SP6

Ransomware Is Advancing, So Should You

Why Ransomware Is a Bigger Problem Than You Think

A Technical Summary

The state of ransomware is becoming increasingly alarming. **Ransomware attacks have continued to grow in frequency and sophistication**, affecting businesses, organizations, and individuals worldwide.

It is currently estimated that a ransomware attack occurs every 11 seconds, and according to the IBM Cost of Data Breach Report, in 2022 a single ransomware attack cost global companies on average $4.5 million dollars, and U.S. companies up to $9.4 million dollars – these figures don't include the ransoms themselves. So, it is clear the risk is growing, and with changing trends in ransomware group tactics, it's becoming even harder to minimize potential loss.

We're a far cry from the days when simply paying a ransom or recovering from backups would solve the problem. The launch of ransomware-as-a-service (RaaS) platforms exponentially increases the likelihood that a company can be targeted for ransomware. This is because bad actors no longer need an intricate technical skillset to carry out a ransomware attack. Script kiddies can license ransomware service providers to carry out an attack for them, much like what SaaS providers do for commercial software. With so many companies willing to pay the ransom, bad actors see ransomware as an easy payday with a relatively low-risk to high-reward ratio.

In 2022 a single ransomware attack cost global companies on average $4.5 million dollars, and U.S. companies up to $9.4 million dollars.

One of the most significant developments in the ransomware landscape is the rise of ransomware-as-a-service (RaaS) platforms. As mentioned before, these platforms provide would-be attackers with easy-to-use tools and resources to launch attacks, making it more accessible for criminals without significant technical expertise to conduct successful ransomware campaigns. Ransomware as a Service (RaaS) platforms are considered riskier than traditional ransomware attacks for several reasons:

Accessibility: Cybercriminals with little technical expertise can more easily start ransomware attacks thanks to RaaS platforms. The barrier of entry into the ransomware attack space is lowered by the fact that these platforms frequently include user-friendly interfaces, clear instructions, and technical assistance.

Scale: RaaS platforms can potentially reach a much wider audience than traditional ransomware attacks, as they can be used by multiple cybercriminals simultaneously. This increases the number of potential victims, making it more likely that attacks will succeed and generate increased profits for the attackers.

Customizability: RaaS platforms often come with customizable features, allowing attackers to adjust the ransomware code to suit their specific targets. This makes it easier for criminals to evade traditional cybersecurity defenses and carry out successful attacks.

Attribution: In a traditional model, TTPs would be indicative of a group or persons that were responsible for the attack, thus making it easier to track the attacker and monitor for repeat offenses in the future. The RaaS model makes that increasingly more difficult as software with traditional TTPs we would recognize is modified slightly, which in turn makes it more difficult to detect. Signatures change, TTPs become less recognizable, and less skilled cyber criminals are given a boost to their repertoire.

TrendMicro reported the most active attackers in 2022 are attributed to hosting RaaS platforms: LockBit, BlackCat, Black Basta, and Karakurt

Who Is Responsible for This?

Although the responsibility for Ransomware as a Service (RaaS) platforms is difficult to attribute to a single entity, TrendMicro reported these four families to be the most active attackers in 2022 and are attributed to hosting RaaS platforms: LockBit, BlackCat, Black Basta, and Karakurt, deemed to be the extortion arm of the Conti ransomware group. Generally speaking, these platforms are operated by criminal organizations or individual hackers who create and distribute ransomware code, often in exchange for a percentage of the profits generated from successful attacks. However, some experts have also pointed to the role of underground marketplaces and forums in facilitating the sale and distribution of RaaS platforms. These marketplaces provide a centralized location for cybercriminals to advertise and sell their services, including RaaS platforms, to other criminals.

Additionally, some have suggested that the lack of effective law enforcement in certain regions may contribute to the proliferation of RaaS platforms. With little risk of being caught and punished, some cybercriminals may be more willing to engage in these types of activities. Ultimately, the responsibility for RaaS platforms lies with those who create and operate them, as well as those who facilitate their distribution and use. It is up to law enforcement, governments, and cybersecurity experts to work together to combat this growing threat and hold those responsible accountable for their actions.

Ransomware Is Continuing to Evolve

RaaS platforms represent a growing threat to organizations and individuals, as they lower the barriers to entry for cybercriminals and make it easier to launch successful ransomware attacks. It is crucial for individuals and organizations to remain vigilant and implement robust cybersecurity measures to protect themselves from these types of attacks.

Another concerning trend is the shift towards double extortion attacks, where attackers not only encrypt the victim's data, but also steal sensitive information and threaten to leak it if the ransom is not paid. This approach has led to an increase in ransom demands, and even if the victim decides to pay, they are still at risk of reputational damage and regulatory penalties. In addition, the targeting of critical infrastructure has also been on the rise, with attacks on hospitals, utilities, and transportation systems causing significant disruption and potential danger to human lives. Furthermore, ransomware attacks have increasingly been used as a tool for geopolitical gain, with nation-states accused of conducting attacks to disrupt their adversaries' operations.

> *It is crucial to remain vigilant and implement robust cybersecurity measures to protect themselves from these types of attacks.*

What's Being Done to Solve the Problem

The shift in TTPs to include extortion of data represents an existential shift in the way companies that have been infected with ransomware have to approach their breach. No longer can we just restore infected systems from backups. No longer can we just pay the ransom to mitigate the risk. Exfiltration and extorsion mean adversaries can sell your sensitive documents, or in worst cases, account information, to other adversaries. This in turn exponentially increases your risk of future breaches. Ransomware is seen as an easy payday for adversaries, and with the launch of RaaS platforms, the ability of bad actors to carry out ransomware attacks is increasing exponentially. The scale, frequency, and complexity of the adversary are evolving, and as such, we as defenders must evolve too.

To combat the ransomware threat, governments and businesses have been implementing new security measures and frameworks, including improved backup and disaster recovery procedures, multi-factor authentication, deploying and enforcing the principle of least privilege, and more effective employee training on cybersecurity awareness. However, these are just the basics. You will hear these solutions proposed to every cybersecurity problem, and although it isn't wrong, it isn't exactly keeping up with our advancing adversary. Your MFA needs to extend to RDP sessions — don't just limit it to your initial network access. This implied trust makes it much easier for the adversary to traverse your network once they are inside. On top of that, ensure Privileged Access Management is enforced at the highest level. There is no reason for everyone in your IT department to have administrative rights. Use a Privileged Access Management (PAM) solution to help enforce managing those elevated permissions.

How Can We Do Better Moving Forward?

But what can we as defenders do to really advance from where we are today? There is a concept in the software development lifecycle that security practitioners should adopt. We must stress test our security controls and put them through a QA/QC process iteratively and often. The approach up to this point has been deploying a security control in our environment, crossing our fingers, and hoping that it stops every piece of malicious activity that comes our way. If we asked you the questions, *can your firewall solution prevent Blackbasta from being downloaded from the internet? Does your email filter flag and block email attachments that contain LockBit signatures? Does your EDR solution recognize and prevent an executable that is attempting to encrypt a file?* Most of you reading this probably cannot definitively answer these questions. You're most likely saying to yourself, "well I hope my controls hold up and do what they are supposed to do."

What if we told you there was a better way? You can put your security controls through an SP6 Ransomware Readiness Assessment to get definitive answers to these questions. A one-time assessment with a Breach and Attack Simulation (BAS) tool runs these real-world scenarios in your environment. Not only will we test your controls, but we will give you the answers to the test when we are done so you can make improvements. With BAS, you are able to understand the impact of ransomware on your environment before it happens – all while in a controlled manner to learn where your weaknesses are. Are there particular Business Units less prepared than others? Are some subnets more susceptible than others? Ultimately, you can improve and iterate on these weaknesses continuously. It's easy to stick our heads in the sand and hope the breach never happens, and yes, it's a whole lot harder to advance with our adversaries and try to stay one step ahead of them – but which approach do you want to take for the ultimate protection?

Overall, the state of ransomware in 2023 remains a significant threat to global cybersecurity. While progress is being made in mitigating the risks associated with ransomware attacks, more work is needed to prevent attackers from exploiting vulnerabilities and causing significant harm. Our adversaries are advancing every day and we must advance with them. Every organization is becoming an easier target with each passing day.

SP6

About SP6

SP6 is a niche technology firm specializing in cybersecurity, cyber compliance (with a heavy emphasis on CMMC), and systems availability. Our organization is committed to ensuring that clients and their systems are secure, compliant, and highly performant.

Request a Conversation

For more information, visit **www.SP6.io**

or contact us at **Service@SP6.io**.