



# **Outsmart Ransomware with Security Controls Validation**



# Table of Contents

<b>01  </b> Abstract .....	2
<b>02  </b> Introduction .....	3
<b>03  </b> The Five Basic Steps of a Ransomware Attacks .....	3
<b>04  </b> Who Are Ransomware Attacks Prime Targets? .....	4
<b>05  </b> Ransomware Typology – The Seven Types of Ransomware .....	4
<b>06  </b> Why Are Ransomware Attacks So Effective? .....	5
<b>07  </b> Why Are Ransomware Attacks So Devastating? .....	6
<b>08  </b> Basic Hygiene to Minimize Ransomware Damage .....	7
<b>09  </b> Proactive Ways to Prevent Damages From Ransomware Attacks .....	8
<b>10  </b> Appendix A: Breakdown of Cymulate's XSPM Integrated Solutions .....	11
• Attack Surface Management (ASM) .....	11
• Red Teaming Campaigns .....	11
• Breach Attack Simulation (BAS) .....	11
• Advanced Purple Teaming .....	11
• Attack-Based Vulnerability Management (ABVM) .....	12
<b>11  </b> Appendix B – Sources .....	13

## 01 | Abstract

Ransomware attacks doubled in frequency in 2021, and the 2021-2022 trend confirms that attackers are focusing on the approaches yielding the best results. As forewarned is forearmed, the first step to avoid falling prey to ransomware attackers is to understand their goals and techniques. This paper examines the nature of ransomware, its various modus operandi, its recent evolution and trends, and the successful way to preempt successful ransomware attacks.

## 02 | Introduction

Despite everyone, from governments and business leadership to the general public, high level of attention, ransomware continues to wreak havoc worldwide, targeting private and governmental organizations and even non-profits and private individuals. It doubled frequency in 2021, targeting 37% of organizations in 2021 according to IDC and, according to CISA, 14 critical infrastructure sectors. Gartner forecasted that, by 2025, 30% of governments will edict legislation regulating ransomware payments. Yet, despite these grim considerations, our 2022 Ransomware Survey clearly shows that there are techniques increasing organizations' resilience against ransomware. Yet, as always, the first step is to understand ransomware, from who is a prime target to what it is – how it works and the different types. Then, it is time to evaluate the best preemptive and protective measures to implement to minimize the risk of falling victim.

## 03 | The Five Basic Steps of A Ransomware Attacks

Though, according to VirusTotal's Ransomware in a Global Context Report, there are up to 130 variations in the type of malware used by attackers, a ransomware attack full kill-chain typically follows the same generic steps:

### 01 Distribution

Typically, the ransomware attacker successfully tricks its target into clicking an infected link, downloading an attachment, or accessing a compromised website, and the malware gains access to the target's endpoint. They also resort to other distribution techniques, such as acquiring Remote Desktop Protocol (RDP) either through direct attack or by purchasing stolen ones, through exploiting unpatched vulnerabilities, or even through brute force attempts.

### 02 Infection

The distributed malware installs itself on the infected endpoint, launches new processes, and attempts to progress laterally and vertically within the organization's network. Depending on the specific malware degree of sophistication, this step might include a stealth phase designed to maximize its reach across a network or immediately proceed to the next steps.

### 03 Communication

In some, still rare cases, the malicious code contacts the attacker's server and begins exfiltrating as much content and data as possible. At the same time, it scans your content with a view to encrypt it and sometimes also attempts to uncover access to accessible backups it could also infect.

### 04 Encryption

Having ascertained that it has reached its maximum possible reach prior to detection, the attack proceeds by encrypting files as widely as possible.

### 05 Extortion

The attacker ensures that the only content accessible from the infected network or endpoint is the message requiring payment, typically in cryptocurrency, in exchange for a decryption key. Today, double and triple extortion processes are becoming the norm. From a technical perspective, the additional extortion steps leverage the data acquired during the communication phase, so extortion is the last step of the cyber part of the attack.

## 04 | Who Are Ransomware Attacks Prime Targets?

Defining the ideal target for ransomware attacks based on sector or activity, annual revenue, location, or other socio-economic factors is fraught with difficulties. The generally accepted victim profile in 2021 identified the Banking and Finance Service Industry, Utilities, and Retail sectors as the most likely to experience an attack attempt. However, statistics emanating from different security vendors painted other pictures. So even if those sectors were slightly more targeted in 2021 and 2022 Q1, every sector is at

risk. Ransomware attackers tailor the 'ransom' amount to the presumed financial resources of their victims, and smaller targets, though they yield a lower ransom, are also typically easier to breach and less likely to have the means to launch a counterattack than large organizations. After weighing the risk/benefit ratio, ransomware attackers are likely to target anyone and everyone, so it is safe to assume that your organization systems, or even your personal computer, are potential targets.

## 05 | Ransomware Typology The Seven Types of Ransomware

Between the first locker ransomware variant apparition in 2007 and the 2017 WannaCry 'pandemic' infecting over 200 000 machines and costing billions in damages across the globe, ransomware was an annoying occurrence, but ransoms were relatively small, a few hundred to a few thousand dollars, and did not warrant extensive preventive measures. Today, ransoms can reach a few million dollars, and a ransomware attack's total costs make it an even more crucial issue, made harder to manage as ransomware attacks today come at least seven different categories:

- **Encrypting Ransomware** uses advanced encryption algorithms to block system files. Ransom demand is shown on the screen, demanding that the user pays for the decryption key to unblock the files.
- **Locker Ransomware** locks the victim out of the operating system, which makes it impossible to access the desktop, applications, and files. Although the files are not encrypted, the attackers still ask for a ransom to unlock the infected computer.
- **MBR Ransomware** is a type of locker ransomware that infects the Master Boot Record (MBR), preventing the operating system from booting up. Failure of the boot process prompts a ransom note to be displayed on the screen, demanding a ransom to unlock the MBR.
- **Scareware** is a different type of ransomware that falsely claims to have uncovered an issue on your device and requires payment to fix it.
- **Doxware or Leakware**, is the blackmailing version of ransomware, where the attacker threatens to reveal compromising information about the victim organization or individual unless payment is sent now also used as a second-tier attack to encrypting ransomware, as attackers either threaten to publish the stolen data or approach the victim organization's users directly to make them pressure the organization into paying.
- **Wiping Ransomware** is a type of ransomware attack where the data is totally erased. In some rare cases, the attackers also demand payment to restore it, even if they have no intention to do so.
- **RaaS (Ransomware as a Service)** is an off-the-shelf ransomware software that can be purchased as a service, in the same way as a SaaS (Software as a Service) for regular services. The emergence of RaaS has given access to ransomware technology to thousands of wannabe hackers who, until then, lacked the technological capability to launch a ransomware attack.

Gartner's emerging risk trends for Q1 22 score new ransomware models as high risk, which indicates a high likelihood that new ransomware models will emerge within a year.

## 06 | Why Are Ransomware Attacks So Effective?

They feature unbreakable encryption, preventing victims from decrypting the files on their own.

They can encrypt all kinds of files, including documents, pictures, videos, and audio files.

They can scramble file names, preventing victims from knowing which data was affected.

They display a ransom note message with payment instructions in cryptocurrency to avoid detection.

They have a dead man's switch; once the ransom is not paid on time, either the data is destroyed forever or stolen data is published, further tarnishing the brand image of the targeted organization or the individual reputation.

It uses a complex set of evasion techniques to bypass traditional antivirus.

They display a ransom note message with payment instructions in cryptocurrency to avoid detection.

## 07 | Why Are Ransomware Attacks So Devastating?

They interrupt the normal flow of business during the attack.

They expose the victim to potential blackmail.

Paying the ransom does not guarantee that the data will be returned, the encryption key provided, or that the provided decryption key will restore the system without damage.

The disclosure obligation means that users have to be informed, tarnishing the organization's reputation.


In addition to the ransom itself, additional costs such as business interruption, reputational damages, potential damages due to users whose data has been compromised, legal fees, insurance premium hikes, and more.

Restoring machines to a known good state can be more complex than restoring the data from backup.


The growing number of ransomware attacks endanger countries' economic stability.

## 08 | Basic Hygiene to Minimize Ransomware Damage

With the high likelihood of being targeted by a ransomware attack in the near to median future, there are a few basic steps anyone can take to minimize the attack's impact, should the system fail to prevent a breach.




Keep up-to-date back-ups encrypted, stored off-line or out-of-band, including hardware backups, source code, and executables, and regularly test them.




Have an Incident response playbook ready and regularly practice and update it.




Keep all systems up to date.



Review port settings to minimize the use of RDP port 3389 and SMB port 445 as those are favored by numerous ransomware variants.




Make sure your IDS is always up to date.




Make sure MFA is employed to the maximum possible extent.



Implement least privilege extensively.



Segment your network.

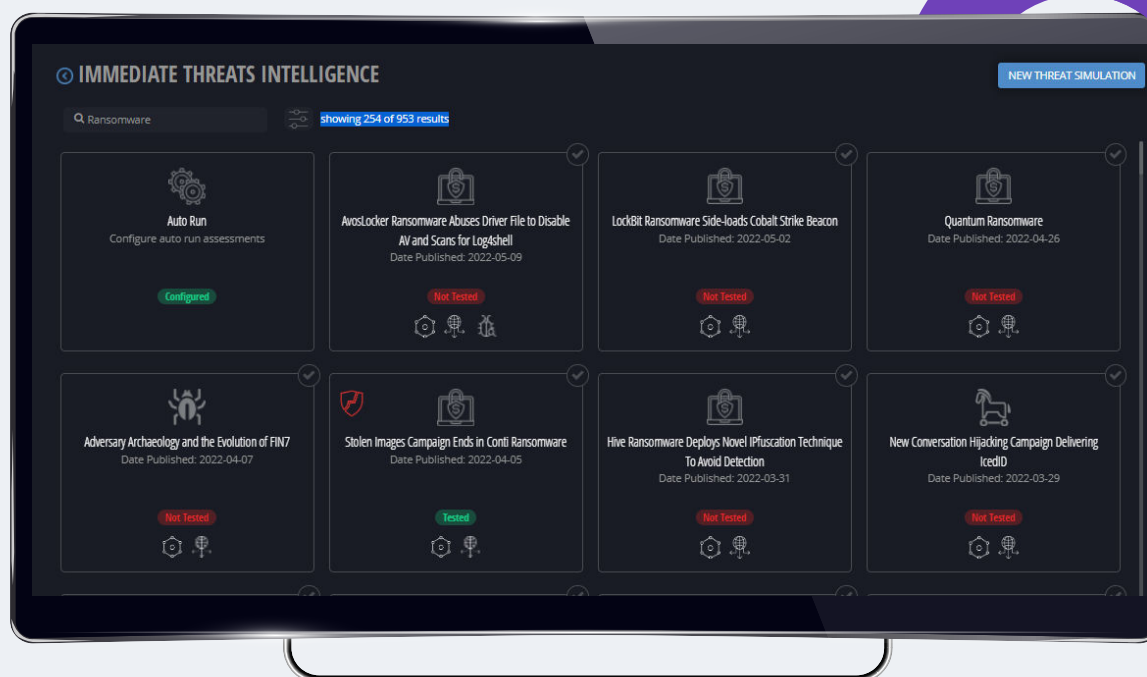


Keep IT and OT separate.

## 09 | Proactive Ways to Prevent Damage From Ransomware Attacks

Cymulate's Q4 2021 Ransomware Study: Unexpected Reasons for Optimism clearly shows that incorporating offensive security solutions to manage their security posture had a profound impact on their protection level against ransomware attacks and, as a bonus, a comprehensive range of other attacks. As opposed to simply attempting to implement best practices and cyber hygiene recommendations to the maximum possible extent with existing resources and hoping for a maximal cybersecurity impact, it is worth using offensive security solutions to validate that assumption. Offensive security technologies used to be limited to pen-testing. Today, though an annual or

bi-annual pen testing exercise might still satisfy the compliance regulator, the rate of change in the threat landscape and modern organizations' digital infrastructure experiencing frequent new deployments renders running infrequent pen testing exercises an almost futile endeavor. Emerging technologies automate the lion's share of security validation and enable running them continuously. A platform like Cymulate's Extended Security Posture Management (XSPM) provides an expansive collection of ransomware payloads and attack templates to validate your environment resilience at a click without any coding.



Checking your email gateway resilience to ransomware can also be performed at a click with ready to go, crafted ransomware payloads that mimic ransomware behaviors such as:

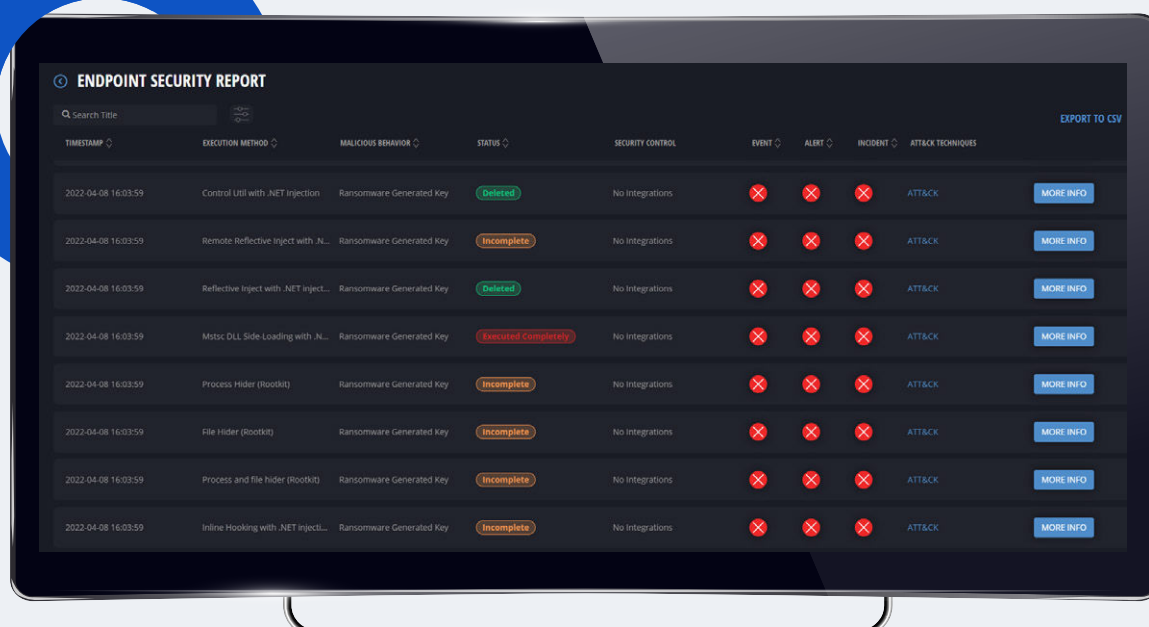
- Scanning for sensitive files to be encrypted
- Encrypting files using an asymmetric encryption algorithm (SHA256).

This bulk or granular attack emulation automatic is repeated per attack vector with vector-specific attack methods and payloads.

For example, the Endpoint Security vector can automatically run hundreds of multi-step ransomware attack scenarios with production-safe malware payloads posing no danger to your

environment. When integrated with your EDR, it corroborates the number of attacks launched with the number of attacks detected and, ideally, neutralized.

The automatically generated dynamic report lists all the pseudo-attacks results, displaying each attack's timestamp, execution method, type of malicious behavior, status (**Executed Completely** – Each stage of the attack scenario was completed successfully, therefore the attack scenario as a whole was executed completely, **Incomplete** – The attack scenario did not complete since one of the stages in the attack was unsuccessful, and did not proceed to the next stage, or **Deleted** – The payload was deleted during the attack), and more.



TIMESTAMP	EXECUTION METHOD	MALICIOUS BEHAVIOR	STATUS	SECURITY CONTROL	EVENT	ALERT	INCIDENT	ATTACK TECHNIQUES	
2022-04-08 16:03:59	Control Unit with .NET injection	Ransomware Generated Key	Deleted	No integrations	×	×	×	ATT&CK	MORE INFO
2022-04-08 16:03:59	Remote Reflective inject with .NET	Ransomware Generated Key	Incomplete	No integrations	×	×	×	ATT&CK	MORE INFO
2022-04-08 16:03:59	Reflective inject with .NET inject...	Ransomware Generated Key	Deleted	No integrations	×	×	×	ATT&CK	MORE INFO
2022-04-08 16:03:59	Msvc DLL Side Loading with .NET	Ransomware Generated Key	Executed Completely	No integrations	×	×	×	ATT&CK	MORE INFO
2022-04-08 16:03:59	Process Hider (rootkit)	Ransomware Generated Key	Incomplete	No integrations	×	×	×	ATT&CK	MORE INFO
2022-04-08 16:03:59	File Hider (rootkit)	Ransomware Generated Key	Incomplete	No integrations	×	×	×	ATT&CK	MORE INFO
2022-04-08 16:03:59	Process and file hider (rootkit)	Ransomware Generated Key	Incomplete	No integrations	×	×	×	ATT&CK	MORE INFO
2022-04-08 16:03:59	Inline Hooking with .NET inject...	Ransomware Generated Key	Incomplete	No integrations	×	×	×	ATT&CK	MORE INFO

For each individual attack, clicking the “more info” button opens a detailed report related to that specific pseudo-attack, detailing the success or failure of each of the pseudo-attack steps and providing an extensive scenario summary.



Further information about a specific step, including information about detection, mitigation recommendation, in-depth analysis, and dynamically generated sigma rules.

Similar in-depth analyses are available for all vectors (Immediate threat Intelligence, Email Gateway, Web Gateway, Web App Firewall, Endpoint Security, Data Exfiltration) and for full kill chain scenarios and campaigns.

## Sigma Rules

Sigma rules are catching on more and more for SOC teams, as a way to write one rule that can be used across multiple environments. Cymulate's unique built-in ability to generate in-context relevant Sigma rules at a click optimizes and accelerates mitigation whilst saving SOC team members considerable time.

## About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign. With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness. **Measuring your cybersecurity performance is fundamental towards creating a more secure organization!**

Contact us for a live demo, or get started with a free trial

[Start Your Free Trial](#)

## 10 | Appendix A: Breakdown of Cymulate's XSPM Integrated Solutions Ransomware Damage

Cymulate's XSPM extensive umbrella of integrated technologies covers the entire kill chain to maximize your environment resiliency with your existing tools stack and optimizes the use of resources, [increasing your cybersecurity investments' ROI](#).

### **Attack Surface Management (ASM)**

Ransomware attackers are looking for unmonitored assets to stealthily penetrate your organization's digital infrastructure, emulating an attacker's reconnaissance phase, during which they perform a comprehensive analysis of their target organization. ASM tools scan the domains, sub-domains, IPs, ports, etc., for internet-facing vulnerabilities. It is also looking for Open-Source Intelligence (OSINT) that can later be used in a social engineering attack or a phishing campaign. This tool helps organizations understand how hackers might get an initial foothold.

### **Automated Red Teaming Campaigns**

Well configured Detection tools can detect and stop a number of known attacks but fail to emulate the creativity that is the hallmark of successful ransomware attackers. Red Teaming campaigns tools go beyond just the ASM reconnaissance page to answer the question: "How can an adversary breach my defenses and internal segmentation?" These tools simulate an end-to-end campaign attempting to penetrate the organization by analyzing exposed vulnerabilities and autonomously deploying attack techniques that penetrate the network. For example, they can trigger the attack with a well-crafted phishing email. After gaining the initial foothold, the attack subsequently propagates within the network in search of critical information or assets.

### **Breach Attack Simulation (BAS)**

Ransomware attackers are looking for gaps in your security controls to find an entry point and expand their attack laterally and vertically. Breach and Attack Simulation tools answer the question: "How well are my security controls and processes performing?" It launches simulated attack scenarios out-of-the-box and correlates findings to security controls (email and web gateways, WAF, Endpoint, etc.) to provide mitigation guidance. These are primarily used by the blue team to perform security control optimization.

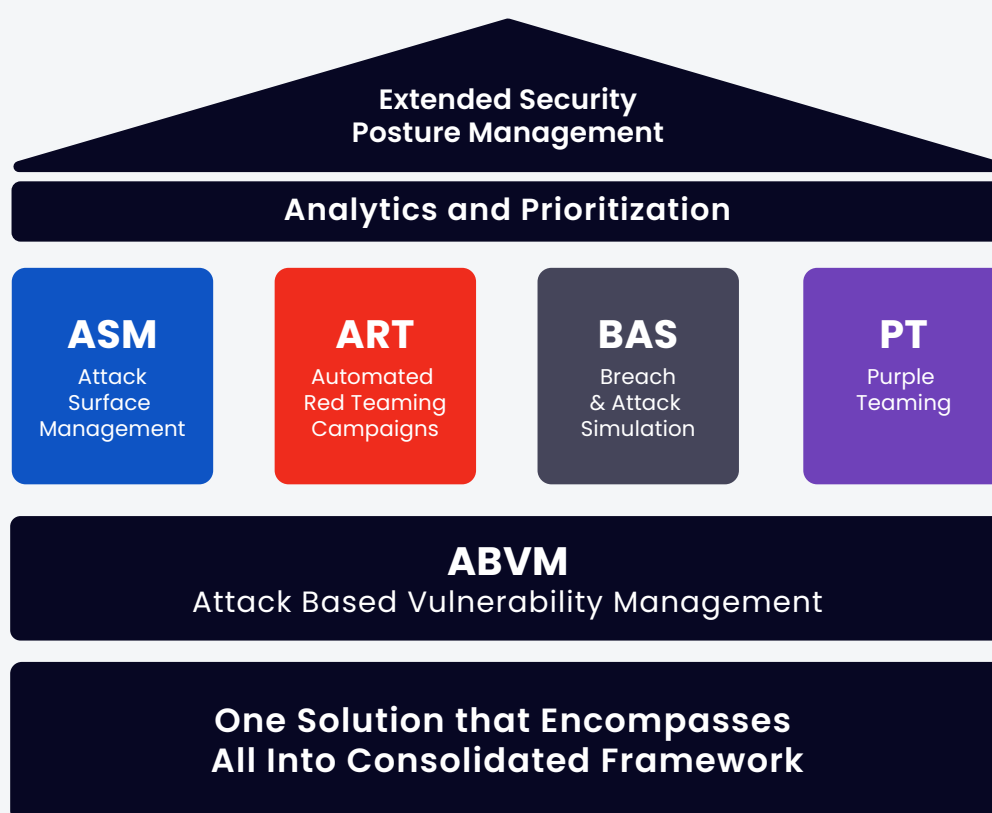
### **Advanced Purple Teaming**

Each organization has its specificities that no off-the-shelf automation can entirely cover. Purple teams expand BAS into creating and automating custom advanced attack scenarios. These tools usually extensively leverage the MITRE ATT&CK® framework, enabling advanced security teams to create complex scenarios from predefined resources and custom binaries and executions. Custom scenarios can be used to exercise incident response playbooks, pro-active threat hunting, and automate security assurance procedures and health checks.

### Attack-Based Vulnerability Management (ABVM)

Ransomware attackers' second favorite path to maximize their reach is taking advantage of unpatched vulnerabilities. The ever-growing volume of vulnerabilities is flooding IT teams with an unmanageable patching load, resulting in patching delays. Relieve the chronic vulnerability patching overload by drastically reducing the number of critical patches required. ABVM check which vulnerabilities are effectively compensated for by the defensive array and deprioritize them, focusing the patching effort on vulnerabilities that effectively endanger your infrastructure

In addition to the highest available level of protection against ransomware, continuous security posture management provides clear-cut business and technical benefits at strategic levels. Selecting a solution that works off a single platform, that is fast and simple to deploy, can be managed effectively, and is beneficial to all security professionals no matter the maturity skill level is key. The platform needs to be comprehensive in coverage and provide prescriptive, simple-to-follow technical remediation tips as well as executive reports clearly explaining risk and how it can be managed and reduced. The vendor should also be committed to an open, vendor agnostic education program. By doing so, enterprises will see significant reductions in risk, optimization of security posture, and their investments in cybersecurity maximized and simplified.



You can test your ransomware resilience now with a free trial

# 11

## Appendix B – Sources

- Abnormal – 2022 – Ransomware Volume Drops as a Main Player Exits the Stage – <https://abnormalsecurity.com/blog/ransomware-volume-drops-q1-2022>
- BleepingComputer – 2022 – Costa Rica declares national emergency after Conti ransomware attacks – <https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks>
- CISA – 2022 – 2021 Trends Show Increased Globalized Threat of Ransomware – <https://www.cisa.gov/uscert/ncas/alerts/aa22-040a>
- Cymulate – 2021 – Ransomware Study: Unexpected Reasons for Optimism
- IDC – 2021 – 2021 Ransomware Study – <https://www.idc.com/getdoc.jsp?containerId=US48093721>
- Forbes – 2021 – The Evolution Of Ransomware: Blocking Sophisticated 5th Generation Attacks – <https://www.forbes.com/sites/forbestechcouncil/2021/10/07/the-evolution-of-ransomware-blocking-sophisticated-5th-generation-attacks/?sh=38eb99e38af0>
- Forrester – 2022 – The Ransomware Survival guide – <https://www.paloaltonetworks.com/resources/research/forrester-the-ransomware-survival-guide>
- Gartner – 2022 – Top emerging Risk Trends – <https://www.gartner.com/en/audit-risk/trends/top-ten-emerging-risks>
- Gartner – 2021 – Threat of New Ransomware Models is the Top Emerging Risk Facing Organizations – <https://www.gartner.com/en/newsroom/press-releases/2021-10-21-gartner-says-threat-of-new-ransomware-models-is-the-top-emerging-risk-facing-organizations>
- Gartner – 2021 – The top 8 Cybersecurity Previsions for 2021-2022 – <https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022>
- Google Security Blog – 2021 – Protects Your Account – Even When You No Longer Use Them – <https://security.googleblog.com/2021/10/google-protects-your-accounts-even-when.html>
- Microsoft – 2022 – Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself – <https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/>
- NIH – 2021 – Ransomware: Recent advances, analysis, challenges and future research directions – <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8463105/>
- NIST – 2022 – Ransomware Risk Management: A Cybersecurity Framework Profile – <https://csrc.nist.gov/publications/detail/nistir/8374/final>
- TechTarget – 2022 – Ransomware attacks continue to plague public services – <https://www.techtarget.com/searchsecurity/news/252512797/Ransomware-attacks-continue-to-plague-public-services>
- Trend Micro – 2022 – Ransomware Spotlight AvosLocker – <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-avoslocker>
- Trend Micro – 2022 Ransomware by the Numbers – <https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers>
- Verizon – 2021 – Data Breach Investigations Report – <https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/>
- VirusTotal – 2021 – Ransomware in a Global Context – <https://storage.googleapis.com/vtpublic/vt-ransomware-report-2021.pdf>
- VMware – 2022 – Ransomware Attacks and Techniques – Analysis from VMware Threat Report – <https://blogs.vmware.com/security/2022/03/ransomware-attacks-and-techniques-analysis-from-vmware-threat-report.html>