Global Ransomware Report

October 2022

EXECUTIVE SUMMARY

Increasingly digitizing business and financial transactions and sharing more data in computer systems has provided more targets for attackers. It seems that the amount of digital data that the operations of threat actors can target is not only increasing but also expanding in variety.

Threat actors who attack using ransomware have evolved over the past five years, from encryption techniques to software. They have undergone many operational changes, such as their programming languages. However, the focus of the change we have experienced lately is how the post-attack causes more damage to the target institution rather than how the actors carry out their attacks.

As the attackers are no longer content with just encrypting files in the systems they target, there are more and more instances where attackers threaten to share their data with the public to harm the reputation of the target organization. In addition, the number of cases where threat actors carry out DDoS attacks on target systems is increasing to compel the parties who resist ransom negotiations or try to leave them.

The reason behind such a strategy change is to increase the pressure on the attacked targets to pay the requested ransom in the wake of increased ransomware attacks.

This report, prepared by the SOCRadar research team, aims to provide comprehensive information on ransomware, one of the most common weapons used by cybercriminals.

Adopting a 'publish and smear' strategy, threat actors try to gain access to the system to discover sensitive data before encrypting the system.

- The institutions' data about business partners and customers also attracts the attention of the attackers.
- The impacts of a ransomware attack extend far beyond the organization whose systems have been encrypted and harm anyone dependent on the attacked organization's goods and services.
- 94% of companies said obtaining cyber insurance has become more complex over the past year. The insurance industry is under tremendous pressure due to the increase in ransomware attacks and the prevalence of nation-state threat actors using cyberspace as an asymmetric warfare tool.

ABOUT SOCRadar®

Who is SOCRadar?

As an Extended Threat Intelligence (XTI) platform and inventor of the concept, SOCRadar's approach effectively integrates Threat Intelligence, Digital Risk Protection, and External Attack Surface Management (EASM). Adapting proactive security with a hacker mindset, we aim to help security teams to detect blindspots before attackers.

SOCRadar provides extended cyber threat intelligence (XTI) that combines Cyber Threat Intelligence, Digital Risk Protection, and External Attack Surface Management Services. SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Darknet and Deep Web Monitoring: SOCRadar's fusion of its unique dark web Recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

Protecting Customers' PII: Scan millions of data points on the surface web, deep web, and darknet to accurately identify the leakage of your customers' personally identifiable information (PII) in compliance with regulations.

360-Degree Visibility: Achieve digital resiliency by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

Why Global Ransomware Report?

SOCRadar researchers monitor the activities of 45+ ransomware groups simultaneously. The researchers followed the activities of the groups throughout 2021 and until June 2022. They analyzed which countries and industries and at what frequency were targeted by the attackers.

These studies shed light on the sector, geography, and ongoing attacks and allow the defenders to evaluate themselves. When you actively monitor ransomware groups, you realize that many new groups are established without a gap when a group is disbanded. No market allows a gap. Ransomware never does.

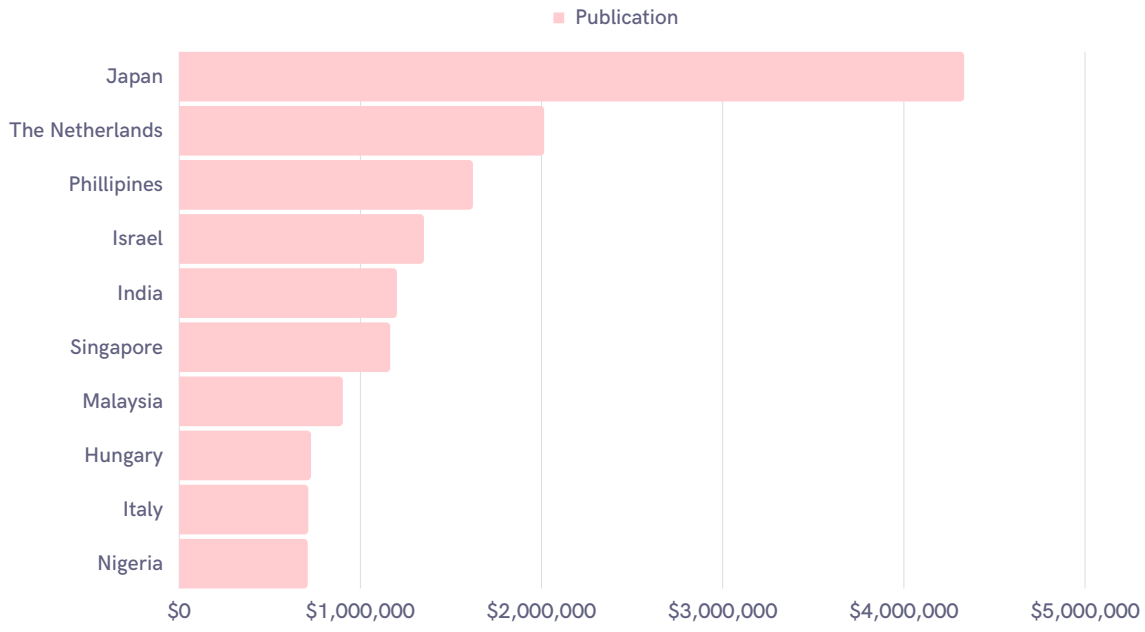
Introduction

Ransomware is a type of malware that encrypts a victim's files. The attacker demands a ransom so the victim can regain access to their data.

Users are given instructions on how to pay a fee to receive the decryption key. The ransom fees are requested in cryptocurrencies, usually in Bitcoin. The ransom amount can range from a few hundred to thousands.

Although many institutions, especially law enforcement agencies, recommend that targets who are attacked by ransomware not pay ransom to attackers. However, many institutions, including state governments in the USA, prefer to pay ransom to attackers. One thing to remember is that even if the ransom is paid, it may not be possible to recover the encrypted data because there is no reasonable justification for cyber attackers to keep their word.

Whether the data is recovered, attackers always try to extract valuable data from a compromised machine. All sensitive data on the device could be compromised, including usernames and passwords for internal or web resources, payment information, email addresses of individuals, and more.



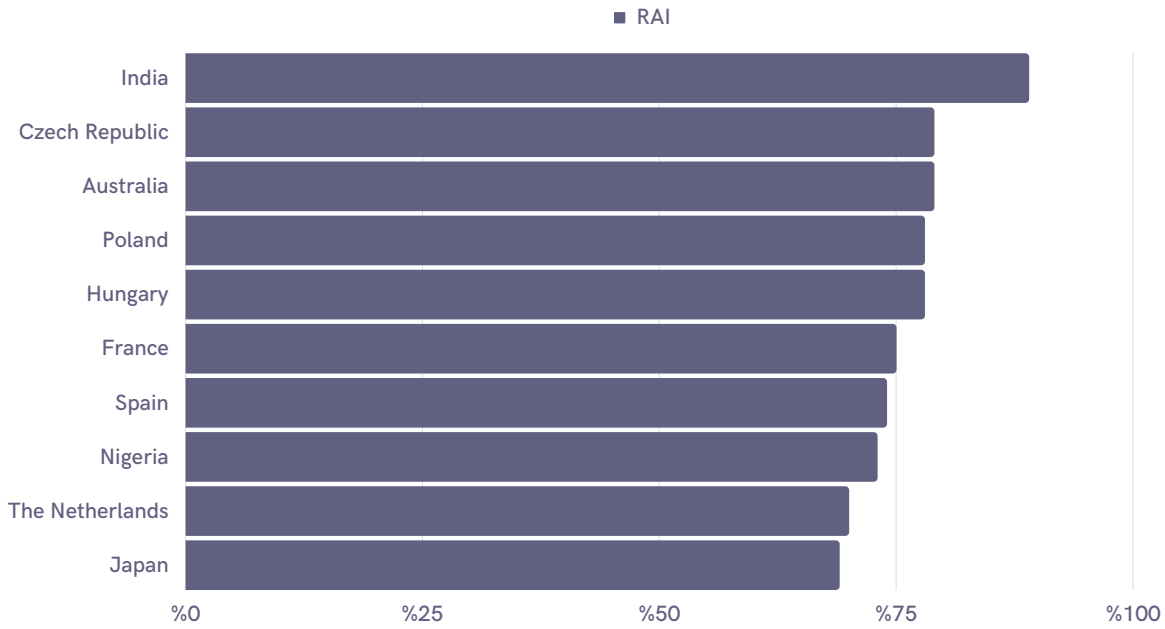
Average Ransom Payments by Country ($) (Source: SOPHOS The State of Ransomware 2022)

Ransomware attacks on organizations and individuals have many adverse effects, such as:

- Temporary or permanent loss of sensitive and private information,
- Disruption of regular operations,
- Financial losses incurred to restore systems and files, and
- Loss of reputation.

Although there are cybercrime gangs and nation-state-supported hacker groups among the cyber threat actors who resort to ransomware attacks, other organized crime groups have added cyber capabilities to their structure and use these attacks as a source of income.

It is also known that states subject to sanctions by regional and international institutions, such as Iran, Russia, and especially North Korea, use ransomware attacks to obtain crypto money to provide hot cash flow.



Encryption Rate (%) in Ransomware Attacks (Source: SOPHOS The State of Ransomware 2022)

Ransomware Attack Vectors

Since ransomware has threatened companies for decades, it's not considered an unexpected threat. Despite that, organizations large and small continue to be trapped by file-encrypting malware. Ransomware attacks often leave organizations choosing between rebuilding most computer systems from scratch or paying ransom to cybercriminals.

When the companies that have been attacked by ransomware are analyzed, three common attack vectors are recurring: e-mail phishing attacks, remote desktop protocol, and security vulnerabilities.

Phishing Attacks

E-mail phishing remains the top attack vector for ransomware campaigns. This is because phishing emails are easy to send and give attackers a faster return on investment. As part of social engineering schemes, phishing urges victims to act before they realize that a malicious threat actor is targeting them.

The later the targeted user becomes aware of the attack attempt, the more efficient the attack will be for the attacker. Similarly, targeted attacks are intended to make phishing emails appear from a trusted sender.

When users perform the action requested by the attacker (click on the given link, etc.), their data is encrypted and directed to the necessary instructions for paying the ransom. Phishing emails that install credential-stealing malware or remote access trojans also remain a common attack vector.

RDP

It is a legitimate tool that allows IT administrators to access systems remotely. However, any criminal who can access RDP endpoints can use connected systems to gain a foothold in a corporate network and attempt to access many other related systems by escalating their privileges.

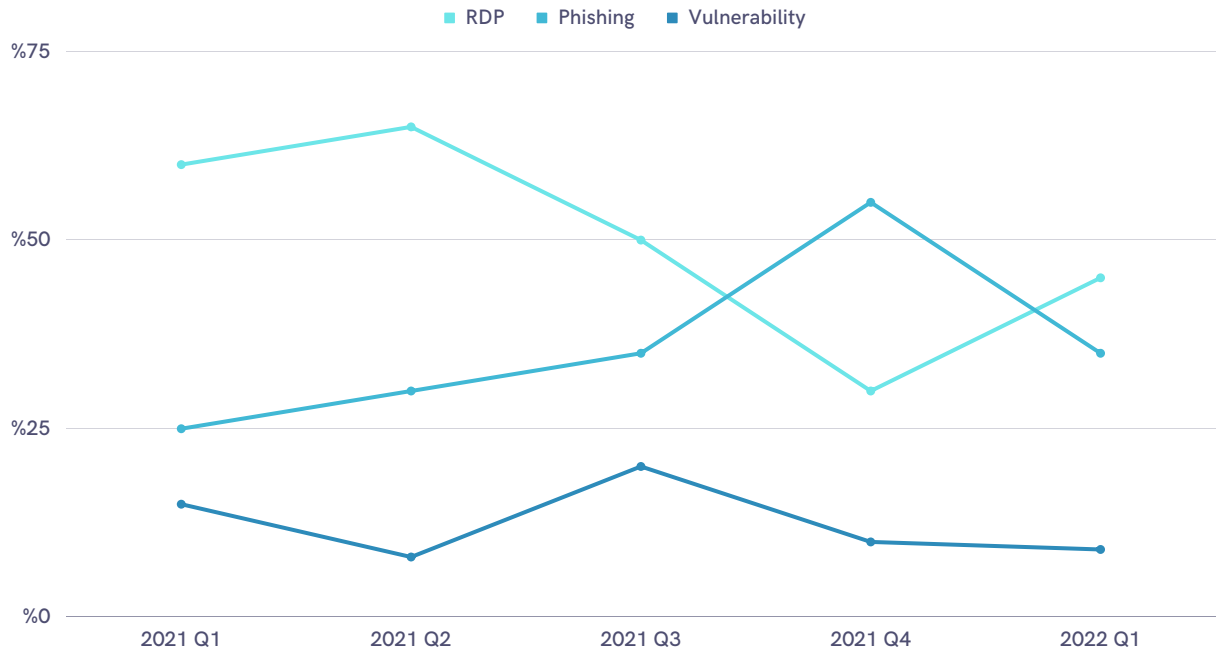
With the pandemic, many employees started to work from their homes rather than workplaces. This transition increased the use of RDP by 41%. As a result, the number of threat actors using RDP to gain access has also increased.

In Q1 2021, compromised remote desktop protocol connections were the most common attack vector. RDP remains a common security vulnerability despite well-known secure remote connection best practices.

Vulnerabilities

Even though there are patches for the vulnerabilities in the software, not patching them creates an excellent opportunity for ransomware attackers.

Most major ransomware attacks are carried out by exploiting known vulnerabilities. Postponing updates not to risk business continuity leaves the door open to cyber attackers looking for an opportunity to infiltrate systems. Conti launched attacks throughout 2021 using more than 30 vulnerabilities.



Distribution of Worldwide Ransomware Attacks by Vectors Between the First Quarter of 2021 and 2022 (Source:Coveware)

Global Ransomware Trends

One of the critical points in the fight against cyber-attackers is understanding how threat actors update their operations and how they move their focus. In a dynamic environment such as cyberspace, where threat elements continually change, new attack vectors are added to existing ones, and digital assets can potentially become a risk at any moment. Therefore, it is critical to predict the cyber criminals' next move. Cyber threat intelligence will provide organizations with strategic gains in the effective fight against the cyber risks they face.

The technical infrastructure of ransomware attacks, the behavioral patterns and motivations of the groups organizing the attacks, and strategic and operational intelligence, such as how the groups choose their targets, is essential. Because this intelligence provides proactive protection to institutions against ransomware attacks, at the same time, it also provides institutions with a roadmap for what steps to take when an attack occurs.

According to 2021 data:

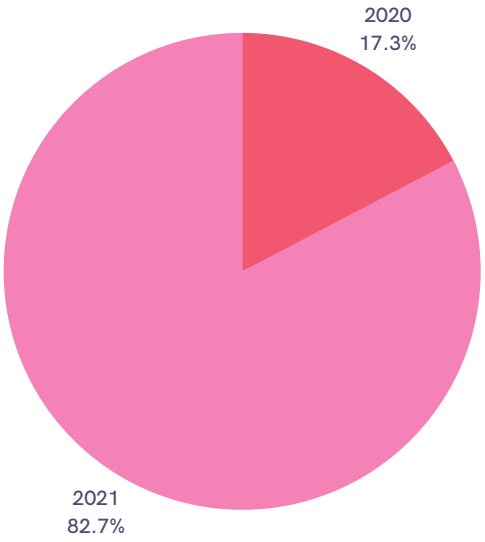
- 66% of organizations have been attacked by ransomware.
- 46% of ransomware victims got their data back by paying cybercriminals.
- Also, 26% of organizations able to restore data from backups still decided to pay the ransom.
- The highest average ransom payments were in the manufacturing sector at $2.04 million and in energy and utilities at $2.03 million.
- The lowest average ransom payments were in healthcare at US$197,000 and state/local governments at US$214,000.

Increasingly, ransomware attackers use two ways to pressure their targets to pay the ransom. One of them is to disclose the data in the system they infiltrated, which they think is essential for the institution, through the websites established for this job.

It aims to undermine the institution's reputation and drag it into internal turmoil by leaking information that is "private" to the institution, from the imbalance in the employees' wages to the offers given to the customers. Organizations are given a threatening time limit and amount. Then the private data is started to be shared when payment is not made.

Another pressure method by ransomware groups is the threat of DDoS attacks. Threat actors threaten organizations that refuse to pay the ransom with DDoS attacks on their systems.

SunCrypt is a ransomware group that uses DDoS as a pressure element. The SunCrypt team has started performing DDoS attacks on the websites of the targeted institutions that are unwilling to pay the ransom or leave the negotiations. This way, the group aims to get the desired ransom from the attacked institutions.



Relation of Ransomware Ransom Payments to Countries' Poverty Rate (Source: SOPHOS The State of Ransomware 2022)

Average Ransom Payment

The average ransom payment has nearly doubled over the years, and this trend shows no signs of slowing down. While a few thousand dollars may seem insignificant for large businesses, it can be paralyzing for smaller companies that can't afford to lose their data.

Paying a ransom due to a ransomware attack is twice the cost of dealing with a ransomware attack.

Average ransom payments rose from $170,000 in 2020 to $812,000 in 2021.

Cost of Downtime Due to Ransomware Attack

Even the most straightforward ransomware software, ever-evolving as an attack tool, can cost significant time and money. Still, more severe attacks can deal a crippling blow or destroy a company before it saves anyone, even large, leading organizations.

Unprepared users and businesses can quickly lose valuable data and money from these attacks. This is particularly dangerous in times of economic uncertainty, as individuals and companies seek to manage and mitigate risks while planning.

A ransomware-based cyberattack by hackers causes much more monetary damage than ransom payments. Most companies are experiencing operational disruptions/interruptions along with data loss due to a ransomware attack. Downtime causes a severe loss of customers` trust in the company and the cost of lost business.

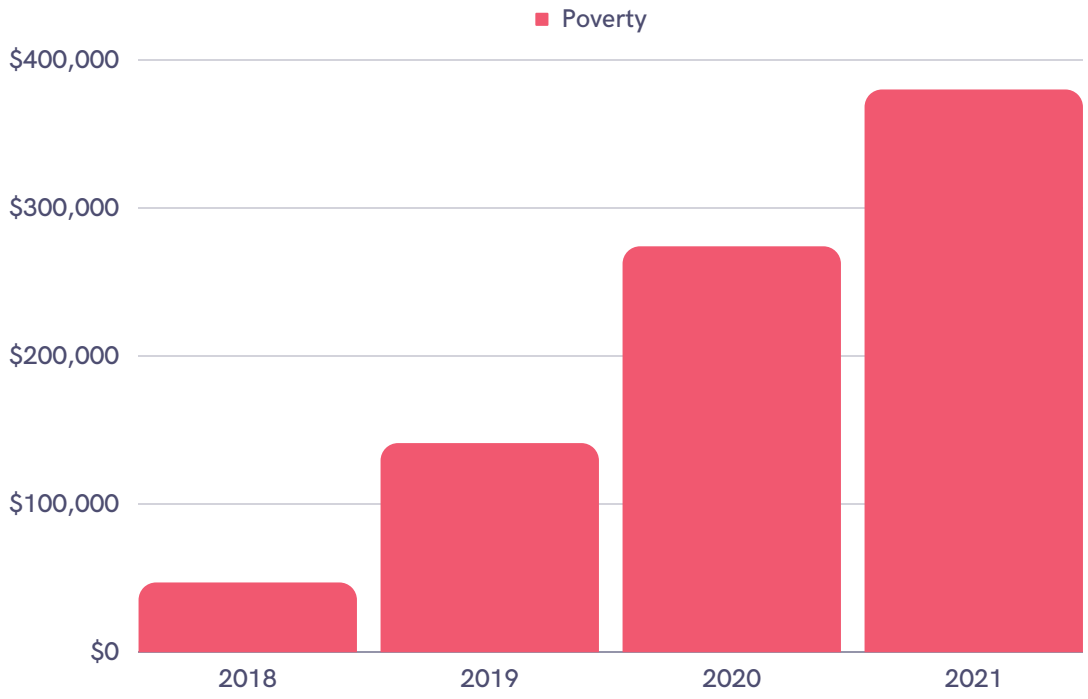
When long downtimes are experienced in institutions that operate critical infrastructures such as hospitals, financial institutions, and internet operators, it causes serious problems that will negatively affect social life.

The UHS hospital network, a Fortune 500 company with more than 400 hospitals, suffered a massive outage from a ransomware attack. The institution had to turn away some patients and close its emergency room and laboratory.

Some hackers corrupt and delete a company's files while they wait for a ransom payment to show they are serious. Regardless of the cybercriminal's ultimate actions, the actual cost of ransomware goes beyond mere price.

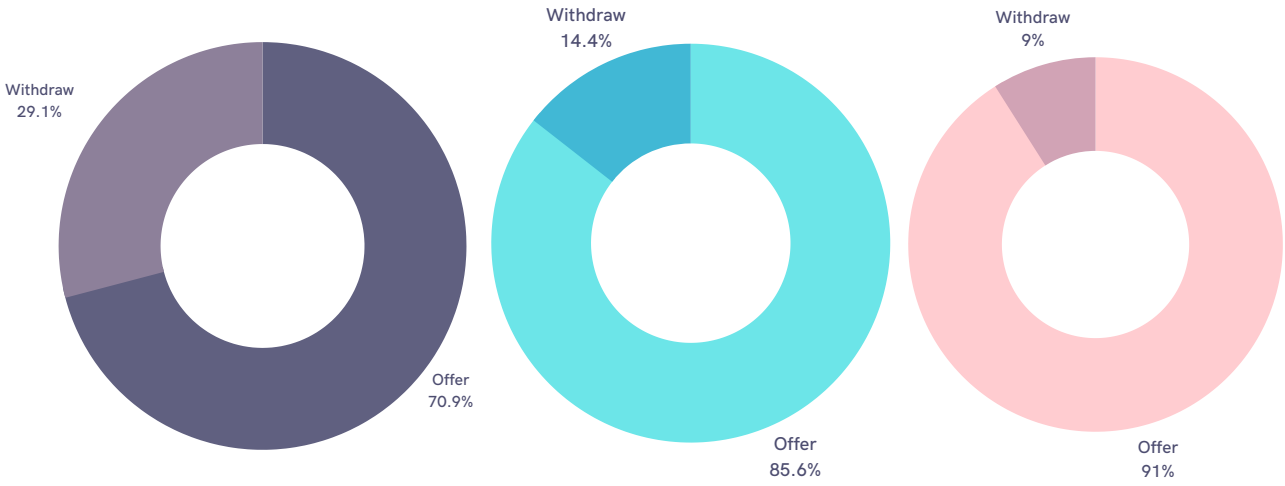
Digital extortion by hackers ultimately does more monetary damage than hackers can generate from an attack. Most companies say they have experienced data loss and significant outages due to a ransomware attack. These consequences are extremely costly, especially for larger businesses with hundreds of employees.

Significant outages can result in millions of dollars in lost revenue and a rapidly increasing cost. The average price of downtime caused by ransomware has doubled in recent years. Even worse, downtime also reduces consumer confidence, especially in cultures that value their relationships with the organizations, hurting future businesses.



Relation of Ransomware Ransom Payments to Countries' Poverty Rate (Source: Safetydetectives: Ransomware Facts, Trends & Statistics))

Most Dangerous Ransomware Groups

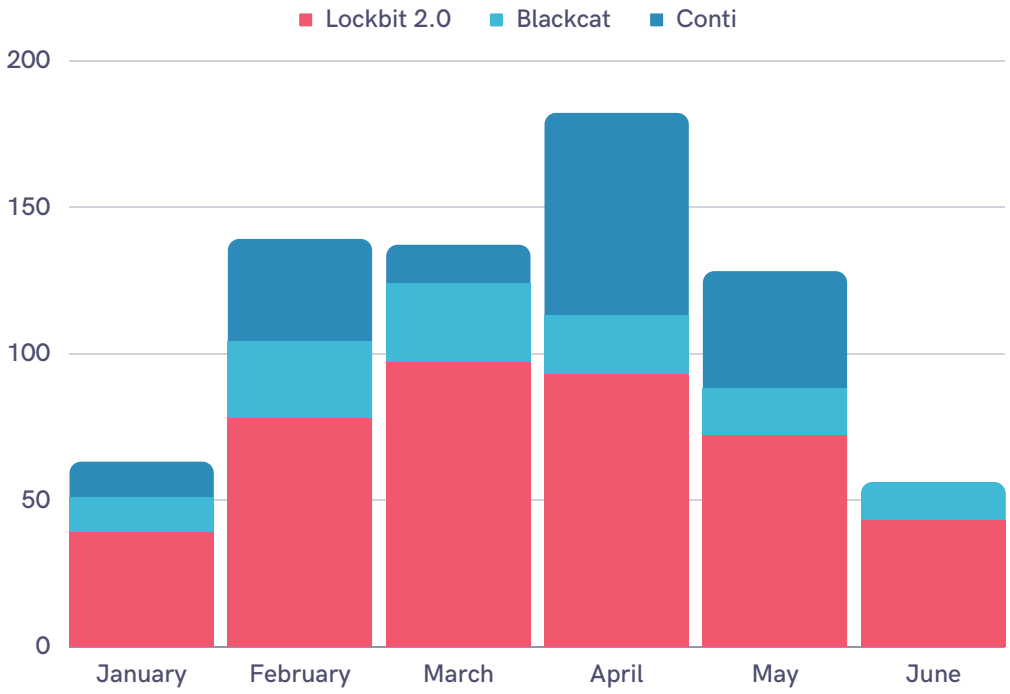


Withdraw and offer rates of the first three ransomware groups "32 % LockBit 3.0 , 13 % Conti , 9 % AlphVM BlackCat" (Source: SOCRadar)

Knowing the enemy is one of the most critical steps of defense. Knowing the most active groups that actively targeted institutions in 2021 and if they stopped or continued their attacks in 2022, analyzing their key tactics and critical attacks is one of the essential items in preparation for ransomware attacks.

Russia-based REvil group, immensely active in 2019 and 2020, can be seen behind many ransomware attacks in that period. The United States offered a reward of up to $10 million for information to identify or locate individuals in key leadership positions in the Revil gang.

In early 2022, Russia said the ransomware group REvil had "disappeared" after raids and arrests. The Russia-based Conti group, which we saw its first activities in 2020, has emerged as the most active group in 2021. Like REvil, the United States government offered a reward of up to $10 million for information about the group in early May 2022.



Ransomware Attacks in the First Half of 2022 (Source: SOCRadar)

The Conti group made public statements and blamed the American government after an article by Reuter detailing the US Government's collective actions to eliminate the REvil ransomware group.

SOCRadar researchers keep tracking ransomware activity. Our focus is on the malicious actor groups behind the three ransomware families that have run the most significant number of successful attacks.

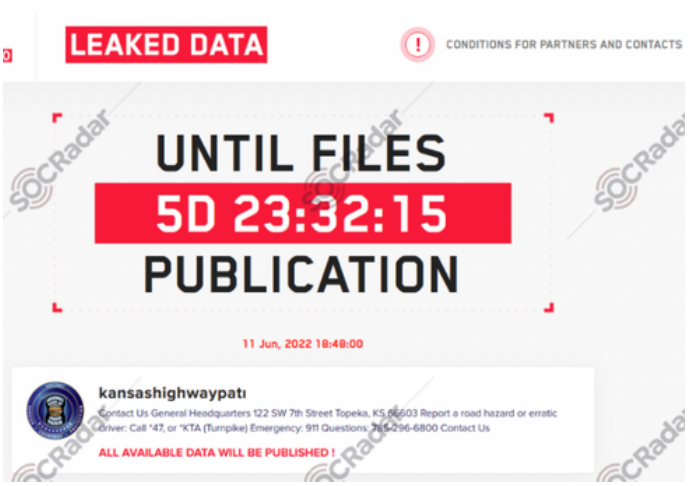
- LockBit 2.0 group claimed the most ransomware attacks in 2021 and 2022,
- Conti group, which went into disbandment at the end of May 2022,
- Blackcat group, rising actor of 2022

LockBit 3.0

The LockBit group is a Ransomware-as-a-Service (RaaS) operator and has been active for about 3.5 years. They were formerly known as the ABCD ransomware group. For six months, they have been promoting their latest ransomware, LockBit 2.0.

Recently, the number of developers and threat actors associated with the LockBit group has been increasing. As a result, more LockBit 2.0 ransomware attacks can be expected shortly. LockBit 2.0 is the latest ransomware released in August 2021 by the LockBit ransomware group. The group's ad claims to provide the fastest encryption ransomware.

Also, ransomware operators modify ransomware based on threat actors' needs. LockBit 2.0 ransomware searches system and user settings. It will not attack the system if the language is set to specific languages.



According to SOCRadar Platforms data, LockBit 2.0 published 450 attacks in 2021 and was followed as the group that carried out the most attacks.

When we reached June 2022, it was identified as the most active group among all monitored ransomware groups, with 379 attacks. Operators and affiliates behind the LockBit ransomware started transitioning to LockBit 3.0 around June 2022.

Rapid affiliate adoption of LockBit 3.0 has resulted in many victims being named on the new "Version 3.0" leak sites, a network of public blogs that identify non-compliant victims and release extracted data.

Conti

The Conti group is among the most dangerous threat actors. They began their first activities in early 2020 and made harmful attacks in 2021. According to SOCRadar data, Conti was the second group that initiated the most attacks publishing 412 attacks in 2021.

However, in 2022, we see that the Conti group has disbanded. According to research, the group's first disagreements started in late February after Russia invaded Ukraine. Shortly after the war began, Conti pledged support to the Russian government and threatened to attack the critical infrastructure of his enemies. Later Conti softened the initial statement, but it was already too late. Expressing support for the Russian government ignited internal debate and leaked internal data, including chats and source code.

The factor that determined the fate of the Conti group was that the commitment of allegiance to Russia led to the group's association with the Russian government.

Russia's war against Ukraine has received significant sanctions from the western nations, meaning that any payment to cyber criminals, including Conti, could be considered a payment to Russia, which would be an indirect violation of the sanctions. Therefore, Conti had essentially cut himself off from his primary source of income, as many victims were found to be barred from paying ransom to Conti. Other victims and companies negotiating ransomware payments were more prepared to risk the financial loss of not paying the ransom.

Even though Conti became a toxic brand, the operation was too large and profitable to be scrapped entirely.

However, the Conti leadership decided that instead of suddenly disappearing after the REvil group's experience - REvil tried this approach, and it didn't go well - they would gradually move on to a new strategy long before the Conti brand expired.

The researchers say the Conti group now includes fully autonomous groups such as Karakurt, Black Basta, and BlackByte that do not use data-encrypting malware and instead rely solely on stealing valuable information to blackmail victims. Researchers have previously noted that some of these groups appear to be linked to Conti.

Blackcat

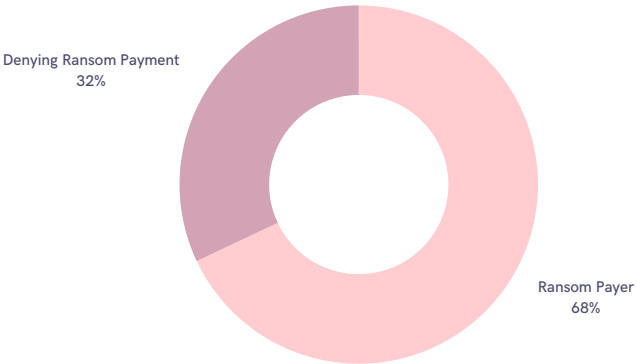
BlackCat Ransomware operates as the RaaS (Ransomware-as-a-Service) model. In other words, they give other attackers access to infrastructures and malicious code. In return, they receive a share of the ransom. Also, members of the BlackCat gang are likely responsible for interviews with victims. All their affiliates have to do is gain access to the corporate environment. BlackCat is gaining momentum so fast because of its "all-inclusive" principle. Their malware was already used to attack companies worldwide.

BlackCat has several services. The first is the encryptor of the same name. Thanks to the cipher they wrote in Rust, the attackers created a cross-platform tool with malware versions that work in both Windows and Linux environments. In BlackCat ransomware incidents, companies in the oil, gas, mining, and construction industries have observed at least one attack. The software has also infected several customers of an enterprise resource planning provider based in the Middle East.

SOCRadar Ransomware Attacks Analysis

Attackers generally make announcements first, threatening companies with exposing data. They share the data publicly if they do not receive the relevant payment. When the graph above is analyzed, we can interpret that 68% of the attacked companies are trying to prevent data leakage by paying. In some scenarios, data leaks may occur without any announcement. Although the figures above provide approximate results, we can say that 32% of the attacks avoid payment, based on the data analysis revealed after contacting the company directly or the ransomware group's primary broadcast.

When both 2021 and the period till June 2022 are examined, SOCRadar researchers found that an average of 18% of all companies were attacked by more than one ransomware group.



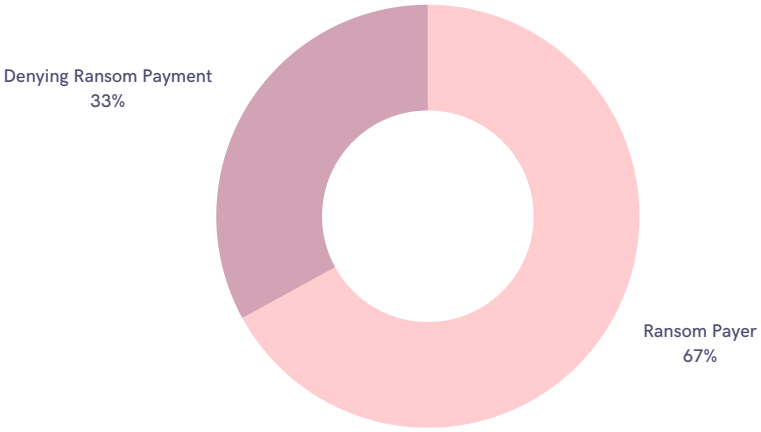
Proportion of Paying and Refusing Payments in Ransomware Attacks in 2021 (Source: SOCRadar)

SOCRadar researchers actively monitor ransomware groups and their activities. Every day, a new ransomware group is started to be monitored, and existing groups may disperse or stop their activities due to raids. While it is often possible for researchers to combine the activities of a new group with a previous group as a new ransomware group becomes popular, their affiliation remains only an estimation unless the group attributes itself as the continuation of the previous one. Although the following TTPs give an idea about a new group, the TTPs could change when attackers regroup.

Detailed analysis was carried out by researchers on a total of 1987 ransomware during 2021. 1351 of the published attacks are in the form of announcements (the attacker announces that the victim is infected with ransomware and then gives the attacked company a specific time). 636 are data breaches (data disclosure at the end of the given period, in some cases, we also see data sharing without an announcement).

When we consider attacks until June 2022, researchers conducted a detailed analysis of 1154 ransomware cases. 772 of these attacks were in the form of announcements, and 382 were in the form of data leaks. Since the values are similar to 2021 rates, SOCRadar thinks that about 68%-70% of companies have reached an agreement with the attackers. Between 32-35% of companies refuse to pay. Compared to the 2022 survey results, we can say that the number of paying companies is relatively high.

The researchers recorded fundamental facts such as the event, history, responsible criminal gang, victim information, and the victim's industry and geography.



Proportion of Paying and Refusing Payments in Ransomware Attacks in the first half of 2022 (Source: SOCRadar)

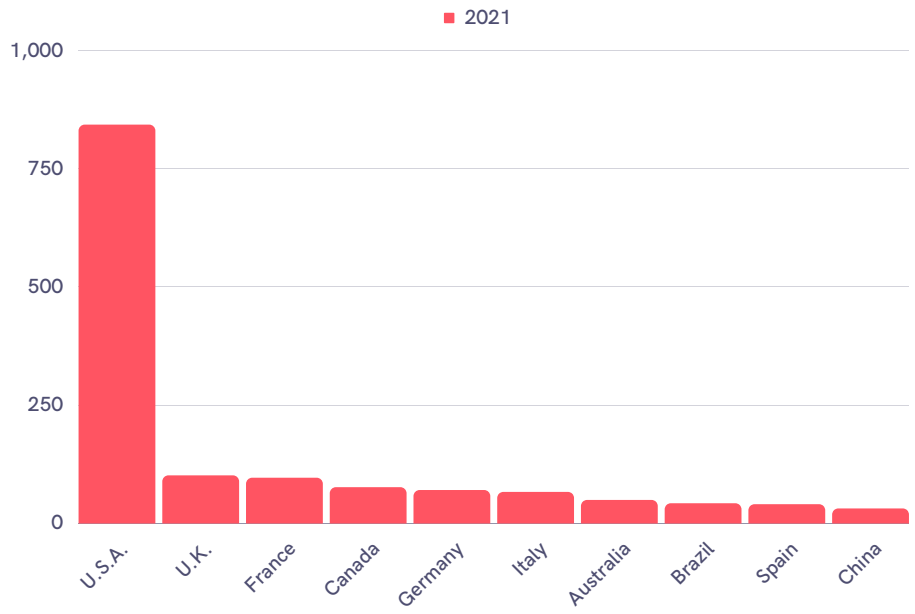
Countries Targeted by Ransomware Attacks

In the 1987 ransomware attack, detected by SOCRadar researchers throughout 2021, there were attacks targeting 102 different countries. Among these countries, not only economically and infrastructurally rich countries but also attacks in countries such as Bangladesh and Haiti were observed.

We can conclude that the attackers targeted companies in the United States the most for 2021 in continental Europe and the Americas.

When we examine the countries where ransomware attacks are most common, we see a significant increase compared to the previous years, especially in Brazil. One of the main reasons for this is recent data breaches in the Brazilian region. Leaked personally identifiable information (PII) data from the breaches can be used as phishing material for ransomware attacks.

When we evaluate the year 2021 in Turkey, we see that a total of 42 companies whose activities are in Turkey are targeted. Only 16 of these companies are based in Turkey. Also, 2% of all attacks target Turkey.

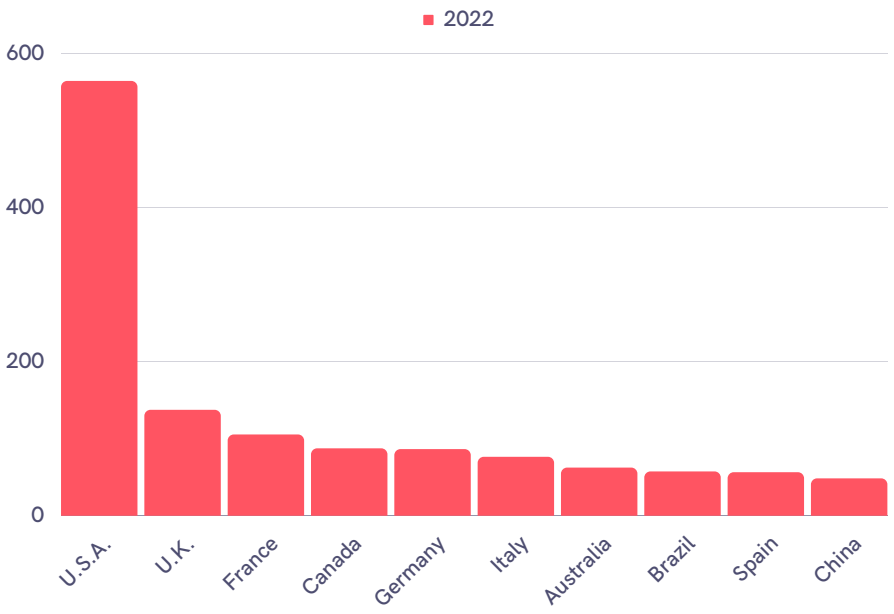


Countries Targeted by Ransomware Attacks in 2021 (Source: SOCRadar)

A total of 1154 ransomware attacks were monitored until June 2022. We can observe that most of the attacks were targeted against companies in the United States of America.

The population size of the United States, the excess number of companies, and the fact that the headquarters of many companies worldwide are in the United States are essential factors. In addition, ransomware groups usually based in Russia are another critical reason for targeting American companies.

Companies based in Australia, Germany, Canada, Italy, UK continue to be targeted in 2022 as in 2021. Unlike in 2021, we see increased attacks on Swiss-based companies in 2022.



Countries Targeted by Ransomware Attacks in 2022 (Source: SOCRadar)

Industries Targeted in Ransomware Attacks

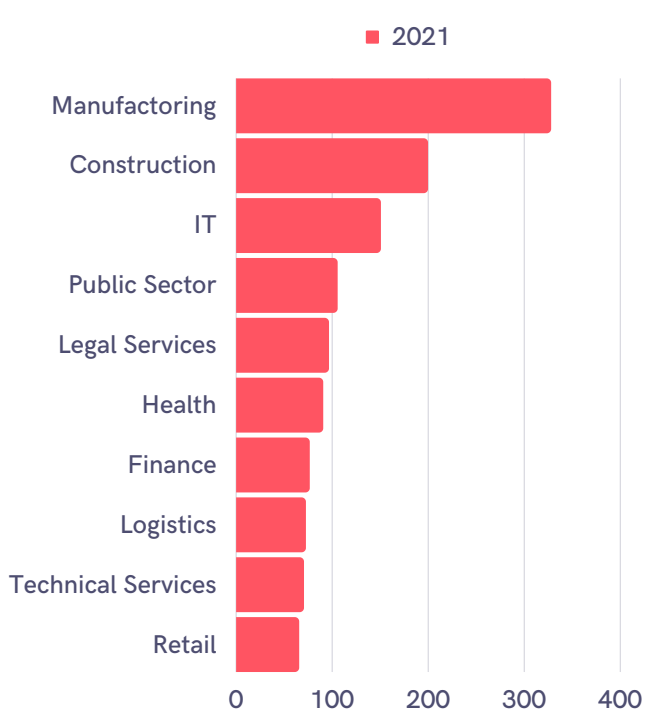
While research shows that ransomware attackers don't have a sectoral selectivity for their targets, they do show that they focus on sectors that will do the most damage and where the targets will have to pay the ransom. One of these sectors is the manufacturing sector. Nearly one-fifth of ransomware attacks target the manufacturing industry, according to statistics from 1987 attack patterns tracked through 2021.

The second most targeted sector is the construction sector for similar reasons as the production sector.

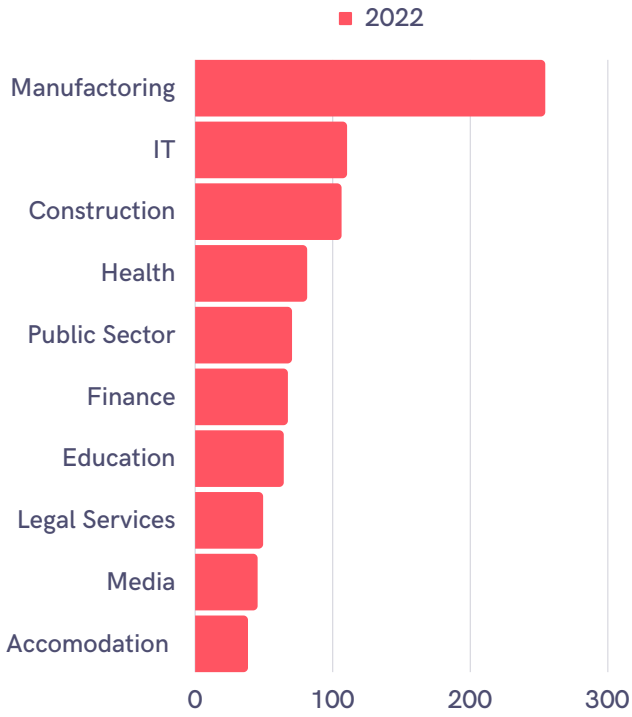
While the attacks on the IT sector have increased rapidly and placed in third place, the attacks on government institutions have decreased compared to the previous years.

Attacks on these three sectors show that ransomware threat actors are looking for victims, such as manufacturing and production networks, with a low tolerance for downtime. Organizations that need high uptime can lose millions of dollars daily due to downtime. Therefore, ransom payments will be more likely to regain data access and continue operations.

In addition to these sectors, an increase is observed in ransomware attacks on the energy sector. Especially the Colonial pipeline case in May 2021 showed us that a cyber attack that may occur in the energy sector has political and chaotic consequences.



Industries Targeted by Ransomware Attacks in 2021 (Source: SOCRadar)



Industries Targeted by Ransomware Attacks in 2022 (Source: SOCRadar)

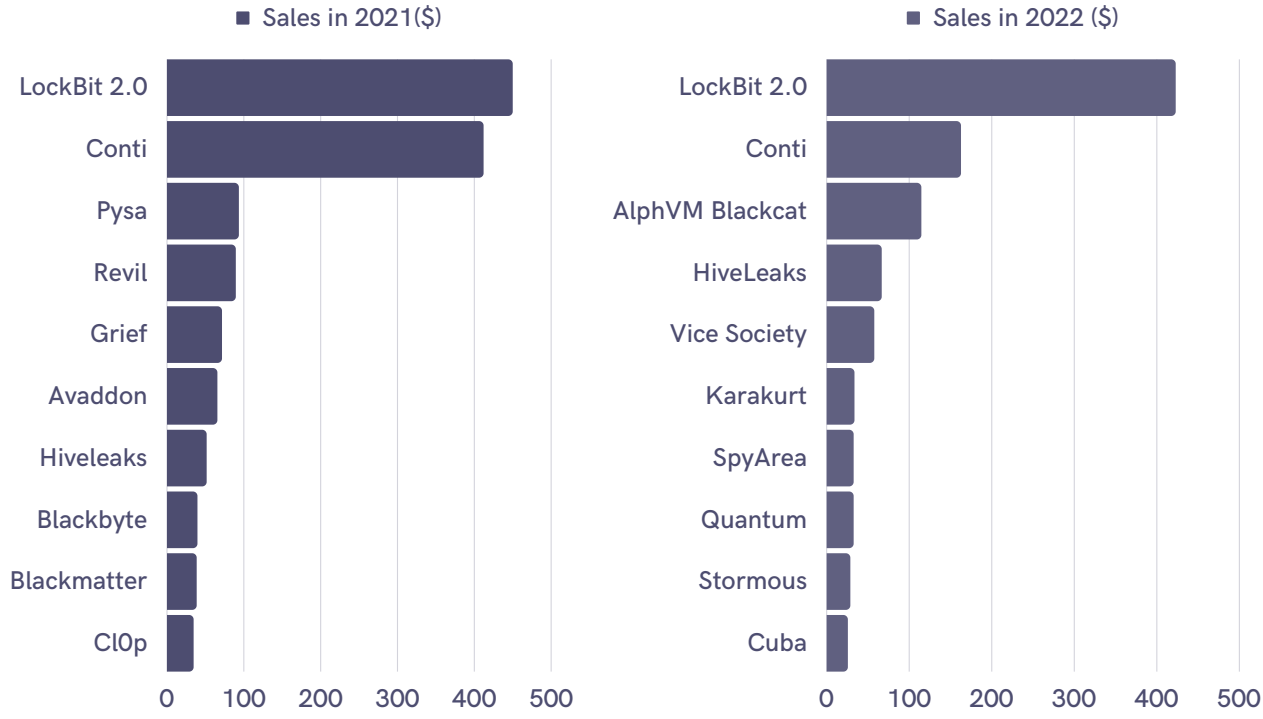
When the statistics until June 2022 we examined;

While the manufacturing sector is still at the forefront, we observe that the ransomware attacks against the sectors serving in the IT sector are increasing.

Groups Performing Ransomware Attacks

SOCRadar researchers are actively monitoring the activities of more than 45 ransomware groups.

- The ten groups that carried out the most attacks in 2021 within the SOCRadar research framework are listed in the table below.
- The ten groups that carried out the most attacks in the first five months of 2022 within the SOCRadar research framework are listed in the table below.



Breakdown of Attacks by Month

The distribution of attacks followed by SOCRadar researchers by months is given in the tables below.

Prevention and Protection

Dealing with the consequences of ransomware attacks is quite an arduous process. Sending the ransom may seem like the only option to recover locked data. However, paying the ransom does not mean that your organization will return the affected data.

Because of that, you are detecting an ongoing ransomware attack is not good enough. It would help if you focused on preventing ransomware infection in the first place. You can do this by following the safety precautions listed below:

1- Take Out Your Digital Asset Inventory

To protect yourself against ransomware, you must first know what hardware and software assets are connected to the network. You should create a comprehensive list of assets by passive discovery to identify assets used by staff from different departments.

2- Customize Your Anti-spam Settings Properly and Use Powerful Spam Filters

Most ransomware is known to spread via deceptive emails with malicious attachments. Some of these attachments may contain Word documents or other file formats commonly used in your organization. Some may come in a rarely used form, either. Many ransomware actors think they can get through your email filters by hiding their payload in attachments that contain compressed or archived files. That's why you need powerful spam filters that block such files from reaching users.

3-DO NOT Open Suspicious-looking Attachments

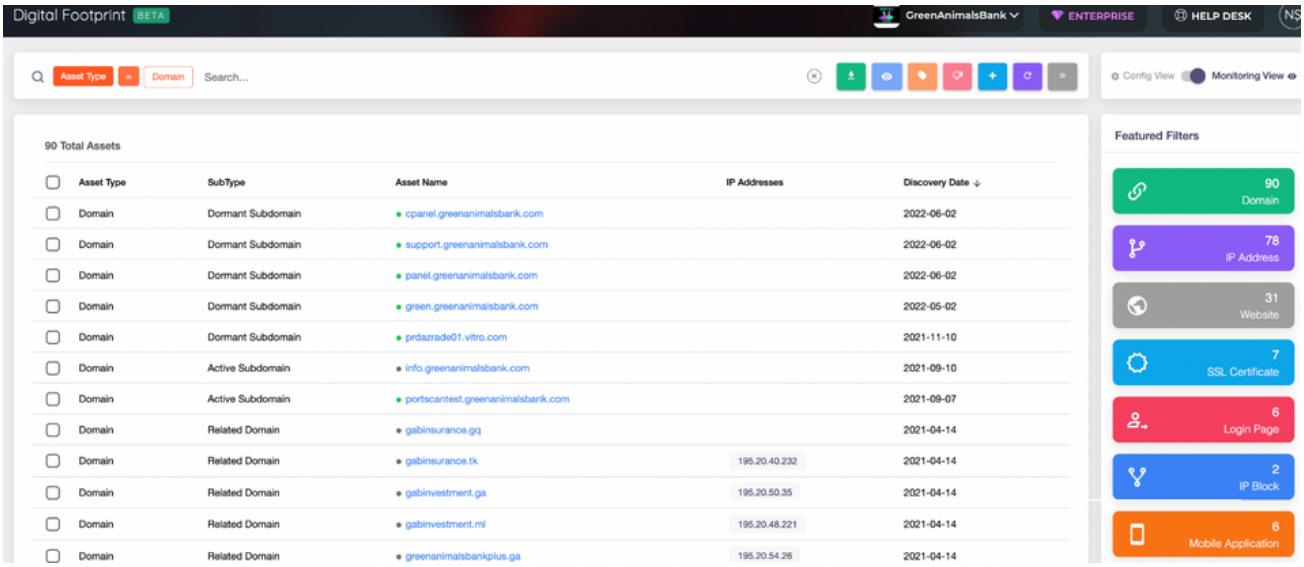
This item applies to messages sent by people you do not know, and senders you believe are your acquaintances—the vast majority of ransomware attacks that originate from phishing result from obtaining the credentials of administrator-level employees.

4- Avoid Giving Personal Information

Malicious actors can target the ransomware to send a phishing email, but they need to get your information from somewhere. They could get this information from a data breach posted on the dark web. However, they could also obtain it using OSINT techniques by reviewing your social media posts or public profiles for private information.

5-Use the Show File Extensions Feature

Show File Extensions is a native Windows function that lets you quickly identify what files are being opened to avoid potentially harmful files. This small trick is handy when scammers try to use a confusing technique where a file appears to have two or more extensions.



6-Patch Your Software and Keep It Updated

In the absence of a patch, malicious actors can exploit a vulnerability in your operating system, browser, antivirus tool, or other software programs with the help of an exploit kit. These kits contain codes for exploitation of known vulnerabilities that could allow them to drop ransomware and other malicious payloads.

7- Authenticate E-mail Users

It will help if you use technologies such as the Sender Policy Framework (SPF), Domain-based Message Authentication Reporting & Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent malicious individuals from using email spoofing techniques.

8-Install a Browser Plug-in to Block Pop-ups

Pop-ups serve as a common entry point for attackers to launch ransomware attacks. That is why you should look into installing browser add-ons to stop pop-ups.

9-DO NOT Use Unfamiliar Media Devices Like USB Sticks

It is a known attack method for cyber attackers to compromise an organization's supply chain and send media devices with trojans. It would be best if you did not use media devices that do not belong to you.

10-Make Sure You Disable File Sharing

It would be best if you disabled file sharing to prevent attackers from infecting multiple machines in your environment. In the event of a ransomware attack, the malware will remain isolated on the infected device and will not spread to other assets.

11-Disable Remote Services

Attackers can use remote Desktop Protocol to expand the attack surface and gain a foothold on your network. To block this threat, you should disable remote services. Doing so will help close a vector for remote attacks.

12-Turn Off New Wireless Connections Such as Bluetooth or Infrared Ports

There are cases where attackers use Bluetooth to compromise a machine. It would be best if you addressed this threat vector by turning off unused Bluetooth, infrared ports, and other wireless connections in the organization.

13- Block Knew Malicious Tor IP Addresses

Tor (short for the Onion Routing project) gateways are one of the primary means for ransomware to communicate with Command&Control servers. Therefore, you can block known malicious Tor IP addresses as it can help prevent critical malicious processes from getting through.

14- Disable Windows Script Host

Some cyber criminals use.VBS files (VBScript) to run ransomware on an infected computer. It would be best if you disabled Windows Script Host to prevent malware from using this file type.

15- Disable Windows PowerShell

PowerShell is a task automation framework specific to Windows computers. It consists of a command line shell and a scripting language. Attackers often use PowerShell to run ransomware from memory, helping to evade detection with traditional anti-virus solutions. So unless you have a legitimate use for the framework, you should consider disabling PowerShell on workstations.

16- Increase the Security of Your Microsoft Office Applications

Cybercriminals tend to use weaponized Microsoft files to distribute their malicious payload. These files specifically use macros and ActiveX. Recognizing this fact, you should disable macros and ActiveX to prevent malicious code from executing on Windows PC.

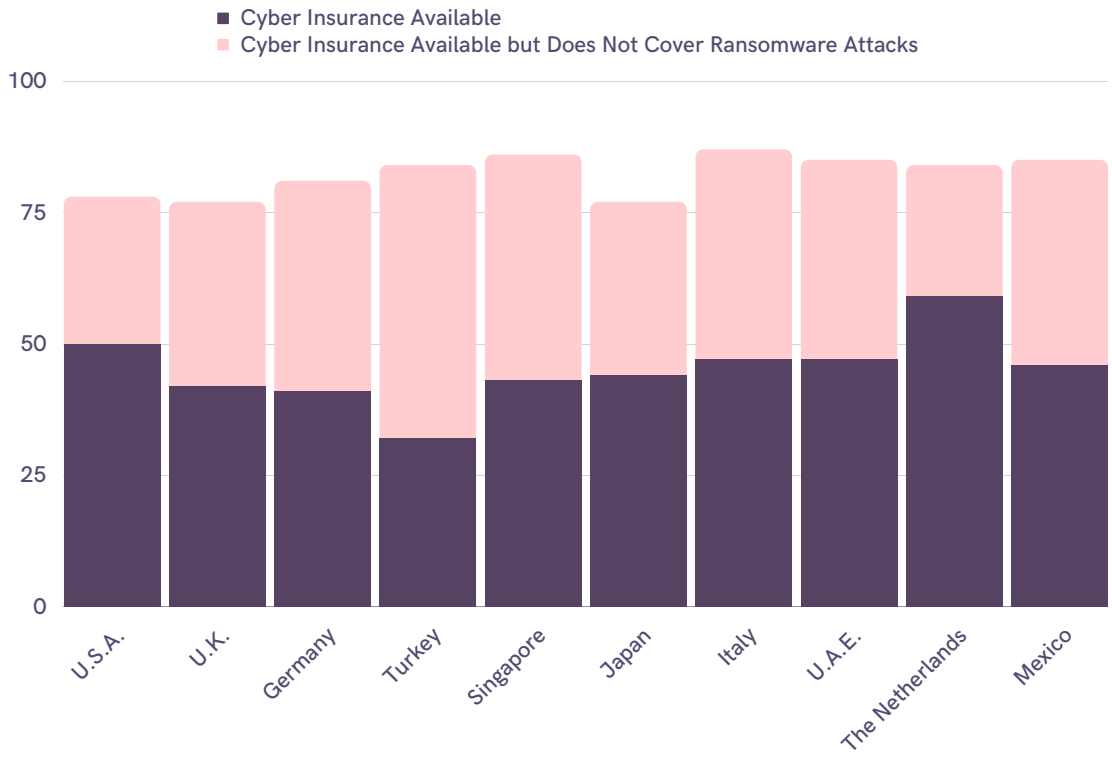
17-Disable the Web Immediately If You See Any Suspicious Activity on Your Computer

This technique is particularly effective at an early stage of the attack. Most ransomware instances must connect to command and control (C&C) servers to complete their encryption routines. Without access to the Internet, ransomware remains idle on an infected device.

Such a scenario allows removing the malicious program from an infected computer without decrypting any data. This trick is helpful to help prevent ransomware infection since it uses ProgramData, AppData, Temp, and Windows\SysWow.

5 Suggestions:

1-Start with the assumption that you will be attacked
2-Invest in relevant technologies to protect against ransomware
3-Make sure your cyber insurance covers ransomware.
4-Train your users
5-Use cyber threat intelligence solutions



Percentage of Organizations with Cyber Insurance

Decryption Tools That Can Be Used in Ransomware Attacks

When you are attacked by ransomware, the attackers encrypt digital files on your device. Even if you pay the attacker ransom to get the password, there is no guarantee that you will get your files back. The No More Ransom site, prepared by Europol and some cybersecurity companies, with concrete suggestions on what to do when you are attacked, could help you:

https://www.nomoreransom.org/tu/index.html

They check if there is a suitable solution by filling out a form to determine the type of ransomware infecting your systems through its service on the community website. In addition, the project includes password-cracking tools from many security companies that contributed to the initiative.

How Can You Use SOCRadar for Early Detection of Ransomware Attacks?

SOCRadar, with its Extended Threat Intelligence service, helps you protect yourself from ransomware attacks with the following modules.

SOCRadar Attack Mapper module

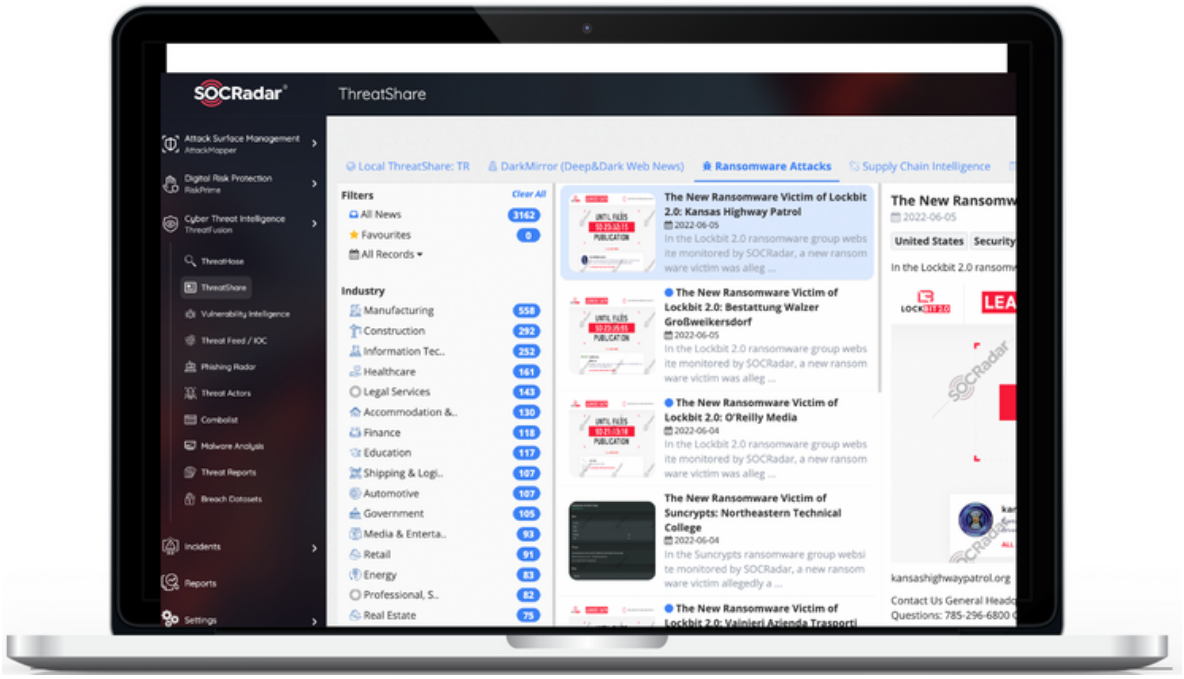
It allows you to prevent and quickly detect ransomware attacks by discovering & tracking your assets on the Internet:

- Creating and updating an online digital asset inventory,
- Critical port notification,
- 0-Day vulnerability detection.

SOCRadar RiskPrime Module

It enables the detection of intelligence information about your assets and your company:

- Creating alarms in possible situations by automatically tracking company domains in Dark and Deep web environments,
- Powerful phishing system
- Thanks to the HUMINT capability of SOCRadar dark web analysts, communication with the threat actor, confirmation of the accuracy of up-to-date information, and removal of the shared message to increase the company's reputation when necessary is possible.



How Can You Use SOCRadar for Early Detection of Ransomware Attacks?

SOCRadar ThreatFusion Module

It facilitates to collect of intelligence on current cyber events:

- Vulnerability tracking for internal/external systems and applications, Integration of IOCs used by threat actors into security devices,
- Making integrations to detect and block phishing domains used for phishing purposes by ransomware groups,
- Thanks to country-based and sector-based detections for ransomware attacks, sending actionable notifications and alarms to companies that may be affected by these attacks.
- Active monitoring of threat actors,
- Active informing of security personnel through ThreatShare about ransomware attacks
- Analyzing suspicious files with the Threat Analysis module