

## STATE OF RANSOMWARE 2023

Over the course of last year, ransomware showed no signs of slowing down. Faced with federal level sanctions, the act of rebranding is now a widespread strategy ransomware groups use to obfuscate their identities and sidestep crackdowns. Several new ransomware groups emerged in 2022 and existing ones rebranded before showing their faces in the threat landscape once more.

- Quantum ransomware operation became Dagon Locker
- Notorious cybergang Conti siphoned their brand into smaller groups including Hive, BlackCat, and HelloKitty
- DarkSide transitioned into BlackMatter, followed by further splinters including AlphV.
- DoppelPaymer rebranded into Grief
- Rook ransomware transitioned into Pandora

Ransomware tactics and techniques continued to evolve, which demonstrates ransomware threat actors' growing technological sophistication and an increased ransomware threat to organizations globally. Cybersecurity authorities [1] in the United States observed the following behaviors and trends among cyber criminals in past couple of years:

- **Gaining access to networks** via phishing, stolen Remote Desktop Protocols (RDP) credentials or brute force, and exploiting vulnerabilities. Phishing emails, RDP exploitation, and exploitation of software vulnerabilities remained the top three initial infection vectors for ransomware incidents in 2021 and 2022. Once a ransomware threat actor has gained code execution on a device or network access, they can deploy ransomware. Note: these infection vectors likely remain popular because of the increased use of remote work and schooling which started during the pandemic. This increase expanded the remote attack surface and left network defenders struggling to keep pace with routine software patching.
- **Using cybercriminal services-for-hire.** The market for ransomware became increasingly "professional" and the criminal business model of ransomware is now well established. In addition to their increased use of ransomware-as-a-service (RaaS), ransomware threat actors employed independent services to negotiate payments, assist victims with making payments, and arbitrate payment disputes between themselves and other cyber criminals.
- **Sharing victim information.** Eurasian ransomware groups have shared victim information with each other, diversifying the threat to targeted organizations. For example, after announcing its shutdown, the BlackMatter ransomware group transferred its existing victims to infrastructure owned by another group, known as Lockbit 2.0. In October 2021, Conti ransomware actors began selling access to victims' networks, enabling follow-on attacks by other cyber threat actors.
- **Shifting away from "big-game" hunting in the United States.** In the first half of 2021, cybersecurity authorities in the United States observed ransomware threat actors targeting "big game" organizations—i.e., perceived high-value organizations and/or those that provide critical services—in several high-profile

incidents. These victims included Colonial Pipeline Company, JBS Foods, and Kaseya Limited. Overall victims included businesses, charities, the legal profession, and public services in the Education, Local Government, and Health Sectors.

- **Diversifying approaches to extorting money.** After encrypting victim networks, ransomware threat actors increasingly used “triple extortion” by threatening to (1) publicly release stolen sensitive information, (2) disrupt the victim’s internet access, and/or (3) inform the victim’s partners, shareholders, or suppliers about the incident.

Ransomware groups have increased their impact by:

- **Targeting the cloud.** Ransomware developers targeted cloud infrastructures to exploit known vulnerabilities in cloud applications, virtual machine software, and virtual machine orchestration software. Ransomware threat actors also targeted cloud accounts, cloud application programming interfaces (APIs), and data backup and storage systems to deny access to cloud resources and encrypt data. In addition to exploiting weaknesses to gain direct access, threat actors sometimes reach cloud storage systems by compromising local (on-premises) devices and moving laterally to the cloud systems. Ransomware threat actors have also targeted cloud service providers to encrypt large amounts of customer data.
- **Targeting managed service providers.** Ransomware threat actors have targeted managed service providers (MSPs). MSPs have widespread and trusted accesses into client organizations. By compromising an MSP, a ransomware threat actor could access multiple victims through one initial compromise. Cybersecurity authorities in the United States, Australia, and the United Kingdom assess there will be an increase in ransomware incidents where threat actors target MSPs to reach their clients.
- **Attacking industrial processes.** Although most ransomware incidents against critical infrastructure affect business information and technology systems, the FBI observed that several ransomware groups have developed code designed to stop critical infrastructure or industrial processes.
- **Attacking the software supply chain.** Globally, ransomware threat actors targeted software supply chain entities to subsequently compromise and extort their customers. Targeting software supply chains allows ransomware threat actors to increase the scale of their attacks by accessing multiple victims through a single initial compromise.

## Key takeaways from 2022

2022 saw a steep increase in supply chain attacks [8], SEO poisoning/malvertising [9], and cracked software. The growing theme in attacks from last year saw threat actors steering towards the path of least resistance for greater rewards.

Through software supply chain attacks, actors exploit weaknesses in a vendor's development cycle to inject malicious code into a certified application. While many organizations have worked to monitor and detect such threats since the attack on SolarWinds in 2020, threat actors are still leveraging open-source modules for initial intrusion. Identity management giant, Okta for example, found themselves the target of a supply chain attack last year when its 2FA provider, Twilio, was breached.

SEO poisoning has also risen to the top as a way for threat actors to take advantage of existing infrastructure for malicious purposes. By poisoning the mechanisms that influence search engine optimization (SEO), attackers have been able to quickly lure and infect unsuspecting users with commodity malware. Cracked software follows the same theme, banking on victims to download unlocked, illegal software which is embedded with dangerous malware.

Attackers were observed attempting to neutralize and sidestep endpoint detection and response (EDR) tools over the past year, using bypass techniques and known vulnerabilities. In February 2022, the FBI and United States Secret Service (USSS) released a joint cybersecurity advisory [4] warning against BlackByte; a ransomware group known for using a "Bring Your Own Driver" technique to circumvent various EDR products available on the market today.

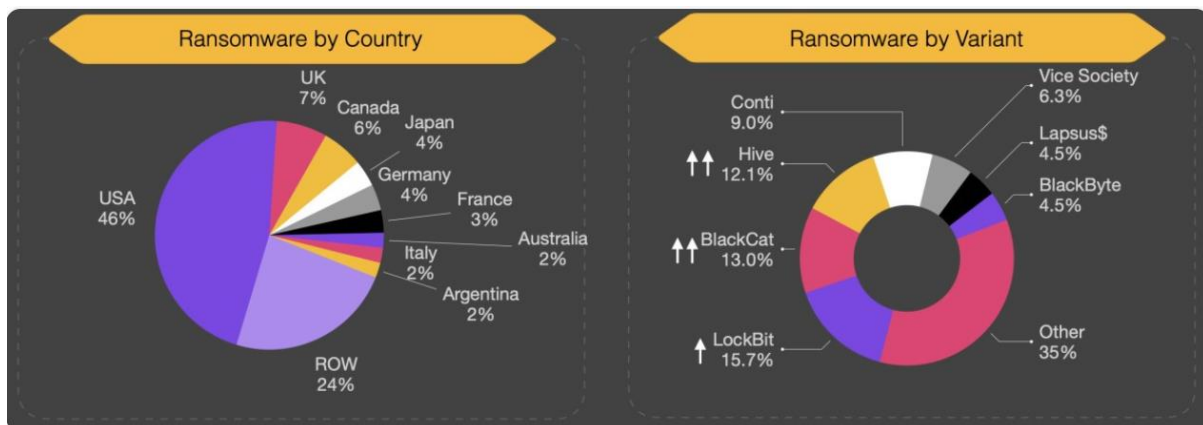
The most notable commodity tooling observed in 2022 by threat tactic as published by SentinelOne [5] are as follows:

- Lateral Movement – Psexec, PDQ Install, Winrm, SMB, WMI, RDP, SSH
- Remote Access – TeamViewer, AnyDesk, Splashtop, ZohoAssist, ConnectWise, VNC, BeyondTrust, GoToAssist, RemotePC, TightVNC, RDP(mstsc), Registry terminal server enable
- Defense Evasion – Gmer, Icesword, Regedit (reg.exe), Process Hacker driver, Powershell, WMI, Service Kill (bat file), Process Kill (bat file)
- Staging – SCCM, Group Policy, Psexec, Powershell Remote, ConnectWise
- Data Exfiltration – RClone, FileZilla, Winscp, cloud services such as MegaSync and megacloud)

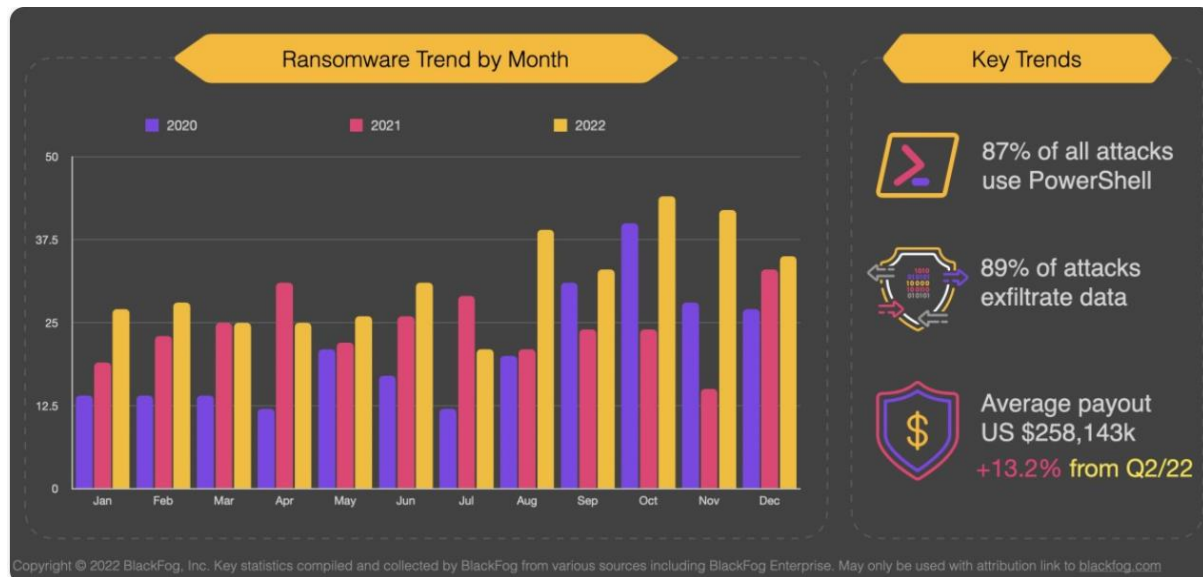
Ransomware authors have also widely adopted both Rust and Golang in their efforts to evade detection. BlackCat, Hive, and a host of other ransomware families also made the switch, taking advantage of their fast file encryption capabilities and wide-ranging cryptographic libraries.

## Important Statistics

Following are some analysis done by Blackfog[2] taking into account all the publicly disclosed attacks in 2022 and grouped based on country and variant. As seen below, the landscape on ransomware variants changed significantly during 2022 with LockBit clearly dominating successful attacks, with 16% of all attacks, followed by BlackCat at 13%, Hive at 12.1% and Conti 9.0%. Most notable is the sheer increase in attacks over 2021. LockBit was hardly even mentioned in 2021 yet saw a 600% increase in 2022. Similarly, BlackCat and Hive were virtually unheard of, but they rounded out 2022 as the second and third most successful variants.



Following statistics show the ransomware trend by month in the past 3 years.



In 2022 we recorded a total of 376 attacks, a 29% increase over 2021 and 34% increase from 2020. Key take aways from these overall numbers is that 89% of all attacks now involve data exfiltration, 9% more than in 2021. From a tactical point of view, we also saw an increase in the use of PowerShell, now at 87% of all attacks, a 7% increase from 2021. While the Dark Web was used in 23% of all attacks, a dramatic increase from 5% in 2021.

## Hive Case Study

First observed in June 2021, Hive is an affiliate-based ransomware variant used by cybercriminals to conduct ransomware attacks against healthcare facilities, non-profits, retailers, energy providers, and other sectors worldwide. Hive is built for distribution in a Ransomware-as-a-service model that enables affiliates to utilize it as desired.

Hive ransomware actors have victimized over 1,300 companies worldwide, receiving approximately US\$100 million in ransom payments, according to FBI information. Hive ransomware follows the ransomware-as-a-service (RaaS) model in which developers create, maintain, and update the malware, and affiliates conduct the ransomware attacks. From June 2021 through at least November 2022, threat actors have used Hive ransomware to target a wide range of businesses and critical infrastructure sectors, including Government Facilities, Communications, Critical Manufacturing, Information Technology, and especially Healthcare and Public Health (HPH).

The variant uses common ransomware tactics, techniques, and procedures (TTPs) to compromise victims' devices [6]. While taking live actions, the operator disables anti-malware protections and then exfiltrates sensitive data and encrypts business files. Their affiliates use multiple mechanisms to compromise their victims' networks, including phishing emails with malicious attachments, leaked VPN credentials, and by exploiting vulnerabilities on external-facing assets. In addition, Hive places a plain-text ransom note that threatens to publish the victim's data on the TOR website 'HiveLeaks' unless the victim meets the attacker's conditions.

The joint FBI-CISA-HHS advisory warns that Hive typically gains access to victim networks by using stolen single-factor credentials to access organizations' remote desktop systems, virtual private networks and other internet-facing systems. But CISA also warns that the ransomware group also skirts some multi-factor authentication systems by exploiting unpatched vulnerabilities.

### Initial Access

The method of initial intrusion will depend on which affiliate targets the network. Hive actors have gained initial access to victim networks by using single factor logins via Remote Desktop Protocol (RDP), virtual private networks (VPNs), and other remote network connection protocols [T1133] [7]. In some cases, Hive actors have bypassed multifactor authentication (MFA) and gained access to FortiOS servers by exploiting Common Vulnerabilities and Exposures (CVE) [CVE-2020-12812](#). This vulnerability enables a malicious cyber actor to log in without a prompt for the user's second authentication factor (FortiToken) when the actor changes the case of the username.

Hive actors have also gained initial access to victim networks by distributing phishing emails with malicious attachments [T1566.001] and by exploiting the following vulnerabilities against Microsoft Exchange servers [T1190]:

- [CVE-2021-31207](#) - Microsoft Exchange Server Security Feature Bypass Vulnerability
- [CVE-2021-34473](#) - Microsoft Exchange Server Remote Code Execution Vulnerability

- [CVE-2021-34523](#) - Microsoft Exchange Server Privilege Escalation Vulnerability.

### **Execution**

Hive actors look to stop the volume shadow copy services and remove all existing shadow copies via vssadmin on command line or PowerShell [\[T1059\]](#).

### **Defense Evasion**

After gaining access, Hive ransomware attempts to evade detention by executing processes to:

- Identify processes related to backups, antivirus/anti-spyware, and file copying and then terminating those processes to facilitate file encryption [\[T1562\]](#).
- Stop the volume shadow copy services and remove all existing shadow copies via vssadmin on command line or via PowerShell [\[T1059\]](#) [\[T1490\]](#).
- Delete Windows event logs, specifically the System, Security and Application logs [\[T1070\]](#).

### **Persistence**

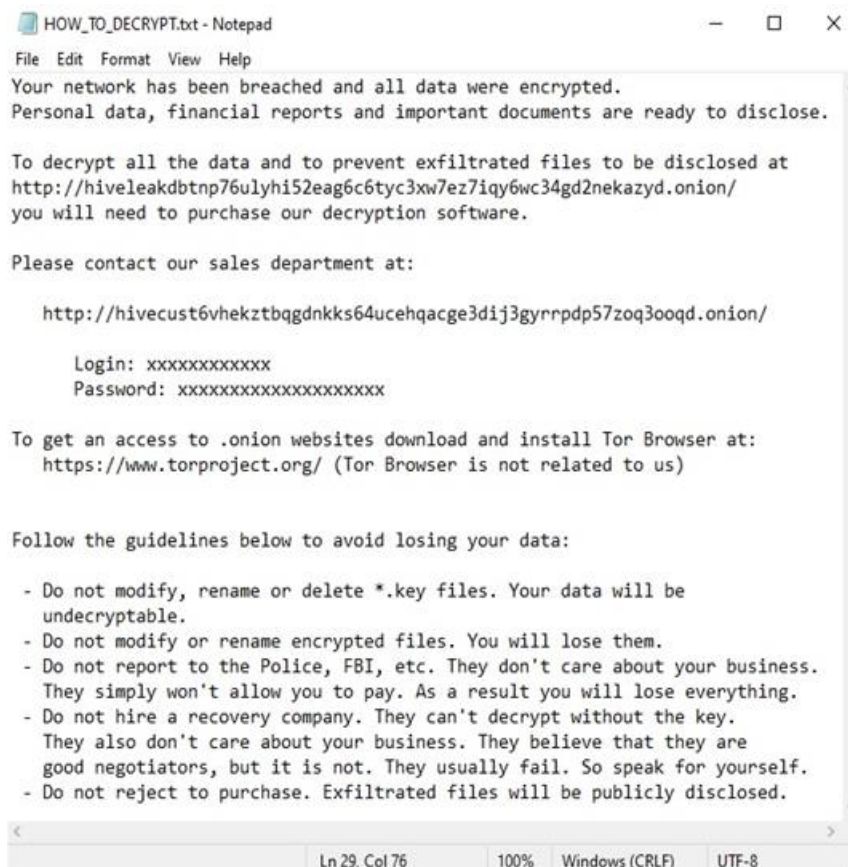
Prior to encryption, Hive ransomware removes virus definitions and disables all portions of Windows Defender and other common antivirus programs in the system registry [\[T1112\]](#).

### **Data Exfiltration**

Hive actors exfiltrate data likely using a combination of Rclone and the cloud storage service Mega.nz [\[T1537\]](#). In addition to its capabilities against the Microsoft Windows operating system, Hive ransomware has known variants for Linux, VMware ESXi, and FreeBSD.

### **Impact**

During the encryption process, a file named \*.key is created in the root directory (C:\ or /root/). Required for decryption, this key file only exists on the machine where it was created and cannot be reproduced. The ransom note, HOW\_TO\_DECRYPT.txt is dropped into each affected directory and states the \*.key file cannot be modified, renamed, or deleted, otherwise the encrypted files cannot be recovered [\[T1486\]](#). The ransom note contains a “sales department” .onion link accessible through a TOR browser, enabling victim organizations to contact the actors through a live chat panel to discuss payment for their files. However, some victims reported receiving phone calls or emails from Hive actors directly to discuss payment. The ransom note also threatens victims that a public disclosure or leak site accessible on the TOR site, “HiveLeaks”, contains data exfiltrated from victim organizations who do not pay the ransom demand. Sample ransom note is shown below:



```
HOW_TO_DECRYPT.txt - Notepad
File Edit Format View Help
Your network has been breached and all data were encrypted.
Personal data, financial reports and important documents are ready to disclose.

To decrypt all the data and to prevent exfiltrated files to be disclosed at
http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion/
you will need to purchase our decryption software.

Please contact our sales department at:

http://hivecust6vhkztbqgdnkks64ucehqacge3dij3gyrrpdp57zoq3ooqd.onion/

Login: xxxxxxxxxxxx
Password: xxxxxxxxxxxxxxxxxxxxxx

To get an access to .onion websites download and install Tor Browser at:
https://www.torproject.org/ (Tor Browser is not related to us)

Follow the guidelines below to avoid losing your data:

- Do not modify, rename or delete *.key files. Your data will be
  undecryptable.
- Do not modify or rename encrypted files. You will lose them.
- Do not report to the Police, FBI, etc. They don't care about your business.
  They simply won't allow you to pay. As a result you will lose everything.
- Do not hire a recovery company. They can't decrypt without the key.
  They also don't care about your business. They believe that they are
  good negotiators, but it is not. They usually fail. So speak for yourself.
- Do not reject to purchase. Exfiltrated files will be publicly disclosed.
```

Additionally, Hive actors have used anonymous file sharing sites (mentioned below) to disclose exfiltrated data.

[https://anonfiles\[.\]com](https://anonfiles[.]com)

[https://mega\[.\]nz](https://mega[.]nz)

[https://send.exploit\[.\]in](https://send.exploit[.]in)

[https://ufile\[.\]io](https://ufile[.]io)

[https://www.sendspace\[.\]com](https://www.sendspace[.]com)

[https://privatlab\[.\]net](https://privatlab[.]net)

[https://privatlab\[.\]com](https://privatlab[.]com)

Once the victim organization contacts Hive actors on the live chat panel, Hive actors communicate the ransom amount and the payment deadline. Hive actors negotiate ransom demands in U.S. dollars, with initial amounts ranging from several thousand to millions of dollars. Hive actors demand payment in Bitcoin.

Hive actors have been known to reinfect—with either Hive ransomware or another ransomware variant—the networks of victim organizations who have restored their network without making a ransom payment.

Hive was initially written in Go to take advantage of the language's concurrency features to encrypt files faster. Go malware is usually considered difficult to reverse engineer, primarily due to the wealth of tangentially related imported code baked into every executable. It's important to isolate the code contributed by the malware developers. However, Microsoft's Threat Intelligence Center (MSTIC) researchers warned [10] that Hive had upgraded its malware by migrating its code from Go to the Rust programming language, enabling it to use a more complex encryption method for its ransomware as a service payload. Hive isn't the first ransomware written in Rust—BlackCat, another prevalent ransomware, was the first. By switching the underlying code to Rust, Hive benefits from the following advantages that Rust has over other programming languages:

1. It offers memory, data type, and thread safety
2. It has deep control over low-level resources
3. It has a user-friendly syntax
4. It has several mechanisms for concurrency and parallelism, thus enabling fast and safe file encryption
5. It has a good variety of cryptographic libraries
6. It's relatively more difficult to reverse-engineer

The new Hive variant uses string encryption that can make it more evasive. Strings reside in the .rdata section and are decrypted during runtime by XORing with constants. The constants that are used to decrypt the same string sometimes differ across samples, making them an unreliable basis for detection.

The most interesting change in the Hive variant is its cryptography mechanism. The new variant was first uploaded to VirusTotal on February 21, 2022, just a few days after a group of researchers from Kookmin University in South Korea published the paper "A Method for Decrypting Data Infected with Hive Ransomware" on February 17, 2022. After a certain period of development, the new variant first appeared in Microsoft threat data on February 22.

The new variant uses a different set of algorithms: Elliptic Curve Diffie-Hellmann (ECDH) with Curve25519 and XChaCha20-Poly1305 (authenticated encryption with ChaCha20 symmetric cipher).



## **Lessons learnt**

Organizations are getting better at restoring data after an attack. As ransomware has become more prevalent, organizations have got better at dealing with the aftermath of an attack. Backups are the #1 method used to restore data, many organizations use multiple restoration approaches to maximize the speed and efficacy with which they can get back up and running.

The ransom sums are just part of the story, and the impact of ransomware ranges much more widely than just the encrypted databases and devices. 90% of those hit by ransomware in the last year said the most significant attack impacted their ability to operate. Furthermore, among private sector organizations, 86% said it caused them to lose business/revenue.

It has become increasingly easy for cybercriminals to deploy ransomware, with almost everything available as-a-service. Many organizations rely on cyber insurance to help them recover from a ransomware attack – 83% of mid-sized organizations had cyber insurance that covers them in the event of a ransomware attack. Cyber insurance providers have covered a wide range of ransomware recovery costs, including the ransom, likely contributing to ever higher ransom demands. As per a study done by Sophos [3], Cyber insurance almost always pays out – In 98% of incidents where the victim had cyber insurance that covered ransomware, the insurer paid some or all the costs incurred (with 40% overall covering the ransom payment). The study has revealed an ever more challenging attack environment together with the growing financial and operational burden ransomware places on its victims. It also shines new light on the relationship between ransomware and cyber insurance, and the role insurance is playing in driving changes to cyber defenses. 94% of those with cyber insurance said that their experience of getting it has changed over the last 12 months, with higher demands for cybersecurity measures, more complex or expensive policies and fewer organizations offering insurance protection. However, the results indicate that cyber insurance is getting tougher and in the future ransomware victims may become less willing or less able to pay sky high ransoms. Sadly, this is unlikely to reduce the overall risk of a ransomware attack.

## Conclusion

Ransomware attacks have become even more impactful in recent years as more ransomware as a service ecosystem have adopted the double extortion monetization strategy. All ransomware is a form of extortion, but now, attackers are not only encrypting data on compromised devices but also exfiltrating it and then posting or threatening to post it publicly to pressure the targets into paying the ransom. Most ransomware attackers opportunistically deploy ransomware to whatever network they get access to, and some even purchase access to networks from other cybercriminals. Some attackers prioritize organizations with higher revenues, while others prefer specific industries for the shock value or type of data they can exfiltrate. 2022 showed that threat actors continue to use what works while investing in novel techniques in response to countermeasures by security teams and security software.

Identifying and sharing trends in new vulnerabilities, attack vectors, and malware strains are key to staying steps ahead of cyber attackers. Though new threats will undoubtedly continue to emerge, there are many ways enterprises can mitigate risk and harden their defenses. The more information that is shared about past, current, and emerging threat actors, the better enterprises can implement the processes and technology needed to combat ransomware challenges.

Threat actors will continue to upgrade their methods and tools of attack, innovating on attack vectors and finding new vulnerabilities. Although detecting and responding to such incidents can be challenging, most malicious activities can be prevented by having the right security tools, incident response plans, and patches for known vulnerabilities in place.

## References:

- [1] [United States Cybersecurity and Infrastructure Security Agency](#)
  - [2] "The State of Ransomware in 2022" published in BlackFog
  - [3] "The State of Ransomware 2022" published in Sophos by Sally Adam on April 27, 2022
  - [4] <https://www.ic3.gov/Media/News/2022/220211.pdf>
  - [5] "WatchTower | Trends and Top Cybersecurity" January 26, 2023 by SentinelOne.
  - [6] [Stopransomware.gov](#) is a whole-of-government approach that gives one central location for ransomware resources and alerts.
  - [7] See [MITRE ATT&CK for Enterprise](#) for all referenced tactics and techniques.
  - [8] "Defending the Enterprise Against Digital Supply Chain Risk in 2022" April 25, 2022, by Chris Boehm in SentinelOne.
  - [9] "Breaking Down the SEO Poisoning Attack | How Attackers Are Hijacking Search Results" January 19, 2023, by Tom Hegel in SentinelOne.
  - [10] "Hive ransomware gets upgrades in Rust" by Microsoft on July 5, 2022.
- "Hive ransomware actors have extorted over \$100M from victims, says FBI" published in TechCrunch by Carly Page on November 18, 2022.
- "Hive Attacks | Analysis of the Human-Operated Ransomware Targeting Healthcare" by Jim Walter Sentinel Labs on Aug 23, 2021.