The Tech chronicle

Start Fighting Cyber Crime with Knowledge and Action.

Sirtawn Systems

Our Newsletter for Issue #170 is dedicated to Ransomware.

Your Ransomware Survival Guide

What is ransomware?

Ransomware is a type of malware, or malicious software, that hackers launch to disable or limit an organization's access to its data until a ransom is paid. The hackers then instruct the organization on how to pay the ransom in order to release the decryption key that will allow the company to decrypt the data and potentially gain access to its files, databases and applications. Ransomware attacks are increasing rapidly, generating substantial revenue for cybercriminals and causing significant damage to businesses and government bodies. Attack groups are constantly adapting and evolving their tactics, devising new ways to extort ransom from victims. As long as these gangs can extort payment from businesses, ransomware attacks will continue to escalate. To combat this, businesses like yours need to develop a solid cyber defense strategy to minimize the risk and mitigate the impact of ransomware so that they can recover quickly if their systems are compromised.

Top attack vectors (Methods)

When you understand how ransomware attacks work, including the vectors and avenues used by bad actors, you can lower your chances of falling victim to them. Listed below are a few popular attack vectors hackers use to launch ransomware:

Email phishing

Email phishing is a social engineering attack designed to entice targets into clicking on a link in an email that leads to a hacker gaining access to your network or sensitive information. In most cases, attackers are interested in stealing account credentials, personally identifiable information (PII) and company trade secrets.

Unsecured RDP ports

Hackers gain direct access to a server or computer by scanning the network and discovering open RDP ports that have not been adequately secured. Attackers aim to gain complete control over a system, obtain credentials or unleash malicious code on a target.

Software/patching vulnerabilities

Software vulnerability is a flaw or weakness in software that compromises the overall security of the system. A data breach or system attack can easily cost businesses millions of dollars in compromised files, operational challenges, and system fixing and maintenance

Malicious websites

Cybercriminals create malicious websites to steal sensitive data or plant malware, such as ransomware, on victims' computers. These websites often spoof legitimate sites and lure visitors with phishing.

Pop-ups/ads

Pop-ups may appear in your browser due to adware that you might have accidentally downloaded, possibly by clicking a malicious advertisement. Another possibility is opening an attachment or clicking on a link in an email containing adware.

Sirtawn Systems

Your Cyber Security Experts

Top ransomware trends

Ransomware gangs continuously rethink and upgrade their techniques as new technologies emerge and more businesses try to protect themselves against attacks. Here are a few of the latest techniques ransomware gangs and their affiliates use to target their victims:

Supply chain attacks

To maximize the attack radius and impact, threat actors target weak links in supply chains, threatening not only a single business but also an organization's entire ecosystem.

Double extortion

Hackers not only encrypt the data, but also steal it and threaten the victim to release it unless a ransom is paid. Sometimes releasing it regardless of payment and in many instances, the victim never gets their data returned to them.

Ransomware-as-a-Service

Affiliates secure access to a subscription-based platform that contains all the ransomware code and operating infrastructure needed to run ransomware attacks.

Increased attacks against small and midsize businesses

After several high-profile indictments of cybercriminals who got caught, law enforcement agencies have seen a shift in criminal behavior from high profile hacking to targeting midsized businesses to evade public scrutiny.

Impacts of a successful attack

The aftereffects of a ransomware attack can be devastating for your business in multiple ways, including:

Extended downtime:

It doesn't matter whether you have paid the ransom or not — a ransomware attack can paralyze your entire business operations for hours, days or weeks, resulting in long-term disruption. Long downtimes can adversely affect your revenue through missed opportunities, production shortages and service outages.

Lost files, wages and equipment

If you don't have proper backup solutions, there is a high probability that you will lose files entirely during ransomware attacks. Plus, you'll have to pay lost wages for employees who are no longer productive as well as wipe and rebuild equipment such as laptops, desktops and servers.

Additional costs

Businesses can incur considerable IT fees for labor, recovery services and hardware replacement when they attempt to restore data or clean up after a ransomware attack.

Damaged reputation and loss of customers

A ransomware attack can significantly damage your company's reputation. It could even leak your existing clients' sensitive data, making it difficult to not just retain existing customers, but also to secure new clients

Regulatory fines

You could be subject to regulatory fines if sensitive customer data is compromised in the attack. You might also be held liable for direct compensation from your clients, putting your business at risk for substantial financial hardship.

Best practices to protect your business from ransomware attacks

The Canadian Centre for Cyber Security recommends the following precautions to shield users against today's sophisticated ransomware threats:

» Hackers can easily exploit vulnerabilities in outdated applications and operating systems because they have more attack surface areas. Update your software and operating systems with the latest patches to stay ahead of threats.

» A standard tactic hackers use to launch ransomware attacks is sending phishing emails with malicious links or attachments. Never click on links or attachments in unsolicited emails.

» Keep your backups safe by taking them offline and ensure they are malware-free.

» To reduce the risks associated with online browsing and remote connections to your network, ensure your employees are aware of security best practices and maintain cyber hygiene.

More best practices include:

» Anti-phishing and email security protocols and tools
Utilizing the right tools to identify and protect against incoming emails should be your first step in preventing ransomware phishing emails.

» Security awareness training
Provide ongoing cybersecurity awareness and training programs for your employees, partners and stakeholders so that they are updated with the latest threats and security best practices.

» Vulnerability scanning
With automated internal and external vulnerability scanning, you can find vulnerabilities in your network and generate a detailed report for remediation before hackers find them.

» Patch management
An automated patch management tool can keep your systems up to date with the latest security patches and bug fixes.

» Endpoint detection and response
Endpoint detection and response (EDR) software detects and blocks ransomware before it infects endpoints, networks and cloud services.

» Network monitoring
Use network monitoring tools to keep track of all your infrastructure components, performance metrics (CPU, memory, disk space, uptime), processes, services, event logs, and application and hardware changes.

» Network segmentation
You can categorize your organization's network into smaller, distinct sub-networks, allowing your network teams to compartmentalize the subnetworks and provide unique security controls and services to each.

» Identity and access management
Identity and access management (IAM) secures your critical assets by ensuring that team members only have access to the tools they need to do their jobs.

» Strong password policies/good password hygiene
Using multifactor authentication (MFA) and maintaining strong password policies prevents credentials from being compromised. Also, the policy should emphasize that Users DO NOT use the same password for multiple applications.

How to respond to a ransomware attack

As ransomware attacks increase in number and severity, you need to know how to respond in the event of a successful attack. According to the Canadian Centre for Cyber Security, here are a few best practices you should follow in the event of a ransomware attack:

» Find out which systems have been compromised and through which attack vector.

» Know the infection status, network topology and virtual currency address provided for payment.

» Do not turn off or shut down any ransomware-affected systems.

» Isolate the infected device and compromised network area immediately.

» Change online account and network passwords right away.

» Gather all available log information.

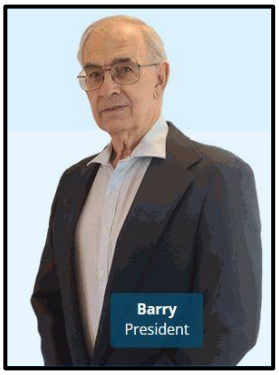
» Check if any domains or IP addresses were communicated right before the attack.

» Use your oldest backup to recover data.

» Employ out-of-band communication techniques and don't place your trust in the entire network.

» Check if any files were dropped onto your system or if any memory captures were taken.

The chances of you falling victim to a ransomware attack are the same as those of any other company. If it happens to you, will you be able to recover fully?



This monthly publication provided courtesy of Barry Brown, President of Sirtawn Systems.

FIGHTING CYBERCRIMINALS ON YOUR OWN CAN BE TIRING WHEN YOU HAVE A BUSINESS TO RUN.

CONTACT US TODAY

FIND OUT WHAT IT'S LIKE TO HAVE OUR CYBERSECURITY EXPERTS IN YOUR CORNER.

We are offering a FREE Network Security Audit with no obligation. You will receive a "Cyber Security Audit" outlining our findings following the audit. Again … **NO Obligation.**++

Sirtawn Systems

Your Cyber Security Experts

Phone: (905) 947-1636
Website: www.sirtawn.com