The Essential Guide to **Ransomware**

A brief history of ransomware attacks, major breaches and malware trends

splunk>

Table of Contents

Ransomware as a business **4**

The landscape — who are the players? **4**

Notable ransomware groups 5

Notable ransomware attacks 7

Common targets **7**

Infection vectors **8**

Cyber insurance, cryptocurrency and the rise of ransomware attacks **9**

Cyber insurance 9

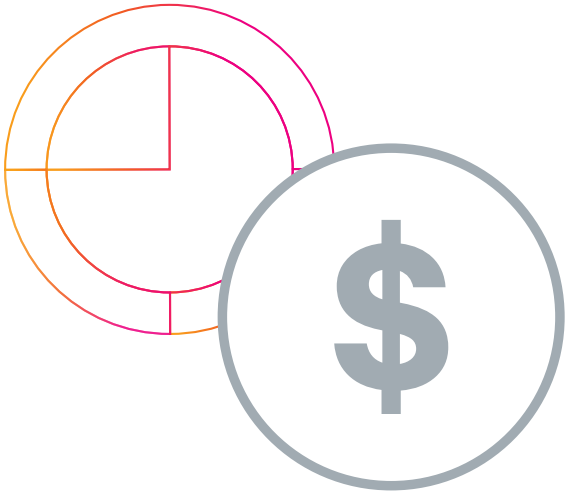
Cryptocurrency 9

Ransomware trends **10**

Ransomware's impact on business **11**

Ransomware's impact on the public sector **11**

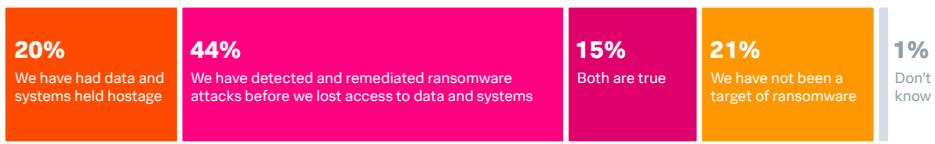
Data-centric security to combat ransomware 12



Ransomware is a growing problem for organizations of every size and kind, with the number of attacks and the money spent to clean up the damage on the rise. Ransomware isn't just a minor corporate issue anymore — it's regularly stealing headlines. In fact, 79% of 1,200 security leaders surveyed in Splunk's 2022 State of Security report say they've encountered ransomware attacks, and 35% admit one or more of those attacks led them to lose access to data and systems.

Most Orgs Were Ransomware Targets

79% fended off an attack ... or fell victim.



Source: State of Security 2022 | Splunk

But, we have to understand what ransomware is before we can understand how big the problem is. Ransomware is a type of malware that holds network data "hostage" by encrypting the data until a price is paid to unlock it.

And organizations paid a big price, according to the State of Security report, which found that the average price paid was about $347,000.

About 66% reported that the criminals were paid, either by the organization (in 39% of cases) or their insurance company (27%). Most security leaders surveyed that fell victim to a ransomware attack said they paid up. Only 33% avoided the ransom by restoring from backup. Ransomware attacks usually target vulnerabilities on endpoints, preying on organizations that aren't fully up to date with their security hygiene — security hygiene is the steps organizations take to keep sensitive data safe, organized and secure.

Basic examples of this in the real world are making sure patches and antivirus software are up to date. Security hygiene can be time-consuming and difficult to maintain, but it's these fundamentals that are the most important focus areas for enterprise organizations.

In this book, we'll explore the history and growth of ransomware, the threat actors behind the attacks, common tactics used to infiltrate an organization, some best practices to protect against an attack and more.

The evolution of ransomware

The different types of ransomware attacks have increased since 2014, with improved encryption capabilities and the growing adoption of cryptocurrency driving hackers. But the origins of ransomware attacks trace back further to the 1980s when malicious actors used floppy disks to install malware on unsuspecting victims.

Since then, ransomware attacks have grown more sophisticated and become easier to deliver — thanks, in part, to the internet. According to the Verizon Data Breach Investigation Report, ransomware attacks increased by 13% between 2020 and 2021, and in 2021 alone ransomware was responsible for $20 billion in damages. And that number is only going up. Ransomware is predicted to cost victims around $265 billion annually by 2031, according to another report.

Ransomware as a business

Depth of signal intelligence gathered from various domains—identity, email, data and cloud—provides insight into the gig economy that attackers have created with tools designed to lower the barrier for entry for other attackers who, in turn, continue to pay dividends and fund operations through the sale and associated “cut” from their tool’s success.

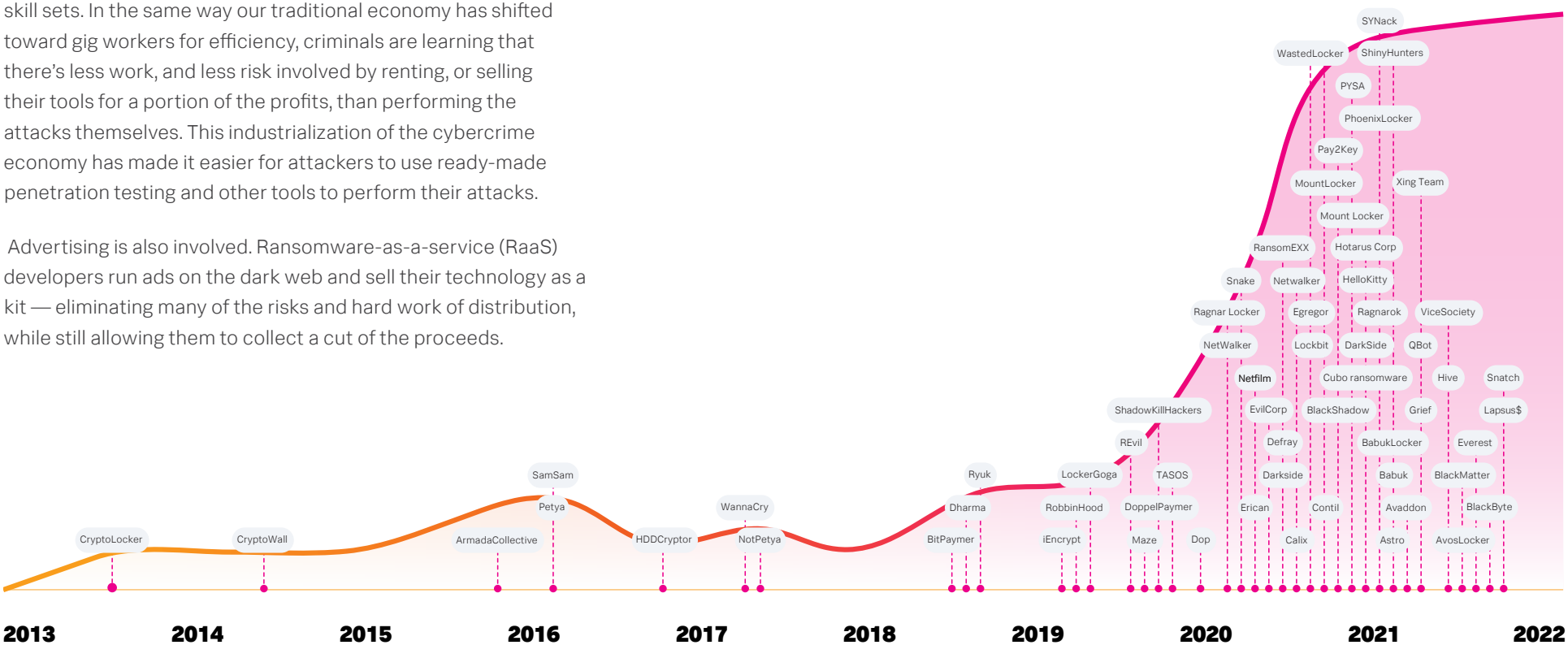
The cybercriminal economy is a continuously evolving connected ecosystem of many players with different techniques, goals and skill sets. In the same way our traditional economy has shifted toward gig workers for efficiency, criminals are learning that there’s less work, and less risk involved by renting, or selling their tools for a portion of the profits, than performing the attacks themselves. This industrialization of the cybercrime economy has made it easier for attackers to use ready-made penetration testing and other tools to perform their attacks.

Advertising is also involved. Ransomware-as-a-service (RaaS) developers run ads on the dark web and sell their technology as a kit — eliminating many of the risks and hard work of distribution, while still allowing them to collect a cut of the proceeds.

The landscape — who are the players?

It’s important to understand who has skin in the game when it comes to ransomware, and how they operate before you can prevent attacks. While there are many ransomware groups, a very small number of threat groups drive most of the malicious activity, which highlights the centralized nature of the ransomware landscape.

A tidal wave of ransomware continues to appear on the threat landscape. This image gives a glimpse into the rise of notable ransomware attacks since 2013.



The total estimated costs of these attacks is still largely unknown.

Notable ransomware groups

The three ransomware groups that laid claim to the highest numbers of successful attacks in the first quarter of 2022 were all widely known for operating under the RaaS model. Based on data from the leak sites of their operators, 35.8% of these attacks were attributed to hacker collectives known as LockBit, while 19% belonged to Conti and 9.6% to BlackCat.

1. **LockBit**

   Lockbit is a RaaS model that encrypts files stored locally and on network shares. LockBit can also identify additional systems on a network and propagate via server message block (SMB). Prior to encrypting files, LockBit clears event logs, deletes volume shadow copies and terminates processes and services that may impact its ability to encrypt files. LockBit has been seen using the file extension ".lockbit" for encrypted files. Mandiant researchers have seen LockBit used by more than 10 uncategorized threat groups with goals relating to financial gain and espionage.

2. **Conti**

   While Conti is considered a RaaS model ransomware variant, there is variation in its structure that differentiates it from a typical affiliate model. Conti developers likely pay the deployers of the ransomware a wage rather than a percentage of the proceeds used by affiliate hackers and receive a share of the proceeds from a successful attack.

   Conti actors often gain initial access to networks through spearphishing, stolen or weak remote desktop protocol (RDP) credentials, phone calls, fake software promoted via search engine optimization, other malware distribution networks and common vulnerabilities in external assets.

3. **BlackCat/ALPHV**

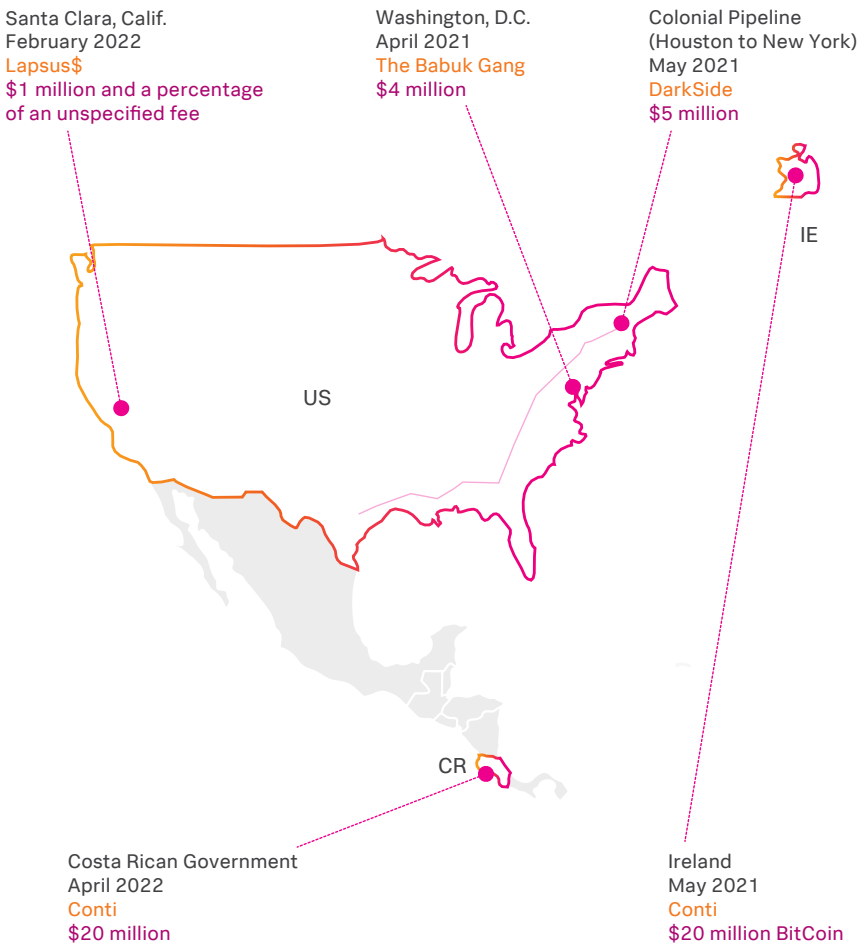
   BlackCat/ALPHV ransomware leverages previously compromised user credentials to gain initial access to the victim system. Once the malware establishes access, it compromises Active Directory user and administrator accounts. The malware uses Windows Task Scheduler to configure malicious group policy objects (GPOs) to deploy ransomware. Initial deployment of the malware leverages PowerShell scripts, along with Cobalt Strike, and disables security features within the victim's network. BlackCat/ALPHV ransomware also leverages Windows administrative tools and Microsoft Sysinternals tools during compromise.

While these remain the big ransomware players, there are several other groups doing damage, such as:

- **REvil**
  REvil is a ransomware-as-a-service criminal enterprise. REvil is said to be related to the criminal group known as GandCrab. In a RaaS scheme, malicious actors partner with affiliates to extend their botnets and reap profits from new additions and attacks brought to them by affiliates. The profit is shared with affiliates, which encourages them to infect more victims.
- **Hive**
  Hive ransomware likely operates as an affiliate-based ransomware and employs a wide variety of tactics, techniques, and procedures, creating significant challenges for defense and mitigation. Hive ransomware uses multiple mechanisms to compromise business networks, including phishing emails with malicious attachments, to gain access and remote desktop protocol (RDP) to move laterally once on the network. Hive ransomware hackers then exfiltrate data and encrypt files on the network. The threat actors leave a ransom note in each affected directory within a victim's system, which provides instructions on how to purchase the decryption software. The ransom note also threatens to leak exfiltrated victim data on the Tor site, "HiveLeaks".
- **Vice Society**
  Vice Society is a little-known double extortion group showing a steady activity encrypting and exfiltrating its victim's data and threatening victims to leak their information to pressure them into paying a ransom. Unlike other RaaS groups, Vice Society focuses on getting into the victim system to deploy ransomware binaries sold on dark web forums.
- **Black Basta**
  Black Basta steals corporate data and documents before encrypting a company's devices. This stolen data is then used in double-extortion attacks, where the threat actors demand a ransom to receive a decryptor and prevent the publishing of the victim's stolen data. The data extortion part of these attacks is conducted on the "Black Basta Blog" or "Basta News" Tor site, which contains a list of all victims who have not paid a ransom. Black Basta will slowly leak data for each victim to try and pressure them into paying a ransom.
- **Ryuk**
  Ryuk encrypts files stored on local drives and network shares. It also deletes backup files and volume shadow copies. Some Ryuk variants can propagate to other systems on a network. Mandiant has seen Ryuk used by FIN6, FIN12 and 10 financially motivated threat groups.
- **Lapsus$**
  Lapsus$ is known for using a pure extortion and destruction model without deploying ransomware payloads. Lapsus$ started targeting organizations in the United Kingdom and South America but expanded to global targets, including governments, technology, telecom, media, retail and healthcare sectors. Lapsus$ is also known to take over individual user accounts at cryptocurrency exchanges to drain cryptocurrency holdings.

Notable ransomware attacks

The following examples of ransomware attacks show the global scope and large costs of attacks, giving an idea of the damage that ransomware can do to companies and people.



Common targets

In 2021, 79% of organizations surveyed in the Splunk State of Security report who were targets of ransomware attacks, were more often than not hit by phishing email campaigns. This usually coincided with a pivot to targeted attacks and big game hunting, where attackers break in, survey a network, move laterally and delete backups before encryption.

In 2021, cybercriminals increasingly targeted government agencies, municipalities, schools, critical infrastructure, hospitals and healthcare providers, either directly or through managed service providers (MSPs). Ransomware operators furthered their strong-arm schemes by compromising mission-critical systems, intimidating organizations and demanding hefty payments.

Not paying ransom often means replacing equipment and starting over, leaving leadership facing difficult business and mission-critical decisions and angry shareholders or citizens. Targeted organizations often believe that paying the ransom is the most cost-effective way to get their data back. This may be the reality, but it directly funds the development of the next generation of ransomware.

Infection vectors

Although ransomware has been around for decades, creators are getting more sophisticated in how they infect systems, avoid detection and foil decryption efforts. To better protect against ransomware attacks, it's important to understand how ransomware can enter a system.

1. **Email**

   Email is a popular cyber weapon because it can exploit users by creating a sense of urgency and legitimacy to perform various actions. It's not surprising that it continues to be the most common vector for attack, with attachments disguised as innocuous files or links to a software download. Once clicked it leads to the ransomware infection.

2. **Drive-by download**

   The ransomware infection is caused by visiting a compromised website, usually with an old browser, software plug-in or unpatched third-party application. The infected website runs an exploit kit that looks for unpatched vulnerabilities.

3. **Remote desktop protocol (RDP)**

   Internet-exposed RDP sessions are common means of infecting computers. Ideally, such sessions are used to remotely log in to Windows' computers and allow the user to securely control the computer. Unfortunately, hackers have become skilled at brute force attacking these exposed computers. In compromising RDP vulnerabilities, hackers use both brute force methods and credentials purchased on dark web marketplaces.

4. **Public facing vulnerable services or servers**

   Adversaries may attempt to take advantage of a weakness in an internet-facing computer or program using software, data or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch or a design vulnerability. These applications are often websites, but can include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install) and any other applications with internet accessible open sockets, such as web servers and related services.

Cyber insurance, cryptocurrency and the rise of ransomware attacks

The last few years have seen a shift in ransomware targets, notably to those with cyber insurance and those using cryptocurrencies. While having cyber insurance may seem like a good idea, understanding your policy and how insurers would handle an attack is imperative to securing an organization's network, while not adding money to the pot of ransomware groups. Additionally, the growing prevalence of cryptocurrency has created a marked uptick in the frequency, sophistication and destructiveness of ransomware attacks.

Cyber insurance

Risk management specialists are blaming cyber insurance companies for the marked increase in ransomware attacks in both the private and public sectors. While law enforcement warns that organizations should never pay ransom demands, there is increasing evidence that the system of cyber insurance is exacerbating the problem, enabling criminal activity and emboldening ransomware crime groups.

Insurance companies are incentivized to pay the ransom, and are nudging organizations to meet the ransom demands because it's less expensive, faster and easier to pay the ransom than cover the cost of rebooting a company from the ground up. Because hackers are aware of this mindset, they target firms that have cyber insurance and conduct reconnaissance to determine the size of the policy and how likely it is that the organization will pay — setting the ransom slightly below the cost. While insurance firms provide negotiation services and support recovery from a ransomware attack, the bottom line is that firms with cyber insurance are more prone than others to pay the ransom.

However, we may be seeing a shift on the part of insurers. Insurers may have been willing to foot the cost of ransomware ransoms a few years ago when they were in the three and four digits, but the prevalence of multi-million-dollar ransoms has changed the game completely — and in recent months, the insurance industry has thrown down its cards.

Surging ransomware losses pushed premiums for cyber insurance policies up by 92 percent during 2021, according to recent reports, while a recent industry audit by the Council of Insurance Agents & Brokers (CIAB) noted that cyber premiums surged by 34.3 percent during the fourth quarter of 2021 alone — the largest quarterly increase in premiums since 9/11.

Insurers are increasingly declining coverage, unless companies can demonstrate that they are running effective security training and have implemented key security protections, such as multi-factor authentication (MFA) — which, although it can be compromised in extreme circumstances, it nonetheless offers better protection than passwords alone.

Cryptocurrency

Payment methods were limited in the early days of ransomware. The odd hacker could deliver a message to send money via Western Union or to a bank account, but the transfer was traceable once the authorities became involved. Then came Bitcoin.

Bitcoin is a secure and untraceable method of making and receiving payments. It's more flexible than traditional payment methods, which require specific financial or login details to use. By operating as a decentralized currency, in which people anywhere in the world pay each other without a middleman, oversight or regulation, it provides an acceptable level of anonymity.

While bitcoin is the best-known cryptocurrency, industry analysts are taking note of Monero, which is being heavily used on dark web marketplaces and is becoming a new payment method of choice for ransomware demands because of its privacy features. The potential for cryptocurrency to enable ever bigger cybercrime is hard to assess, but extortion attempts taking place are now skyrocketing.

Ransomware trends

Ransomware creators are getting more sophisticated in how they infect systems, avoid detection and foil decryption efforts. Ransomware trends include:

- **Blended campaigns**
  Nation-state threat actors are blending cryptocurrency mining and ransomware campaigns to generate revenue and/or distract from other threat campaigns.
- **Big game hunting**
  Spray and pray methods are being replaced by big game hunting, where one big target, such as a hospital or large corporation, gets hit for a big payout. Ransomware is being custom-built for a target to cause the most damage and demand higher ransoms.
- **Intelligence gathering**
  Ransomware crime groups gather intelligence on intended victims. In addition to penetrating the network and performing reconnaissance, threat actors study SEC filings for an organization's financial position and use the information to scale ransom demands.
- **Increased stealthiness**
  Strategies to get below the level of detection include:
  - Randomizing the process instead of encrypting in a linear fashion.
  - Delayed execution to bypass traditional defenses.
  - Using polymorphic code that changes.
  - Deploying multi-tzhreaded attacks that launch child processes.
- **Increased impact**
  Strategies to both increase the impact and thwart recovery include:
  - Encrypting the hard drive and master boot record.
  - Attacking shared network drives.
  - Attacking files stored in infrastructure-as-a-service.
  - Deleting Windows shadow copies and any files with backup extensions.
  - Targeting high-value assets like web servers, applications servers and collaboration tools.
- **Attacks on managed service providers (MSPs)**
  Managed service providers are a growing target for ransomware attackers. An attack on an MSP has the potential to devastate virtually any organization. By exploiting vulnerable security systems typically seen in resource-constrained service providers that manage multiple businesses and municipalities, attackers can get economies of scale and exert pressure for payment.
- **Attacks on cloud services providers**
  Ransomware writers are now targeting cloud service providers with network file encryption attacks as a way to hold hostage the maximum number of customers possible. The fallout from ransomware attacks against cloud service providers is devastating because the business systems of every cloud-hosted customer are encrypted.
- **Wiperware**
  Ransomware is being used as a foil to cover up serious incidents, such as data breaches. Although the attack looks like regular ransomware, typically delivered through phishing emails, the goal is to distract the organization from other security events happening on the network and delete breadcrumbs of the ancillary attack. The hope of the attacker is that the organization is so relieved to have recovered from ransomware that it doesn't investigate further.
- **Oldies but goodies**
  Ransomware continues to exploit older vulnerabilities and those with lower security scores. Research has found that vulnerabilities as far back as 2010 are still trending. One such example is Log4j, which was developed over 20 years ago. This logging framework is deployed on hundreds of millions of systems around the world. The zero-day vulnerability was one of the most critical of the last decade and, unfortunately, it's not likely to be the last. It's time to take stock in the long-term implications for what this vulnerability and others in the future mean for security leaders. Organizations that use CVSS scores as an exclusive way to prioritize patching vulnerabilities for patching will likely miss vulnerabilities being used by ransomware.
- **Double extortion**
  As discussed earlier, ransomware attacks have taken an unwelcome turn as ransomware attackers have started to leak the victim's files as a way to exert additional pressure to pay the ransom. With such an escalated attack, victims now need to be concerned both about recovering their encrypted files and what would happen if their stolen unencrypted files were leaked to the public.

Ransomware's impact on business

Ransomware drains billions from the global economy and shows no signs of slowing down. Beyond the ransom itself, the greatest cost is the financial damage that consists of downtime, lost data, tarnished reputations, system rebuild and recovery costs and regulatory fines. Sadly, the impact to businesses continues to mount:

- Ransoms in excess of $50,000 to $400,000 are no longer uncommon. Depending on the target, ransom demands have reached into the millions. Cybersecurity Ventures predicts that ransomware will cost its victims around $265 billion (USD) annually by 2031.

Ransomware's impact on the public sector

The rise of ransomware has been particularly hard in the public sector across the globe as attacks against government agencies, municipalities and schools have increased. This only got worse during the pandemic, which caused the U.S. government to release a memo on best best practices to protect against a ransomware attack. President Biden took it one step further by issuing an executive order on improving the nation's cybersecurity. The EO outlined five best practices for protecting against ransomware, including:

- Implementing multi-factor authentication (MFA).
- Implementing endpoint detection and response in support of proactive detection, cyber hunting, containment, remediation and incident response.
- Encrypting your data.
- Employing a skilled and empowered security team.
- Sharing and incorporating threat intelligence.

The U.S. government is only one example of global government agencies concerned with ransomware. In fact, governments worldwide saw a 1,885% increase in ransomware attacks, and the healthcare industry faced a 755% increase in those attacks in 2021, according to the 2022 Cyber Threat Report.

Data-centric security to combat ransomware

Fortunately, while organizations should be wary of ransomware threats, they don't have to be scared of them. This type of malware can often be prevented. For instance, keeping track of suspicious network traffic with endpoint detection-and-response systems that block a hash and prevent new processes from spawning from nefarious executables, or detecting any domains associated with known ransomware are two options. Automating security responses according to well-known ransomware variants and behaviors is another route.

But what if you're too late in catching the ransomware attack?

Management and executive boards must consider in what circumstances they would or would not pay a ransom, and then set processes for decision-making and launching an investigation. A policy and communications strategy guided by legal, business and mission factors will reduce stress and allow for an informed response.

Here are additional tips from experts on how to prepare for and defend against ransomware attacks:

- Create a policy on how you'll handle ransomware incidents.
- Build your intelligence ecosystem by collaborating with sharing communities.
- Shore up your fundamentals by ensuring you have strong people, process and technology stack for detection and response.
- Recognizing that threat actors are attacking the cloud, ensure you have full visibility over cloud services.
- Keep all software up to date, including operating systems and applications, as well as clear inventories of all digital assets and their locations.
- Identify valuable data and segment the network. Avoid putting all data on one file share accessible by everyone in the company.
- Perform daily backups, including data on employee devices. Consider online, local and secure offsite locations.
- Perform penetration testing to find and patch vulnerabilities, ensure remote desktop protocol ports can't be accessed by default credentials, and maintain good security hygiene.
- Train staff on security practices, emphasizing the importance of not opening attachments or links from unknown sources.
- Endpoint security software will block many attempts at infection through email, but securing the endpoint is no longer sufficient. Employ a multi-layered threat defense solution.
- Create an isolation plan to remove infected systems from the network.
- In mitigating an attack, perform research to see if similar malware has been investigated by other IT teams and if it is possible to decrypt the data on your own.

Get ahead of attacks with security content from the Splunk Threat Research Team and Splunk SURGe, your trusted advisor for timely security research and guidance.

Also try the Splunk Online Demo Experience—Endpoint where you can use sample data to safely practice security investigation techniques. Also try the Online Demo for Splunk Security Essentials to get started addressing different malware use cases and understand how to build a strong security portfolio.

splunk>

22-25821-Splunk-Essential Guide to Ransomware_SS-106