Whitepaper

Avoid Ransomware Attacks:

Tips to Prevent, Detect and Recover

Ransomware attacks continue to escalate, with a significant surge in activity. The financial toll of these attacks has also reached new heights, with ransomware gangs extorting over $1 billion from their victims in 2023, a record-breaking sum that underscores the growing sophistication of these cybercriminals.

Organizations continue to be the primary target for ransomware attacks due to the potential for significant payouts. The average ransom paid by businesses saw a dramatic increase, reaching $1.54 million in 2023, nearly doubling the 2022 figure of $812,380.

This trend highlights the escalating costs for businesses, not only in terms of the ransoms paid but also in the broader financial impact of these attacks, including downtime, lost productivity, and the cost of remediation efforts.

Managed Service Providers often assist clients with data restoration to avoid the downtime that can be caused by a ransomware attack. They also work with clients to improve their security posture overall so they can proactively protect against ransomware attacks. Here's what your organization needs to know about ransomware and how cloud computing can help protect your critical systems and data.

What is Ransomware?

Not all ransomware is created equally. While there may be more than a hundred types, they all share three common traits:

1. The cybercriminal infects your computer, through a spear-phishing email or something similar (targeted at a specific employee) or a visit to a legitimate website infected with malicious code.

2. They encrypt your files and demand payment (often in Bitcoin) to receive a decryption key.

3. The decryption key is usually successful; however, it can depend on the honesty and follow-through of the cybercriminal.

4. They can result in significant operational disruption, data loss, and financial and reputational impacts.

There Are Two Main Types of Ransomware:

Lock Screen *and* Encryption Ransomware

Lock Screen Ransomware

Lock screen ransomware (or screen locker ransomware) is when a user is restricted from accessing files or logging in until providing payment, often showing up as a pop-up demand. With lock screen ransomware, you are unable to use the infected device.

***

Encryption Ransomware

With encryption ransomware, your data is present, but you aren't able to read or access it because it is encrypted and scrambled. The cybercriminal will then ask for a ransom to unscramble the data.

While you may be able to find a workaround to lock screen ransomware, that's not the case with file-encrypting ransomware. By the time you realize your files are encrypted and unreadable, or you find or receive a ransom note, the damage has been done. The work will be irreversible without the private decryption key held by the attacker.

How Files Get Infected with Ransomware

The increase in ransomware attacks over time has also coincided with cybercriminals changing their tactics. Spam emails used to be the most popular way to spread malware, including ransomware. However, spam filters have taken the wind out of that approach. Now, hackers often use spear-phishing, which targets an individual directly, instead of sending out a mass email.

Hackers most often use email phishing campaigns, software vulnerabilities, and RDP vulnerabilities to carry out ransomware attacks. Other sources of ransomware include social media, malicious advertising (even on trusted websites), and bold cold calls via phone where an attacker poses as a software vendor or IT provider and directly requests access to the user's computer to resolve a purported problem, but instead installs ransomware.

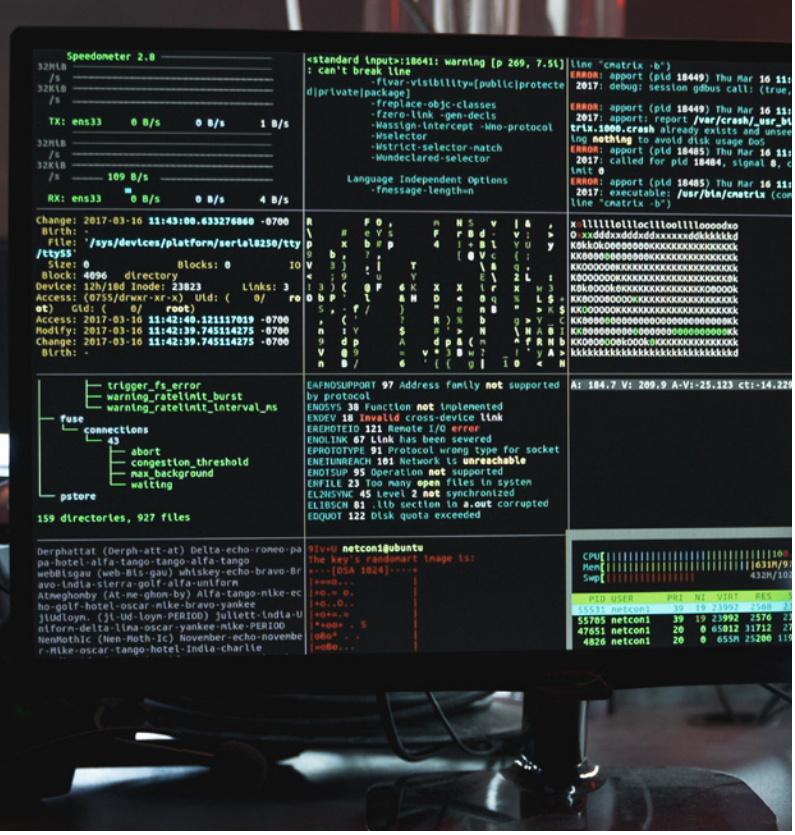
> *You likely won't know you've been hit right away, but within seconds the ransomware virus will silently start encrypting your files.*

How You Know If You Have Been Hit By Ransomware

You likely won't know you've been hit right away, but within seconds the ransomware virus will silently start encrypting your files—and files accessible via your network. The files are generally encrypted with a public encryption key in such a way that you cannot decrypt the files without the second key of the pair. You probably won't get a ransom note until hours or days later when the encryption is complete.

Dwell time is another factor to consider, which is the amount of time a hacker spends hiding in your network before being discovered. Over the past decade, *average global dwell time has dropped* from 416 days to just 24 days. This sounds like good news on the surface – the longer a cybercriminal spends in your network, the greater the chance they have infiltrated key files and will lock your systems. This decline can be partially attributed to the ability to detect threats more quickly. However, some attackers use identification to their advantage, publicizing data leaks in a "name and shame" strategy to extort more money from businesses whose reputations are at stake.

In the meantime, you may discover files that appear to be corrupted. Encrypted files cannot be read by any application. The first sign of damage may be error messages on your computer when opening files. If you're being asked which application should be used for files you're used to opening, that could be a sign of trouble.



When Internet of Things Devices Are Hit by Ransomware

Even smartphone apps and Internet of Things (IoT) devices can be infected with ransomware. We've come a long way since two hackers demonstrated a proof-of-concept of thermostat lock-screen ransomware at the 2016 Def Con conference in Las Vegas. Malware on IoT devices increased 400% between 2022 and 2023.

However, the hacking at Def Con still serves as a powerful reminder of more that could come. Imagine cybercriminals cranking up the building's heat in the summer or turning it off when it's freezing outside, and then locking the device until the ransom is paid with Bitcoin. Like a small computer, the hackers' off-the-shelf smart thermostat ran a version of Linux and had a user input and an SD card. The device was especially vulnerable because the firmware was readable and the code ran from the root.

The introduction of Mirai—a malware and botnet combination—has introduced even more complexity into the ransomware arena. This virus can compromise a wide range of Internet of Things (IoT) devices, including DVRs, security cameras and network gateways. As with much of the more recent distributed denial of service (DDoS) botnet malware, once a device is infected with Mirai, an attacker gains full control of the device and can use it for denial of service attacks— or potentially hold it for ransom.

What Data Is Most Likely to Be Held Hostage?

Ransomware attacks target various types of business data, with a preference for sensitive information, critical to operations, or likely to yield a high ransom payment. Cybercriminals often focus on sectors such as healthcare, finance, and legal services, with large amounts of personal and sensitive data. Industries that rely heavily on data for their day-to-day operations, like energy and utilities, are also at risk because disruptions can have significant service delivery and safety implications.

Large companies and those in wealthy countries are attractive targets due to their financial resources, while industries known for paying ransoms, such as retail and IT services, encourage further attacks. Additionally, sectors with perceived lower security measures, like education and small to medium-sized businesses, are targeted for their ease of penetration. Overall, ransomware attackers are drawn to data that is valuable, sensitive, and integral to a business's functionality, making the threat of ransomware a persistent concern across various industries.

How Much Does Ransom Cost?

Some organizations are being targeted for high ransom amounts. A 2021 study by Sophos found that the average ransom for *midsize organizations is $170,404.* However, by 2023, this figure had risen dramatically to $1.54 million USD, according to the Sophos State of Ransomware 2023. And the average cost of rectifying one of these attacks, including downtime, cost of the device, network, people, and opportunities lost, can cost much more. IBM's Cost of a Data Breach Report found that the average total cost of a ransomware breach, not including the ransom, was $4.45 million.

Unfortunately, the FBI reports that even if payment is made, the decryption key provided by the perpetrator to unlock the files may not work due to system configuration issues. Or the perpetrators may not provide the key after receiving the money and instead follow up with a second ransom demand. The Sophos study found that only 65% of encrypted data gets restored on average.

Backups May Not Be Enough

When dealing with a ransomware threat, a key point is to ensure business continuity by backing up data regularly and testing the backups periodically. Any backups, including cloud backups, need to be secured in a way that they are inaccessible to spreading ransomware virus. Many ransomware infections will encrypt any accessible data including external storage, USB drives and mapped and unmapped network drives. Immutable storage, storage that can't change or deleted after creation, and air gapping, a method that creates a separation between systems by placing them on different networks, can both help prevent spread.

> *"You likely won't know you've been hit right away, but within seconds the ransomware virus will silently start encrypting your files. With ransomware often striking silently, secure backups are critical."*

Having a secure and validated data backup program is the easiest way to avoid having to pay ransom. Preparing in advance with a business continuity plan, disaster recovery plan, and the help of a company with cloud security and disaster recovery expertise can help you avoid the headache of ransomware and other security breaches—and help you to ensure faster mitigation and recovery if your organization is attacked.

Machine Learning: Taking a Bigger Step to Stop Ransomware

Machine learning techniques available today in cloud computing solutions such as Microsoft Azure can provide protection against both known and potentially never-before-seen ransomware and other breaches that may make it past antivirus and SIEM systems. Machine learning allows organizations to track the normal behavior of internal and external users and typical traffic patterns — and act when behavior differs even subtly from what is expected. For example, if a user doesn't usually encrypt, copy or delete large numbers of files, it's a red flag if they attempt to do so. You can bring much more power to your ransomware deflection efforts when you have adaptive systems in the cloud.

> *Two thirds of businesses said they suffered a significant revenue loss because of a ransomware attack.*

Limiting the Reach of a Ransomware Infection

To enhance your organization's resilience against ransomware, it's crucial to adopt a multi-layered security strategy that includes the latest vulnerability tools for patch management and operating system updates. Implementing Next-Generation Firewalls (NGFW) and Extended Detection and Response (XDR) systems can significantly restrict unwanted access. Email security measures and managed detection response services, which analyze user behavior for anomalies, are also vital components of a robust defense. Regular risk assessments are recommended to identify vulnerabilities and create a roadmap for establishing a secure foundation.

When preparing for the eventuality of a ransomware attack, it's wise to operate under the assumption that your infrastructure will be compromised. By adopting a least privileged approach to role assignments and utilizing multi-factor authentication, you can mitigate the risks associated with compromised credentials. Machine learning technologies can further enhance security by predicting the legitimacy of user access attempts.

In the event of a breach, having well-designed and implemented security protocols can prevent or limit the damage. Network segmentation and security zones can isolate critical elements, hindering the lateral movement of attackers. A zero-trust model, where cloud firewall policies default to deny all connectivity, can be adjusted to provide essential services with minimal access required.

Early detection is key to managing threats effectively. Services like TierPoint's XDR are designed to identify potential threats and recommend appropriate responses. A dual approach that combines preventative measures with early threat detection and remediation offers a more robust defense than focusing on a single aspect of security.

To further bolster your security posture, consider the following tools and strategies:

- Antivirus software to detect and remove malicious programs.
- Intrusion Detection/Prevention Systems (IDS/IPS) for monitoring network traffic and preventing attacks.
- Next-Generation Firewalls (NGFW) for advanced network security features.
- Email security solutions to protect against phishing and other email-based threats.

Backups, Replication and Disaster Recovery Plans

Having a secure and validated data backup program is the easiest way to avoid having to risk paying to decrypt files rendered unusable by crypto-ransomware. It's important that your backup and replication plan meets the unique needs of your organization to ensure business continuity. This could exist on the spectrum anywhere from data durability to disaster recovery.

- **Data durability** – Data is needed for compliance or archiving, but might not ever be touched
- **Data protection** – Data or applications need to be restored, but recovery time objectives (RTO) can be longer (perhaps one day)
- **Disaster recovery** – Data recovery needs are urgent, with RTO/RPO of minutes to seconds

Whether your systems go down due to power loss, user error, natural disaster or ransomware, the result can be devastating. The best disaster recovery plans combine backup and replication, ensuring comprehensive data protection and preparation. Backups provide good long-term storage but are limited to the snapshot of data stored at the time of the backup. Replication can meet much lower recovery time (RTO) and recovery point objectives (RPO). Replication runs a mirror image of your data operations and can take over at the moment of failure. Failover to a replicated site can keep a business running with little to no downtime. Regular failover testing is essential to ensure your systems will return to production levels in the timeframe and with the data quality desired after a ransomware attack.

Managed Disaster Recovery as a Service (DRaaS) goes beyond traditional disaster recovery. DRaaS manages a variety of backup and replication systems—in the cloud, co-located and in your own data center—unifying all under a common interface to reduce complexity and improve resilience when you need to restore or failover.

"Having a secure and validated data backup program is the easiest way to avoid having to risk paying to decrypt files rendered unusable by ransomware."

Don’t Let Ransomware Hold Your Business Hostage. It’s Time to Act

In an era where ransomware attacks are not just a possibility but a prevalent threat, safeguarding your business’s data and operations is more critical than ever. TierPoint stands at the forefront of ransomware defense, offering comprehensive disaster recovery and security services designed to outmaneuver these malicious threats before they strike.

Why TierPoint is Your Shield Against Ransomware

- **Proven Expertise:** With a team of certified professionals who have a track record of hundreds of successful disaster recovery implementations and declarations, TierPoint equips your business with the knowledge and tools to stand resilient against ransomware attacks. Our continuous replication and encryption-resistant technologies ensure that your operations can be restored within minutes, minimizing downtime and data loss.

- **Advanced Security Measures:** Our suite of security services, including vulnerability management, next-generation firewalls (NGFW), extended detection and response (XDR), and email security, acts as a formidable barrier against ransomware. By managing detection responses based on user anomalies and conducting thorough risk assessments, we tailor a security strategy that fortifies your defenses.

- **Security-First Approach:** At the heart of our operations is a dedicated cybersecurity team, led by an experienced Chief Information Security Officer (CISO) and supported by cutting-edge AI tools. Our proactive 24/7 monitoring and response capabilities ensure that potential ransomware threats are identified and neutralized before they can cause harm. With TierPoint, you benefit from our partnerships with leading technology providers and our compliance-ready data centers, ensuring a security posture that meets and exceeds industry standards.

- **Compliance and Certification:** Our commitment to security is underscored by our adherence to rigorous certifications and attestations, including ISO 27001, SOC 1&2, HIPAA, NIST, PCI, and more in our 40 state-of-the-art data centers. This not only demonstrates our dedication to maintaining the highest security standards but also provides you with the assurance that your data is in safe hands.

Resources

Disaster Recovery as a Service Solutions Brief:
http://www.tierpoint.com/wp-content/uploads/2016/11/SOLUTIONS-BRIEF-DRaaS1.pdf

FBI Ransomware Prevention and Response for CISOs:
https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

PBS Newshour: Why ransomware attacks are on the rise - and what can be done to stop them
https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them

Federal Government Resource: How to Protect Your Networks from Ransomware
https://www.justice.gov/criminal-ccips/file/872771/download

SonicWall: Cyber Threat Report
https://blog.sonicwall.com/en-us/2021/03/sonicwall-exposes-soaring-threats-historic-power-shifts-in-new-report/

FBI: 2019 Internet Crime Report
https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf

FBI: 2020 Internet Crime Report
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Cofense – Annual State of Phishing Report 2021
https://cofense.com/wp-content/uploads/2021/02/cofense-annual-report-2021.pdf

CISA Ransomware Guide - September 2020
https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

ABC News: The Latest: UN warns cybercrime on rise during pandemic
https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542

M-Trends 2021: Fireeye Mandiant Services Special Report
https://content.fireeye.com/m-trends/rpt-m-trends-2021

Help Net Security: IoT malware attacks rose 700% during the pandemic
https://www.helpnetsecurity.com/2021/07/20/iot-malware-attacks-rose/

ThreatPost: Ransomware Attack Foils IoT Giant Sierra Wireless
https://threatpost.com/ransomware-iot-sierra-wireless/165003/

IDC Survey Finds More than One Third of Organizations Worldwide Have Experienced a Ransomware Attack or Breach – August 2021
https://www.idc.com/getdoc.jsp?containerId=prUS48159121

A Third of Global Companies Have Experienced Ransomware Attack, Survey Finds – VICE August 2021
https://www.vice.com/en/article/jg84q3/a-third-of-global-companies-have-experienced-ransomware-attack-survey-finds

How Much Does a Data Breach Cost? – IBM 2021
https://www.ibm.com/security/data-breach

Ransomware: The True Cost to Business – Cyberreason 2021
https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf

SentinelOne: Global Ransomware Study 2018
https://go.sentinelone.com/rs/327-MNM-087/images/Ransomware%20Research%20Data%20Summary%202018.pdf

Sophos: The State of Ransomware 2021
https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

Talk to us today.

The threat of ransomware is ever-present, but with TierPoint, you have a partner that's fully equipped to protect, detect, and recover from these attacks. Don't wait until it's too late to take action against ransomware.

Call: 877.859.TIER (8437)

E-mail: sales@tierpoint.com

Visit: tierpoint.com

About TierPoint

TierPoint (tierpoint.com) is a leading provider of secure, connected IT platform solutions that power the digital transformation of thousands of clients, from the public to private sectors, from small businesses to Fortune 500 enterprises. Taking an agnostic approach to helping clients achieve their most pressing business objectives, TierPoint is a champion for untangling the complexity of hybrid, multi-platform approaches to IT infrastructure, drawing on a comprehensive portfolio of services, from public to multitenant and private cloud, from colocation to disaster recovery, security, and more. TierPoint also has one of the largest and most geographically diversified U.S. footprints, with dozens of world-class, cloud-ready data centers in 20 markets, connected by a coast-to-coast network.