SECURANCE CONSULTING

the advantage of insight

THE RISE OF RANSOMWARE AND THE PITFALLS OF POOR SECURITY

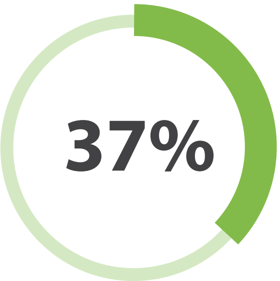
www.securanceconsulting.com

INTRODUCTION

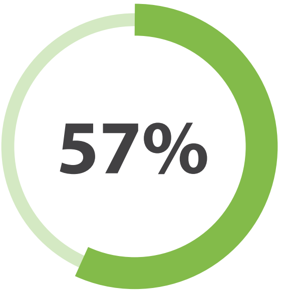
Imagine having to pay hundreds of thousands of dollars to access data you already own. This is what ransomware does by encrypting computer systems and rendering data inaccessible. Malicious hackers exploit data owners by promising to restore access after a ransom is paid— and threatening to destroy or leak data if their demands are not met. This form of cyber attack puts the victim between a rock and a hard place; there's no guarantee that, once the ransom is paid, the stolen data will be returned.

Given the above, it's no wonder ransomware is on the rise. Cyber criminals have nothing to lose and everything to gain in this situation. Even if the bad actor is unsuccessful in eliciting payment from one target, they simply move on to the next, while the victims are left to scramble for a solution.

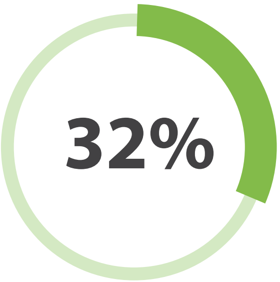
2022 Ransomware Statistics



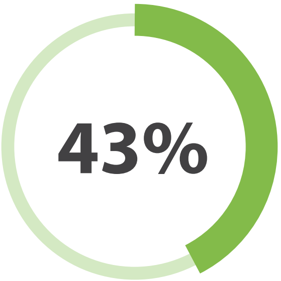
37% of all businesses were hit by ransomware



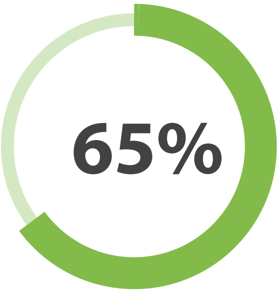
57% of companies recovered their data using cloud backup solutions



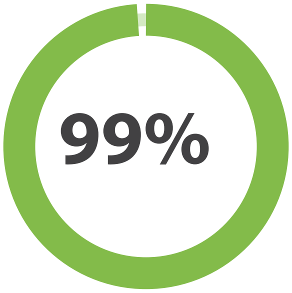
32% of victims paid the ransom



Ransom demands went up by 43%



Paying victims recovered only 65% of their data



Downtime costs due to ransomware increased by 99%

Cloudwards, 2022[1]

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software, or malware, that prevents organizations from accessing computer files, systems, or networks and demands that a ransom be paid for their return.[2] Ransomware continues to be the most prevalent form of malware. Bad actors continuously adjust their tactics to increase their payouts, and so that the effects become increasingly detrimental. This can include threatening to release stolen data if the business refuses to pay, publicly naming and shaming victims, and deleting system backups that make recovery infeasible for the organization.[3]

Types of Attacks

The ransomware landscape continues to grow each year, and 2022 is no exception. Below are examples of recent ransomware attacks that dealt considerable damage to organizations of all backgrounds.

1 **Nvidia—** In February of 2022, the world's largest semiconductor chip company, Nvidia, was the target of an attack by the ransomware group Lapsus$, which leaked employee credentials and proprietary information online. Nvidia's internal systems were also compromised, and this forced them to take some parts of the business offline for two days. Lapsus$ claimed they had access to 1 terabyte of company data and demanded a $1 million ransom from Nvidia.

Fortunately, Nvidia was able to respond immediately by executing its incident response plan, and did not pay the ransom.

> Ransomware strains don't stop evolving and often become more dangerous and sophisticated over time. Every organization must invest in ransomware readiness and mitigation strategies if they want to protect themselves from the heavy costs of an attack.

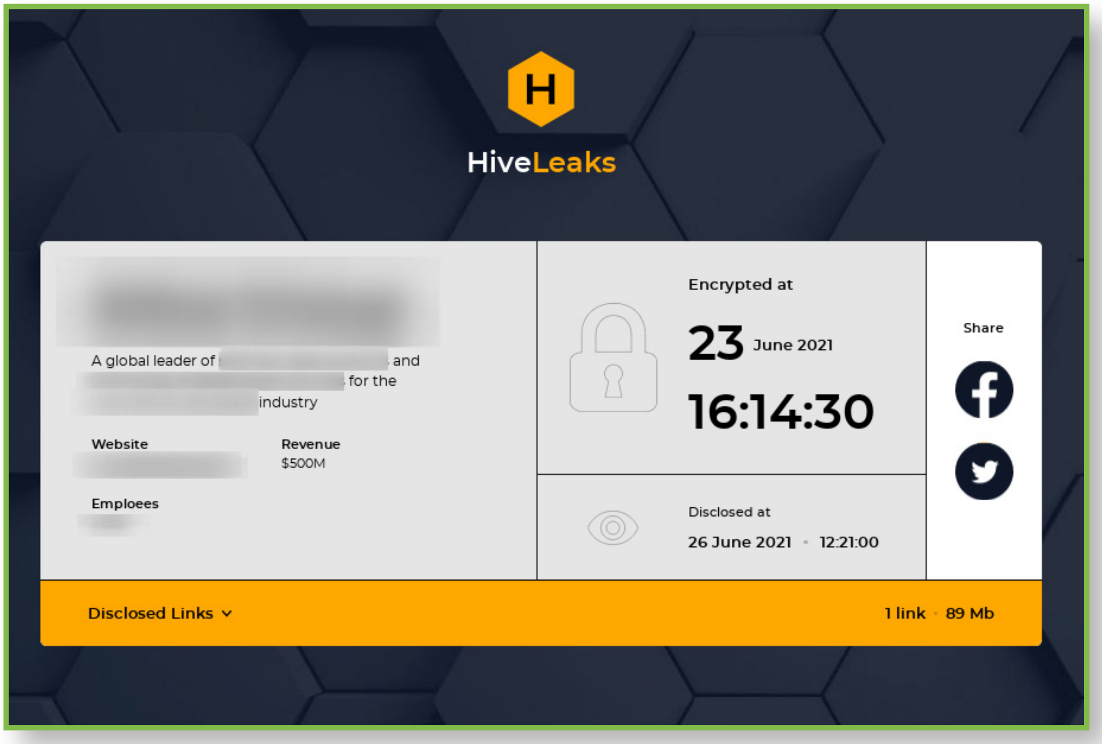
2 **Bernalillo County, New Mexico—** Bernalillo County, the largest county in New Mexico, experienced a crippling ransomware attack that took down several county departments and government offices, including the jail. Security cameras, automatic doors, and electronic locking systems were completely disabled.

Who instigated the attack and how much they demanded are still unknown. But, this incident demonstrated that ransomware can impact a variety of departments, functions, and systems within a single organization, rendering critical technologies useless and causing severe distress in a short amount of time.

3 Costa Rican Government— In 2022, Costa Rica became the first country to declare a national emergency in response to a cyber attack. The government was hit by a series of ransomware attacks, the first of which was launched by the Conti ransomware group. Conti demanded $10 million to restore critical operations and later increased their ransom to $20 million.

The second major attack came from the Hive ransomware group, which took down the Costa Rican social security fund. This attack took the country's healthcare systems offline and prevented nearly every citizen from accessing vital healthcare resources.[4]

Hive Leaks Ransomware Victim Information Sample



HiveLeaks

[redacted]

A global leader of [redacted] and [redacted] for the [redacted] industry

Website [redacted]

Revenue $500M

Emploees [redacted]

Encrypted at

23 June 2021

16:14:30

Disclosed at

26 June 2021 · 12:21:00

Disclosed Links

1 link · 89 Mb

Hornet Security, 2021[5]

The attacks described above show that organizations of any size are susceptible to ransomware, and the effects can be disastrous. Entire countries and critical operations can be dismantled by ransomware attacks, especially if the proper resources and incident response processes are not in place.

CHALLENGES

Paying the Ransom

Within the last 12 months, 63 percent of organizations in the United States that were infected by ransomware paid the ransom.[6] Many experts (and law enforcement agencies) discourage companies from paying, because hackers may keep the stolen data and demand additional payments. However, many businesses still decide to pay up—typically, as a last resort. For example, companies that provide essential services or have lost confidential and sensitive intellectual property may have no other choice.[7] To avoid this dilemma in the first place, organizations should prevent ransomware infections through user education and prepare to respond to successful attacks.[8]

The Internet of Things (IoT)

Technology makes life more convenient. Interconnected technology builds on that convenience but also creates more openings for malicious actors to exploit. On their own, IoT devices are unlikely to cause an attack with far-reaching consequences, but, when connected in a larger ecosystem, their individual vulnerabilities can form an exploitable chain that leads into other systems or networks. Each device's security depends on manufacturer and user diligence. Without proper security, the IoT is more a criminal's playground than a personal convenience.

> **2.8 billion** malware attacks were recorded in the first half of 2022, and there was a **77% rise** in IoT-specific malware — the first escalation of global malware volume in more than three years.[9]

Anonymous Payment Transactions

The popularity of Bitcoin and other cryptocurrencies has also exacerbated ransomware attacks. Although Bitcoin payments are public record, the "wallets" they funnel into can still be anonymous, making it very difficult for law enforcement to track transactions. With the wide array of broker services available today, victims can pay ransoms in a snap. Using ransomware means attackers don't have to monetize stolen data to quickly turn a profit and evade detection.

Human Error

It only takes one employee to open a malicious email's file attachment or click a link to download ransomware or an exploit kit. Phishing emails are the main distribution vehicle for ransomware. With botnets spamming millions of emails a day, chances are that a percentage will be opened and start a chain of undesirable, and potentially costly, events.

For the individual, third-party mobile apps and SMS messages are cause for concern. Malicious downloads pose as convenient apps, such as video players or mobile game plugins, and lock users' phones until a ransom is paid. Both Android and iOS devices can be compromised, which makes it critical for users to only download software from official stores, like Google Play and the Apple App Store.

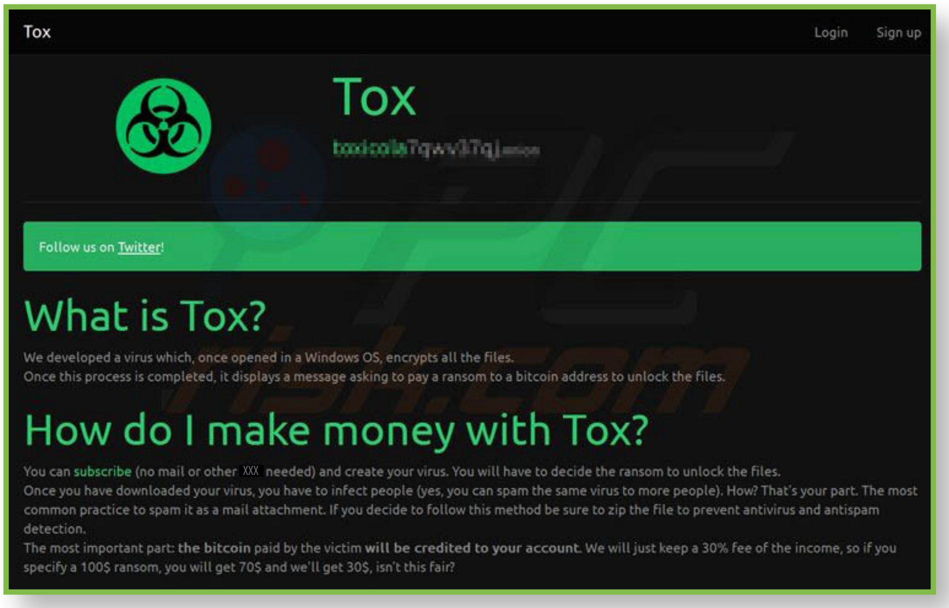
Ransomware as a Service (RaaS)

RaaS is an illegal business model in which affiliates pay to launch ransomware attacks developed by operators. RaaS is essentially a rogue version of Software as a Service (SaaS), a hosted software delivery model in which users pay a subscription fee to access specific services or applications. RaaS allows affiliates lacking the skill or time to develop their own ransomware variants to be up and running quickly and inexpensively. Possibly the most concerning aspect of RaaS is that it is actively marketed on the dark web and has a structured business model.

As if ransomware weren't an easy enough payday, RaaS enables enterprising cyber criminals to sit back, let others handle the dirty work for them, and still get paid. The four most common RaaS revenue models include:

- Monthly subscription for a flat fee
- Affiliate programs (monthly fee model, but with a percent of the profits going to the ransomware developer)
- One-time license fee with no profit sharing
- Pure profit sharing[10]

Below is an example of an advertisement for Tox ransomware. Its similarity to a reputable company's marketing strategy indicates this service is more sophisticated and organized than typical malware attacks.



Tox

[redacted]

Follow us on Twitter!

What is Tox?

We developed a virus which, once opened in a Windows OS, encrypts all the files.
Once this process is completed, it displays a message asking to pay a ransom to a bitcoin address to unlock the files.

How do I make money with Tox?

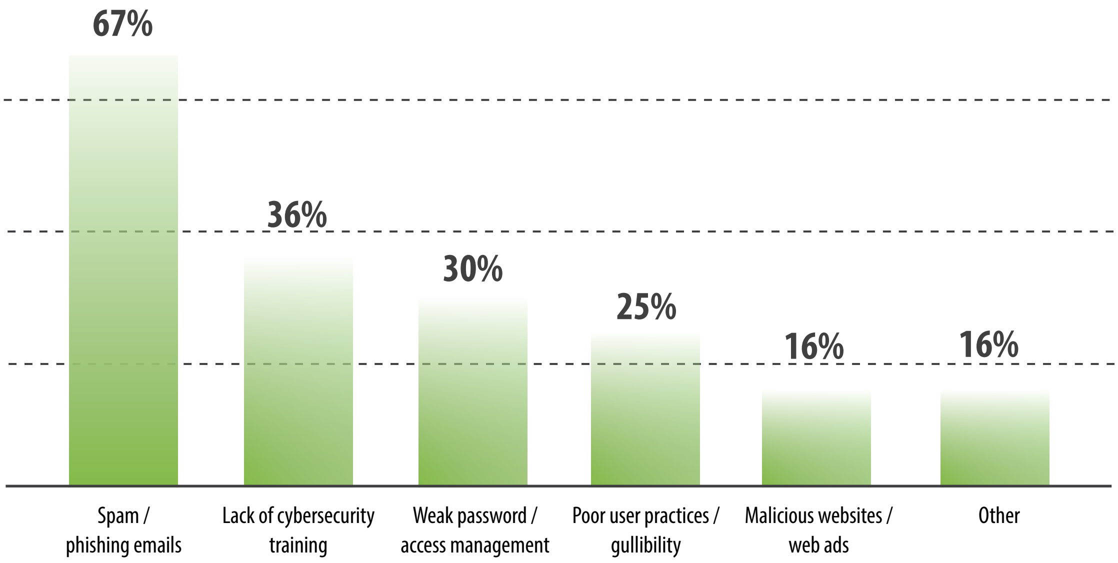
You can subscribe (no mail or other XXX needed) and create your virus. You will have to decide the ransom to unlock the files.
Once you have downloaded your virus, you have to infect people (yes, you can spam the same virus to more people). How? That's your part. The most common practice to spam it as a mail attachment. If you decide to follow this method be sure to zip the file to prevent antivirus and antispam detection.
The most important part: **the bitcoin** paid by the victim **will be credited to your account**. We will just keep a 30% fee of the income, so if you specify a 100$ ransom, you will get 70$ and we'll get 30$, isn't this fair?

Zvelo, 2022[11]

SOLUTIONS

The latest versions of ransomware require organizations to adopt multi-layered, comprehensive security solutions. Fortunately, even if your organization falls victim to ransomware, there are ways for your business to recover with minimal damage.

Most Common Ransomware Infection Methods in North America



Safety Detectives, 2022[12]

Email and Link Verification

Be mindful when opening emails and clicking directly on links, even if the sender appears to be someone you know. Check for typos, misspellings, or a mismatch between the sending email and website domains. Because ransomware often stems from malicious emails, it is wise to prevent them from traveling through the network in the first place. Creating a real-time block list (RBL) or spam uniform resource identifier real-time block list (SURBL) will enable an organization to scan incoming emails and identify spam before it reaches its intended destination.

Update and Maintain Malware Protection Services

In addition to regularly patching software and firmware, your organization should install antivirus software, firewalls, intrusion detection and prevention systems (IDS | IPS), and email filters. Trusted third-party software vendors frequently release patches that you can either install manually or automatically by setting up automatic updates on your device. While these programs are not free, they are well worth the investment and can save businesses millions in the long run.

User Security Awareness Training

Security awareness is one of the best ways to prevent ransomware attacks and cyber incidents. Organizations should institute formal awareness programs and hold regular cybersecurity training sessions to ensure their personnel are informed about current threat actor techniques, such as phishing, vishing, and smishing. An effective program should provide real-world training and educational materials, reinforced through management buy-in, open communication, and consistent follow-through. In addition to an established program, conducting periodic social engineering simulations will confirm your users' awareness and knowledge.[13]

> “In the past, attackers would simply force companies to pay a ransom to unlock data. Today, **70%** of occurrences employ double extortion tactics, where attackers steal sensitive information to coerce companies to pay even more. If payment isn't made, the attackers leak the data onto the dark web.”[14]

Securing the IoT

If we don't want our fixation with convenience to lead us to ruin, we must continue to focus on IoT security. Maintaining network visibility, segmenting devices from other networks, and monitoring, inspecting, and enforcing security policies are all necessary to protect against ransomware and cyber attacks.

Data Backups

Perform frequent backups of systems and important files, and verify backups regularly. If your network becomes infected with ransomware, you can restore systems to their previous states using backups. However, backups will not be helpful if they are compromised. The best practice is to store backups separately using an enterprise cloud backup service or external hard drive, that cannot be accessed from the network.

Incident Response Planning

An incident response plan (IRP) can save resources, time, and costs following a ransomware attack, as long as proper policies and procedures are in place, and staff are adequately trained. IRPs should be tested and updated regularly via tabletop and functional exercises. Besides revealing gaps in an IRP, tabletop exercises help improve response times and adherence to policies. The great news is that they are typically a low-cost service— with a big impact.

CONCLUSION

An Ounce of Prevention is Worth a Pound of Cure

At the end of the day, the best defense against ransomware is prevention. Delete suspicious emails, don't click on links or ads on untrusted websites, and test your incident response plan routinely. For businesses, enterprise-wide education is integral to increasing user awareness about social engineering techniques, such as phishing, vishing, and smishing. Even if a company implements the appropriate technical security measures, an uninformed employee could fall prey to an attack that slips through the cracks.

Although ransomware is growing more sophisticated, savvy organizations can be proactive about securing their systems by conducting routine security assessments, ensuring all software is up to date, and instating reliable processes for backing up critical data and responding to events or incidents before they become costly mistakes.

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://www.cloudwards.net/ransomware-statistics/
2. https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware
3. https://www.cisa.gov/stopransomware/ransomware-faqs
4. https://www.cm-alliance.com/cybersecurity-blog/5-major-ransomware-attacks-of-2022
5. https://www.hornetsecurity.com/en/threat-research/email-threat-review-june-2021/
6. https://www.helpnetsecurity.com/2022/04/06/organizations-successful-ransomware-attacks/
7. https://www.linkedin.com/pulse/6-reasons-pay-ransom-ransomware-attack-dale-shulmistra/
8. https://www.infosecurity-magazine.com/opinions/paying-ransom-option-should-done
9. https://www.sonicwall.com/2022-cyber-threat-report/
10. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
11. https://zvelo.com/raas-ransomware-as-a-service/
12. https://www.safetydetectives.com/blog/ransomware-statistics/
13. https://www.cisa.gov/uscert/ncas/tips/ST19-001
14. https://www.appuntidallarete.com/the-cost-of-ransomware-attacks-why-and-how-you-should-protect-your-data/

The Rise of Ransomware and the Pitfalls of Poor Security

S|C SECURANCE CONSULTING
the advantage of insight

13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com