Stopping Ransomware Attacks with True Runtime Protection

Article after article, every day we seem to hear of another successful ransomware attack against a public or private institution. In fact, the numbers are much higher with research showing 2,084 ransomware attacks in the U.S. in the first half of 2021 alone—a 62% increase from the same period in 2020[1]. And these are just complaints reported to the FBI. The truth is ransomware attacks have been going on for years, and we even see the same organizations falling victim multiple times. So, why is ransomware on the rise and such a challenge to protect against? And how can we take power back from attackers and restore it to its rightful owners? Here, we'll examine some of the key factors that contribute to the success of ransomware attacks as well as recent initiatives and innovations that enable defenders to better mitigate risk and stop attacks before they start.

Ransomware is Big Business

Ransomware as a weapon is relatively low risk and high reward. The techniques are usually successful, and the perpetrators are rarely prosecuted. When combined with the emergence of Bitcoin and other cryptocurrencies as means for payment, cybercriminals are difficult to trace. As a result, ransomware attacks are escalating and becoming more sophisticated and evasive.

Since the COVID-19 pandemic, ransomware has burgeoned into a multi-billion-dollar industry. As extortionists seek out larger and larger scale operations in search of an ever-multiplying bounty, more and more businesses and industries are at risk. In 2021, for the first time, attackers were successful in shutting down critical infrastructure in the U.S., including Colonial Pipeline, the East Coast's largest gasoline, diesel, and natural gas distributor, and JBS, the world's largest meat processor. Initial demands for payment are reaching new heights—exceeding 10 million dollars and sometimes as high as 40 to 60 million—for targets with deep pockets.[2] However, threat actors aren't just setting their sights on multinational enterprises. Plenty of cities and counties across the country have been extorted as well.

Ransomware demands were **up by 225%** in 2020.[3]

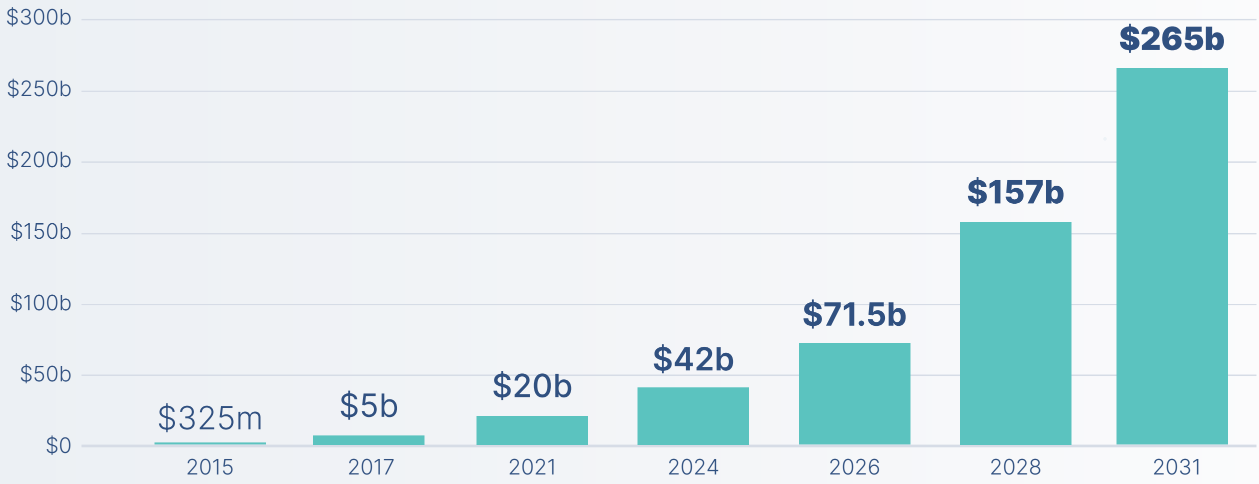
While ransom is the most obvious revenue stream for threat actors, ransomware-as-a-service (RaaS) is unlocking additional sources of revenue for a host of participants in this underground economy. Highly skilled cybercriminals develop and sell their capabilities to malicious actors who don't have the resources to develop these tools on their own. All participants supporting the service—those that provide encryption tools, communications, technical support, training, and ransom collection—share in the profits. Payment models vary and might consist of pure profit sharing, a monthly subscription fee with or without profit sharing, or a one-time licensing fee.

Costs, Beyond the Ransom

When ransomware attacks happen, the ransom payouts usually make the headlines. However, the total financial impact of a successful attack on an organization is even more sobering. Collective global ransomware costs to businesses for 2021 are estimated to exceed $20 billion.[4]

Damages include not just the ransom payment (if made), but other costs in connection to these attacks, like detection and escalation, lost business, notification, and post breach response. In a year when the average total cost of a data breach increased nearly 10% from the previous year, the average total cost of a ransomware breach jumped even higher and has now reached $4.62 million, costlier than any other type of breach.[5] Full recovery can take weeks if not months and can be far more complicated than anticipated, even if organizations appear to be back online within a few days.

Projected ransomware damages[6] are projected to **increase significantly** over the next 10 years:



A Multi-Faceted Challenge

If we take a closer look at why ransomware is proliferating, we can see that it is a multi-faceted challenge. Attacks can be executed in a matter of seconds and leverage a wide range of techniques to break into systems, access sensitive data, hijack operations, deploy encryption tools, encrypt data, and demand a ransom.

Ransomware Is Instantly Weaponized

Ransomware is so destructive because it can be instantly weaponized. It does not require any form of reconnaissance, any form of lateral movement, or privilege escalation. Threat actors don't have to know where they are in your environment or understand what's of value. They simply encrypt everything, and it's irreversible without the key.

Ransomware is most damaging when it moves laterally from desktops to servers, which are online 24/7/365 and house all the critical applications and data necessary to keep an organization operational. On the server workload, malicious code that executes undetected during runtime can do the most damage. It reaches deep into the inner architecture of applications and targets the entire function. This includes the full data set and resources and more broadly, entire server workloads. Once deployed, ransomware can encrypt files and block access.

On the server workload, malicious code that executes undetected during runtime **can do the most damage**.

Unfortunately, more than 75% of companies infected with ransomware are using endpoint protection products (EPP) or endpoint detect and response (EDR) tools that they believe could help mitigate risk.[7] However, EPP/EDR tools are not fully equipped to protect against ransomware that can bypass conventional, probabilistic tools like these. Tactics based on endless threat chasing and trying to seal off porous perimeters have proven to be ineffective.

Commonly Used Ransomware Techniques

In 2020, ransomware surged to grab the third spot in types of actions associated with breaches, more than doubling its frequency from 2019.[8] Initial infiltration is achieved through a variety of techniques, exploiting web-based attacks such as SQL injection, or stealing credentials through phishing or other various social engineering methods. A majority (60%) of ransomware cases in 2020 involved direct install or installation of the ransomware through desktop sharing applications. The remainder of cases involved email, network propagation or download by other malware. Servers are primarily targeted because that's where the data is located.[9]

As organizations setup data backup solutions to mitigate these attacks, threat actors evolved their tactics as well. Now, 81% of ransomware attacks involve the threat to leak exfiltrated data, if the victim doesn't pay the ransom.[10] Depending on the type of data exposed, the leak can compromise digital intellectual property (IP) and erode customer trust and loyalty, unless the ransom is paid.

The Defender's Dilemma: To Pay or Not to Pay?

> Nearly 80% of organizations that pay ransoms are hit again with another ransomware attack. Nearly 46% of the attacks were from the same group that executed the first attack.

Victims of ransomware face a difficult choice. Either pay the ransom and hope to restore their vital data, or risk never recovering any of it. Even if they do recover their data, there is no guarantee it will be intact or not damaged. One study found that only 8% of organizations manage to retrieve their data after paying a ransom, and 29% of organizations received less than half of their data.[11]

As to how many victims pay, the data ranges widely across private versus public targets and across enterprise organizations themselves—from nearly a third[12] to closer to 70%[13] paying a ransom to regain data. Adding insult to injury, almost 80% of organizations that pay ransoms are hit again with another ransomware attack. Nearly 46% of the recurring attacks were from the same group that executed the first attack.[14]

However, for some organizations the decision to pay or not to pay may soon be out of their hands. States, including New York, North Carolina, and Pennsylvania, are considering legislation that would ban state and local government agencies from paying ransom. They argue that prohibiting payments would deter attacks. But some experts point out that attacks will still happen as cybercriminals aren't going to research state laws and back off accordingly. And restoring and rebuilding systems could prove more costly and time consuming, particularly for smaller local governments. Instead of inadvertently further penalizing victims, providing aid to enable better protection is a more effective approach.[15] Many cities are underfunded, but even if the budget is there, cities struggle to retain skilled cybersecurity talent.

Only 8% of organizations manage to retrieve their data after paying a ransom.

29% of organizations received less than half of their data.

The Role of Cyber Insurance

Cyber insurance is becoming an increasingly popular risk mitigation strategy. Most policies cover costs to investigate a ransomware attack, negotiate with hackers, and make a ransom payment. So, it comes as no surprise that the number of companies opting for cybersecurity coverage grew from 26% in 2016 to 47% in 2020.[16]

However, some research suggests that this practice is encouraging cybercriminals. Insurers are not using incentives to reward better security practices or imposing higher fees or penalties for those who fail to improve security practices. Cybercriminals know that companies that have insurance are quick to pay the ransom. They even infiltrate insurance companies to seek customers' identities and scope of coverage so they can target them.

Challenges with gathering data to inform underwriting and risk modeling also make it difficult to accurately price policies. And, larger-scale attacks such as the SolarWinds supply chain breach are generating tremendous losses for the industry and leaving many insurers wondering if the offering is sustainable. While most companies have seen a rise in premiums by up to 30%,[17] the financial stakes are still too high for some insurers, jeopardizing the availability of coverage.

As companies look to renew policies, and first-time customers explore their options, they may encounter reimbursement limits, deductibles, as well as strict requirements for better cybersecurity strategies. It's becoming increasingly clear that cyber insurance is not a silver bullet solution to protect organizations, but instead should be viewed as one part of a risk mitigation strategy that must include best practices, compensating controls, and advanced ransomware protection.

Will the U.S. Government Help?

In the U.S., the Federal Bureau of Investigations (FBI) and the Cybersecurity and Infrastructure Agency (CISA) strongly discourage companies from paying ransoms to criminal actors, but companies often have little choice. Many feel it is better to pay and hope they will be able to resume operations quickly rather than engage in a long shutdown. So, the U.S. government is bringing its sizeable resources to bear on the problem.

In the wake of the Colonial Pipeline attack and the White House Executive Order on Improving the Nation's Cybersecurity issued in May 2021, the U.S. Department of Justice is elevating investigations of ransomware attacks to a similar priority to terrorism. The U.S. attorney's offices will be expected to share updated case details and active technical information with leaders in Washington. The move encourages reporting and tracking of associated activities to accelerate detection and response of large-scale ransomware activity.

The Biden administration has also announced the creation of a multiagency task force to combat ransomware and launched a new website to help companies and government agencies better protect themselves. The site includes detailed guidance and tips for dealing with ransomware, frequently asked questions, and an extensive library of resources. A link to report ransomware incidents to the U.S. government makes it easy to report once, and all relevant agencies will be notified.

In a move to encourage collaboration between government industry, the White House hosted a cybersecurity summit with several major technology companies and announced a series of initiatives designed to help solve the ransomware crisis. These include better integrating cybersecurity into products, improving cybersecurity training, and developing a new framework for improving cybersecurity for technology supply chains.

Pushing the conversation even further, the next step is to involve more companies, bringing the full extent and power of industry insights and innovation to address the problem. As former Cisco Chairman and CEO John Chambers said, "The startups are where the innovation happens."[18] Public and private enterprises have an obligation to think bigger, innovate faster and, ultimately, evolve our collective approach to this scourge of ransomware attacks.

Change Your Security Mindset

Now is the time for organizations to fundamentally change their security strategy. Many companies have an enhanced cybersecurity infrastructure to defend against cyberattacks and safeguard information integrity and business continuity. But if you have an extensive portfolio of security tools that are either unable to detect or stop evasive attack techniques, or are only able to alert you after the damage has been done, then this security approach is not working, is it?

The world runs on software; yet, until now, there was never a way to achieve 100 percent protection at the workload while it is running, wherever it is running. It's time to focus on runtime protection.

The Only Defense is Deterministic Protection

Virsec is taking a radical new approach to security. The Virsec team created the only security product that can determine exactly what your software is supposed to do and stop it from doing what it is not. Its breakthrough technology fully protects the software workload while it is running, wherever it is running. This offering stops threats at runtime and prevents dangerous ransomware attacks targeting applications and workloads most vital to the business.

Secure Environments by Protecting Runtime

Application runtime remains one of the most vulnerable attack surfaces in any organization. Sophisticated, well-funded attacks repeatedly target runtime—from businesses to critical infrastructure to government agencies—and we must mount an effective defense. Ransomware attacks are leveraging multi-step kill chains, deploying fileless malware, and using remote code execution (RCE) techniques that are bypassing conventional, probabilistic security tools.

True runtime protection requires fully understanding the software by mapping everything it is supposed to do, and immediately stopping what it is not. Many cybersecurity tools are unable to gain visibility or control into runtime as application and software code executes. Instead, they seek to protect before and after runtime, but never during. More critically, these tools are focused on the outside of the application and lack a deeper understanding of the intent of the software. Without this knowledge, the tools cannot identify when the software or application deviates from its intended performance.

Only Allow Legitimate Code to Execute

Using patented AppMap™ technology, Virsec Deterministic Protection Platform (DPP) automatically creates a dynamic golden image of all critical application resources, including files, scripts, binaries, container images, and libraries, and only allows authorized processes to execute. This enables organizations to ensure that attackers cannot exploit critical applications to run malicious code.

With AppMap deployed, each application in an organization is protected—no matter where it resides. Whether you have applications in the cloud, on-premises, containers, hybrid, or air-gapped—each application is individually protected. Any deviation in the application's expected performance at runtime is instantly detected, treated as a threat, and blocked.

Software That Offers Protection – Bugs and All

DPP is designed to provide automated and continuous application-aware workload protection at runtime from the inside—bugs and all. By protecting the full attackable surface across the application stack as it relates to web, host, and memory, DPP ensures the integrity of code itself, providing defense from within.

DPP's unique technology "guardrails" critical applications, software, and workloads in any environment, providing system integrity assurance with strict application control and memory protection in a single solution —delivering in-depth visibility across the entire workload. Extortion attacks are identified and stopped immediately, regardless of the level of sophistication of the attack. This also means that if any new tactics, techniques, and procedures (TTPs) are used, your organization is still protected.

Conclusion

Ransomware attacks continue to be pervasive and damaging, but there is a solution and end in sight. Public and private organizations are continuing to innovate their thinking and collective need for a new approach to the problem. With government and industry coming together, a portfolio of risk mitigation strategies and offerings, and first-of-a-kind solutions like the Virsec Security Platform, that immediately blocks ransomware before damage can be done, defenders have the power to make ransomware and cyber attacks irrelevant.

End Notes

[1] U.S.-CERT CISA Alert (AA21-243A)

[2] NPR

[3] U.S.-CERT CISA Alert (AA21-243A)

[4] Cybersecurity Ventures

[5] Cost of a Data Breach Report 2021

[6] Cybersecurity Ventures

[7] Sophos

[8] 2021 Data Breach Investigations Report

[9] 2021 Data Breach Investigations Report

[10] Coveware

[11] HelpNet Security

[12] Sophos

[13] Pindrop

[14] Newsweek

[15] The PEW Charitable Trusts

[16] U.S. Government Accountability Office

[17] U.S. Government Accountability Office

[18] Yahoo! Finance

Additional Sources:

https://www.washingtonpost.com/politics/2021/09/07/cybersecurity-202-ransomware-is-wreaking-havoc-us-cities/

https://www.policyholderpulse.com/ransomware-insurance-coverage/

https://www.insurancejournal.com/news/national/2021/07/07/621416.htm

https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-cyber-security-challenge

https://www.zdnet.com/article/ransomware-has-become-an-existential-threat-that-means-cyber-insurance-is-about-to-change/

https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/

https://www.cisa.gov/stopransomware

About Virsec

Virsec is on a mission to make security response obsolete. Taking a First Principles approach to protection, the Deterministic Protection Platform (DPP) by Virsec automatically and consistently maps exactly what your software is supposed to do and stops, in milliseconds, any deviations — preventing attackers from leveraging vulnerabilities to execute control and run malicious code. DPP is a proven technology that enables leading government and commercial organizations around the world to protect their server workloads, at runtime, against ransomware and other known and unknown threats, reduce operating costs and meet key compliance requirements. Virsec is headquartered in San Jose, California, with offices all over the world. For more information, please visit www.virsec.com.