CyberTalk.org

The CISO's Guide to Ransomware Prevention

TABLE OF CONTENTS

INTRODUCTION

What is ransomware?

Ransomware is a form of malware, which is malicious software that can harm or corrupt your computing infrastructure.

Ransomware is known for freezing computers and rendering files inaccessible. It can also destroy computer systems, either temporarily or permanently

Why does ransomware matter?

Ransomware can hurt businesses in a rapid, acute fashion. A ransomware attack can unfold in less than 45 minutes. As a result, the affected enterprise may not be able to properly use computing infrastructure for hours, days or weeks. In some cases, the impact on productivity, combined with other tangential financial losses, force businesses to fold altogether.

The average ransomware attack costs businesses around $4.4 million.

Ransomware by geographic locale

Although some geographic locales may experience a higher volume and frequency of ransomware attacks than others, ransomware threats loom as a concerning business trend around the world. Each week, more than 1,200 organizations fall victim to ransomware attacks.[1]

The Asia Pacific region is currently experiencing the highest volume of ransomware attacks. North America, Europe, Latin American and Africa trail behind.

Ransomware within your industry

Recent waves of ransomware have ravaged businesses across industry sectors. Businesses in the energy sector, the financial sector, the health and human services sector, the education sector, the retail environment and more have felt the impact of ransomware attacks.

The table below to the right shows which industries are most prone to ransomware attacks in specific regions.[2]

The reality is that all industries are at-risk, without exception.

Asia Pacific	Latin America	Africa	Europe	North America
Insurance/ Legal	Communications	Finance/ Banking	Utilities	Healthcare
Manufacturing	Manufacturing	Manufacturing	Software Vendor	Software Vendor
Healthcare	Retail/ Wholesale	Retail/ Wholesale	Healthcare	Insurance/ Legal
ISP/MSP	Finance/ Banking	ISP/MSP	ISP/MSP	Education/ Research
Government/ Military	Government/ Military	Government/ Military	Government/ Military	Government/ Military

[1] Global surge in ransomware attacks: To pay or not to pay is not the only question, Check Point Software https://blog.checkpoint.com/2021/06/23/global-surge-in-ransomware-attacks-to-pay-or-not-to-pay-is-not-the-only-question/#:~:text=Check%20Point%20Research%20(CPR)%20recently,without%20exceptions%20are%20at%20risk

[2] The new ransomware threat: Triple extortion, Check Point Software https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/

DYNAMIC TRENDS

Ransomware-as-a-Service

Historically, ransomware attacks were largely conducted by ransomware gangs. A ransomware operation was a difficult feat to pull off alone. However, new Ransomware-as-a-Service software enables any threat actor to invest in "off-the-shelf" ransomware products. In turn, any individual can independently execute a ransomware attack.

After Ransomware-as-a-Service (RaaS) based attack is launched, the threat actor's victim or victims are directed to the RaaS operators' payment portal. In some cases, the operators provide "customer service" to help victims pay extortion fees.

Triple extortion threats

Free online ransomware decryption tools, data backups and other savvy tactics can help victims circumvent the difficulties caused by ransomware attacks. For example, enterprises can contend with encrypted files by restoring data from backups, making ransom extortion payment obsolete.

Hackers have caught on. New ways of bringing organizations back to the negotiating table are emerging. Chief among them? Threatening to leak sensitive data belonging to clients or threatening a Distributed Denial of Service attack against the target organization. These days, ransomware not only means infrastructure disruption and a potential for leaked internal data; ransomware threats are now very multi-dimensional.

The bottom line is that ransomware threat actors are adding additional layers of pressure in attempts to force organizations to part with their resources.

Common Ransomware-as-a-Service Strains

- **Ryuk ransomware.** Experts estimate that Ryuk results in about one third of ransomware infections.
- **LockBit ransomware.** LockBit has existed for several years, but has recently become a part of RaaS operations.
- **REvil/Sodinokibi**. This type of ransomware has affected major organizations worldwide.
- **Egregor/Maze ransomware.** Although Maze has stopped its operations, related ransomware variants –like Egregor- remain operational under the RaaS affiliate model.

The Ransomware-as-a-Service strains mentioned above represent a fraction of the number of ransomware strains that exist. However, these have had significant impact on businesses and as a result, RaaS "affiliates" find them lucrative to deploy.

RANSOMWARE, MSPs, AND MSSPs

In July of 2021, a ransomware attack hit the IT firm known as Kaseya. The attack's aftershocks were felt by all of Kaseya's clients, and their client's clients. This could occur because the aforementioned firm is a managed service provider (MSP), meaning that they distribute computing services to other organizations. In turn, these organizations provide computing services to even smaller businesses.

The Ransomware-as-a-Service affiliate who conducted the attack clearly intended to propagate the ransomware to Kaseya's MSP customers. Once the ransomware attack blighted Kaseya, it also immediately affected at least 1,000 additional enterprises. A $70 million ransom payment (in Bitcoin) was requested in order to compensate for all organizations' victimization.

As the aforementioned example shows, MSPs and MSSPs may be at elevated risk of ransomware attacks. They represent easy conduits for attacks, with a potential for downstream effects and corresponding increases in profits. Experts contend that MSPs and MSSPs often fail to take the threat of ransomware seriously. Those that retain sophisticated, strong cyber security infrastructure may be able to weather the storm.

Actionable cyber security steps for MSPs and MSSPs:

- Conduct a risk assessment
- Initiate vulnerability scanning
- Identify a strong cyber security partner (vendor)
- Invest in cyber security solutions that address all attack vectors; email, endpoint, mobile, and more
- Develop and regularly update a cyber incident response plan
- Follow best practices around cyber security; patching, timely software updates, education awareness programs, etc.

Given the increased incidence of ransomware attacks on service providers, organizations should take the opportunity to pursue stronger security.

---

[3] Kaseya, what this ransomware attack fallout means, Cyber Talk
https://www.cybertalk.org/2021/07/06/kaseya-what-this-ransomware-attack-fallout-means/

PREVENTION

To prevent ransomware attack damage, implement these cyber hygiene habits and best practices:

1. Provide employees with cyber security awareness training. Many ransomware attacks start with a convincing phishing email sent to an employees' inbox.
2. Develop stronger user authentication methodologies; these include multi-factor authentication and password policies.
3. Ensure that your organization retains usable backups of all critical data, databases, key applications, and servers in non-networked locations.
4. Test backups regularly as part of your ransomware prevention strategy.
5. Segment networks to prevent lateral movement in the event of a breach.
6. Regularly update and patch software. Organizations have needlessly suffered security incidents due to patching oversights.
7. Deploy proven, effective threat detection tools. Opt for automated threat detection, which can increase advanced attack identification capabilities.
8. Filter most threats out of systems before they can cause harm by using automated email security and endpoint security tools.
9. Pursue a 'defense-in-depth' approach, which refers to layering security measures.
10. Stay up-to-date regarding the latest security threats through vendor-sponsored blogs, like CyberTalk.org.

EXPERT INTERVIEW HIGHLIGHT

Ransomware Insights with Workforce Security Expert Brian Linder

The prospect of a ransomware threat can feel daunting. For some, fighting ransomware may even feel hopeless. Here's what one of Check Point Software's experts has to say on that front...

Brian Linder is a Workforce Security Expert and Member of the Office of the CTO with Check Point Software. He is also a legacy contributor to thought leadership site CyberTalk.org, where his insights and analysis are regularly featured.

To see the full interview, click here.

Is it a battle that we've lost?

'Is it a battle that we have lost?' is a burning question. No, it is not a battle that we have lost. First of all, thanks to the press and thanks to a few high-visibility ransomware attacks that made the cover of the *Wall Street Journal* and other C-level media outlets, the reality of ransomware and all that it encompasses has reached executives.

You need to be looking at innovators in the cyber security white hat ecosystem who have built tools that can not only detect the presence of malware – because it all starts with malware of some kind – but that can also detect the presence of an actual ransomware attack in-progress. You need to be able to stop ransomware in its tracks without human intervention; without highly skilled and hard-to-find cyber security experts staring at a screen 24 hours per day waiting to catch an attack as it unfolds.

You need tools that are working on ransomware detection automatically and that can provide a rapid response. Avoiding ransomware requires an evolved toolset on the endpoint that offers robust, multi-layered protection.

DEFENSE

In the event that a ransomware attack hits your organization, here's how to respond:

1. Contain the breach. Mitigate damage efficiently and avoid allowing the attack to worsen.
2. If possible isolate the infected device/s from your network
3. Ensure that all traces of the ransomware/malware are removed from your system.
4. Scan backups to check for malware. If no threats are found, attempt to restore data from backups.
5. Contact internal IT administrators and executives who should know about the attack.
6. Organizations are also encouraged to reach out to law enforcement, as appropriate.
7. Avoid paying ransom extortion fees. Decryption tools are not guaranteed to work and hackers can still choose to leak data.
8. Regardless of whether or not you maintain a cyber insurance policy, contact your business insurance group.
9. Appropriate departments to notify clients other business relations who may have been negatively affected by the breach.
10. Reach out to your cyber security vendor, which may be able to offer further insights into your specific ransomware experience.

CASE STUDY: TopRx

Fighting back: Next generation ransomware threats

As the coronavirus pandemic swept through society in March of 2020, TopRx needed to quickly extend protection to newly remote employees. The organization also wanted more visibility into remote endpoints, and to replace an older signature-based detection solution with one that used behavior-based techniques.

TopRx engineers had thrown a variety of malware, ransomware and phishing attacks at a variety of platforms. After comparing solutions from Check Point, VMware Carbon Black and CrowdStrike, the group found that Check Point Harmony Endpoint was the only platform capable of stopping all tested threats.

Fighting back: Next generation ransomware threats

Harmony endpoint enabled TopRx to get ahead of the game. Using the built-in deployment policies, the TopRx team protected all endpoints in roughly two days. Harmony Endpoint is also integrated with the Check Point Infinity architecture for effective detection and prevention of imminent threats.

Harmony Endpoint's powerful anti-ransomware features offer complete attack containment and remediation to quickly restore any infected systems. Anti-ransomware functions create small backups of users' files while users are working. In the event that the software detects ransomware starting to encrypt files, it stops the encryption process and instantaneously recovers files that would have been lost.

"I highly recommend Harmony Endpoint to other security professionals," says Catanzaro. "It's very robust and has proven highly effective. TopRx has greatly improved its security posture with far less time invested in maintaining endpoint software. It's great."

To learn more about TopRx's decision, see the complete case study here.

SOLUTIONS

Specific solution types that can help...

1. Prevention-focused solutions that leverage AI within a multi-layered security architecture are best.
2. An intelligent, consolidated ransomware prevention architecture can prevent known and zero-day attacks.
3. Consider purchasing anti-ransomware tools that are part of a larger cyber security solutions package.
4. Seek out cyber security solutions that offer a high ROI and low TCO.

IN CONCLUSION:

Ransomware threats can easily undermine enterprises. The threat persists across industries and across geographic locales. Roughly hewn cyber security architectures are not tough enough to combat next generation threats. The best approach to fighting off ransomware starts with prevention. While there are never any guarantees, with a strategic cyber security roadmap, it is possible to win the fight. For further expert insights into the ever-changing ransomware threat landscape, visit Cyber Talk.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com