021/
- https://www.itworldcanada.com/article/cyber-security-today-august-2-2021-a-record-year-for-ransomware-attacks-predicted-and-warnings-from-microsoft-and-cisco-systems/456546
- https://www.computerweekly.com/news/252504676/Ransomware-attacks-increase-dramatically-during-2021
- https://portswigger.net/daily-swig/four-fold-increase-in-software-supply-chain-attacks-predicted-in-2021-report
- https://www.securitymagazine.com/articles/95238-welcome-to-the-new-world-of-triple-extortion-ransomware
- https://www.techrepublic.com/article/ransomware-attackers-are-now-using-triple-extortion-tactics/
- https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/
- https://threatpost.com/ransomwares-swindle-triple-extortion/166149/
- https://www.reuters.com/technology/kaseya-ransomware-attack-sets-off-race-hack-service-providers-researchers-2021-08-03/

- https://searchsecurity.techtarget.com/feature/The-biggest-ransomware-attacks-this-year
- https://www.blackfog.com/the-state-of-ransomware-in-2021/
- https://www.malwarebytes.com/resources/files/2021/04/2021-state-of-malware-infographic_final.pdf
- https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf
- https://purplesec.us/resources/cyber-security-statistics/ransomware/
- https://www.eweek.com/security/new-ransomware-trends-causing-fear-in-2021/
- https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf
- https://www.securitymagazine.com/articles/95381-clinical-treatment-of-ransomware-in-healthcare
- https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf