# **Ransomware Playbook**

## **Actions you can take to lower the risk and impact of this kind of attack.**

Summary

[**Ransomware Playbook**](#_heading=h.gjdgxs) **0**

[**Actions you can take to lower the risk and impact of this kind of attack.**](#_heading=h.30j0zll) **0**

[**What is Ransomware?**](#_heading=h.3znysh7) **2**

[**Should you pay the ransom?**](#_heading=h.2et92p0) **3**

[**Typical delivery methods**](#_heading=h.tyjcwt) **5**

[**How have attackers changed?**](#_heading=h.3dy6vkm) **6**

[**Ransomware Guide**](#_heading=h.1t3h5sf) **7**

[**Importance of having a Incidente Response Plan**](#_heading=h.4d34og8) **8**

[**Incident response plan checklist**](#_heading=h.2s8eyo1) **8**

[**Develop your recovery plan**](#_heading=h.17dp8vu) **9**

[**Ransomware Protection – Tips to Prevent Ransomware Attacks (CrowdStrike)**](#_heading=h.3rdcrjn) **11**

[**Develop your backup plan**](#_heading=h.26in1rg) **16**

[**Cyber security controls**](#_heading=h.lnxbz9) **16**

[**Establish perimeter defences**](#_heading=h.35nkun2) **17**

[Zscaler Ransomware Protection](#_heading=h.sbtbt2lgvh31) 17

[Implement logging and alerting](#_heading=h.1n291ahq1udz) 19

[Conduct penetration testing](#_heading=h.xmpz39t0k4vg) 19

[Segment your networks](#_heading=h.zkvnr9l495x) 19

[Constrain scripting environments and disable macros](#_heading=h.6zvxubre4j7q) 20

[Patch and update](#_heading=h.ftq2napvhtyz) 20

[Use protective domain name system (DNS)](#_heading=h.qqg9rfwff3ol) 20

[Apply password management](#_heading=h.1jgn5trjytas) 21

[Use email domain protection](#_heading=h.uz7c6p5473kc) 21

[**How to recover from ransomware**](#_heading=h.1ksv4uv) **22**

[**Recovery actions**](#_heading=h.44sinio) **22**

[**Remediate the point of entry**](#_heading=h.2jxsxqh) **22**

[**Implement your backup plan**](#_heading=h.z337ya) **22**

[**Restore your systems**](#_heading=h.3j2qqm3) **22**

[**Engage cyber security professional assistance**](#_heading=h.1y810tw) **23**

[**Inform stakeholders**](#_heading=h.4i7ojhp) **23**

[**Analyze the incident**](#_heading=h.2xcytpi) **23**

[**List of abbreviations**](#_heading=h.1ci93xb) **23**

[**References**](#_heading=h.3whwml4) **24**

## 

## **What is Ransomware?**

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation’s state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Malicious actors continue to adjust and evolve their ransomware tactics over time, and the U.S. Government, state and local governments, as well as the private sector remain vigilant in maintaining awareness of ransomware attacks and associated tactics, techniques, and procedures across the country and around the world.

Diagrama

Descrição gerada automaticamente

When ransomware infects a device, it either locks the screen or encrypts the files, preventing access to the information and systems on your devices. Threat actors can also use your compromised network to spread the ransomware to other connected systems and devices.

Your networks and devices can be infected with ransomware in the following ways:

Visiting unsafe, suspicious, or compromised websites (known as a drive-by download);

Opening emails or files from familiar or unfamiliar sources (phishing);

Clicking on links in emails, social media, and peer-to-peer networks;

Inserting an infected peripheral device (e.g. USB flash drive) into a device; or,

Exposing your systems to the internet unnecessarily or without robust security and maintenance measures, such as patching vulnerabilities and multi-factor authentication (MFA) in place.

If your device is infected with ransomware, you will receive a notice on your screen indicating your files are encrypted and inaccessible until the ransom is paid. You may also receive a message on your lock screen indicating your device is locked and inaccessible until the ransom is paid. The message will instruct you to pay a ransom to unlock the device and retrieve the files. Payment is often requested in the form of digital currency, such as bitcoin, because the transfer would be more difficult to trace. Prepaid credit cards or gift cards may also be requested. You will be provided with a time limit to pay the ransom, after which threat actors may increase the ransom amount, destroy your files permanently, or leak your data. As an additional extortion method, a threat actor may threaten to release your data publicly if you do not pay the ransom.

### **Should you pay the ransom?**

The decision to pay a cyber threat actor to release your files or devices is difficult, and you may feel pressured to give in to their demands. Before you pay, contact your local police department and report the cybercrime. Paying the ransom does not guarantee access to your encrypted data or systems. Ultimately, the decision to pay the ransom is your organization’s to make, but it is important for your organization to be fully aware of the risks associated with paying the ransom. For example, threat actors may use wiper malware, which alters or permanently deletes your files once you pay the ransom. Payment may also be used to fund and support other illicit activities. Even if you pay, threat actors may still carry out the following actions:

* Demand more money;
* Continue to infect your devices or other organizations’ devices;
* Re-target your organization with a new attack;
* Copy, leak, or sell your data.

The following chart (Figure2) from the NCTA 2020 demonstrates the increase in the average ransom payment over the past few years. As Figure 2 demonstrates, after increasing rapidly from 2019 to 2020, known ransom payments appear to have stabilized around $200,000 in 2021, which is down slightly from levels seen in 2020. Ransom payments are likely reaching a market equilibrium, where threat actors are becoming better at tailoring their demands to what their victims are most likely to pay given the growth of recovery cost and the risk of reputational damage from public data leaks.

Gráfico, Histograma

Descrição gerada automaticamente

## **Typical delivery methods**

As the example above shows, the first step of any ransomware attack is to get the malware installed on the host system. This typically occurs using specific techniques for initial access:

• **Spear phishing** - where the victim receives an attachment or link that they click

• **Drive-by** - where an attacker can exploit a vulnerability in the web browser or related applications

• **Exploitation -** where an attacker can exploit a vulnerability and gain access to a remote system or allow the ransomware to propagate automatically

• **Replication through removable media** - this also includes networked media that ransomware encrypts at

the same time as it infects the victim

• **Valid accounts** - where an attacker has valid credentials to the target system and can authenticate to it

**Execution**

The adversary is trying to run malicious code.

Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

## **How have attackers changed?**

For many ransomware attacks in the past, threat actors employed mass spam campaigns to socially engineer users into clicking links or attachments. Once clicked, ransomware encrypted the system and, in an automated fashion, potentially encrypted other systems where access was established or allowed, such as a mapped file share. Increasingly over the past few years, there has been a shift to “big-game hunting” threat actors leveraging access established by taking advantage of poor security controls in an environment. Those controls can often be an unpatched externally facing server, unsecured remote access solutions, or an undetected banking trojan (such as TrickBot, Emotet, or Dridex). When access is gained, the threat actors go “hands on” using post-exploitation frameworks to recon the environment and gain elevated privileges. If a threat actor gains unfettered access to the environment, they can encrypt the network en masse (deploying Ryuk or BitPaymer), leading to complete disruption of business services. Many times this leads to ransomware taking down large healthcare centers and hospitals, manufacturing facilities, educational institutions, municipalities, and other corporations. These big-game hunting threat actors have continued to increase their ransom demands, which are now regularly exceeding seven figures. In addition to rendering the network unusable, some of these threat actors exfiltrate sensitive data and extort their victims by threatening to release the data. In this scenario, criminal groups are increasingly demanding two ransom payments: one for decrypting all the systems on the network and one for keeping the exfiltrated from attacker data sharing platforms. These types of attacks are known as “double extortion ransomware.” There is another emerging scenario of “triple extortion ransomware” whereby attackers infiltrate an organization, steal data, encrypt systems and then demand the traditional payment for decryption keys. If a victim organization refuses to pay, the attackers threaten to publicly release records either all at once, or piecemeal, until payment is made. With the release of data, the attackers then use customer, partner, and/or vendor information stolen from the victim to conduct denial of service attacks on those third-parties or contact those third-parties (to put payment pressure on the original victim organization), and demand smaller payments from these secondary victims to prevent their data from being included in any public release. Recent years have also seen the rise of the “ransomware as a service” (RaaS) business model, which provides ransomware capabilities to would-be criminals who do not have the skills or resources to develop malware on their own. This “as a service” model follows similar evolutions in the mainstream software and infrastructure industries, which have seen success from “software as a service” and “infrastructure as a service” business models.

## **Ransomware Guide**

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increased, with some demands exceeding US $1 million. Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small.

On September 30, 2020, a joint Ransomware Guide was released, which is a customer centered, one-stop resource with best practices and ways to prevent, protect and/or respond to a ransomware attack. CISA and MS-ISAC are distributing this guide to inform and enhance network defense and reduce exposure to a ransomware attack:

This Ransomware Guide includes two resources:

* **Part 1: Ransomware Prevention Best Practices**
* **Part 2: Ransomware Response Checklist**

CISA recommends that organizations take the following initial steps:

* Join an information sharing organization, such as one of the following:
  + Multi-State Information Sharing and Analysis Center (MS-ISAC): <https://learn.cisecurity.org/ms-isac-registration>
  + Election Infrastructure Information Sharing and Analysis Center (EI-ISAC): <https://learn.cisecurity.org/ei-isac-registration>
  + Sector-based ISACs - National Council of ISACs: [MEMBER ISACS | natlcouncilofisacs (nationalisacs.org](https://www.nationalisacs.org/member-isacs-3)
  + Information Sharing and Analysis Organization (ISAO) Standards Organization:[Information Sharing Groups – ISAO Standards Organization](https://www.isao.org/information-sharing-groups/)/
* Engage CISA to build a lasting partnership and collaborate on information sharing, best practices, assessments, exercises, and more:
  + SLTT organizations: [CyberLiaison\_SLTT@cisa.dhs.go](mailto:CyberLiaison_SLTT@cisa.dhs.go)v
  + Private sector organizations: [CyberLiaison\_Industry@cisa.dhs.gov](mailto:CyberLiaison_Industry@cisa.dhs.gov)
* Engaging with your ISAC, ISAO, and with CISA will enable your organization to receive critical information and access to services to better manage the risk posed by ransomware and other cyber threats.

## **Importance of having a Incidente Response Plan**

Ideally organizations want to avoid becoming the victim of ransomware attacks, and there are a number of steps that can be taken to reduce the risk and make the job harder for attackers, detailed below. These measures take time to implement though, and while they should make an organization harder to compromise and more able to recover from attack, no organization can be completely invulnerable. As such, it is critical to have a comprehensive incident response plan in place so that if the worst does happen, you are able to react quickly and efficiently to weather the storm.

It may seem counterintuitive to work on response before the incident, and even before deploying preventative measures, but we strongly recommend you do just that — develop and practice your incident response plan now. You need this in place while you work on your preventative measures so you will be prepared if you have an incident before you can fully implement your defenses. Without the proper preparation, an attack can bring your business to a grinding halt and put your critical information at risk

A comprehensive incident response program will incorporate the following:

1. Preparation - Are you ready if a ransomware attack happens? Do you have a playbook? Does your team know what to do and who is responsible?

2. Identification - What are your measures to identify ransomware before machines are encrypted and a message asks you to pay? How can you identify that an attack is taking place before ransomware is executed?

3. Containment - Do you have proper methods (or have automation workflows) in place to contain threats early in the attack chain? The earlier you’re able to contain the threat, the more likely you are to restrict the ability of an attacker to execute the ransomware.

4. Eradication - Can you eradicate the threat on your own, or do you have an Incident Response retainer set up in the event of a breach? Cleaning things up is one of the last things to do in a ransomware attack. Are you able to scope the incident thoroughly to understand what happened and prevent it from happening again? Do you have the expertise on staff to eradicate the threat completely, ensuring you’re not going to get encrypted in a week?

5. Recovery - Do you have proper measures in place to recover from an attack and get things back to normal as soon as possible?

6. Review Lessons Learned - What is your postmortem process? How can you use this as a lesson to improve your security posture?

### **Incident response plan checklist**

Developing an incident response plan for your organization is the keystone to your cyber defence strategy. You should also consider developing a disaster recovery plan for your business. Through these two plans, your organization considers major events that could cause an unplanned outage and require you to activate your recovery response. Your incident response plan helps you detect and respond to cyber security incidents. Your disaster recovery plan focuses on how the organization recovers and resumes critical business functions after an incident.

There are many benefits to developing an incident response plan:

* Effective incident management lessens the impact of a cyber incident;
* A practised plan will help you make good decisions under the pressure of a real incident;
* Key actions are approved in advance, allowing financial authorities and resources to be available in the immediate steps of your incident response;
* A well-managed response, with clear communication throughout, builds trust with shareholders and customers; and,
* Learning from incidents identifies gaps and issues with your response capability

Uma imagem contendo Texto

Descrição gerada automaticamente

### **Develop your recovery plan**

Your recovery plan should complement your incident response and backup plans. When developing your recovery response, you should consider many variables and clearly identify and document what is to be recovered, by whom, when, and where. Consider the following guidelines detailed in Table 2 when developing your recovery plan:

Texto

Descrição gerada automaticamente

To create an effective plan, you should identify your organization’s critical data, applications, and functions. Critical information may include financial records, proprietary assets, and personal data. Critical applications are the systems running your key business functions and are imperative to your business. These are the systems you need to restore immediately to have business continuity in the event of an unplanned outage or incident. You should consider conducting a risk assessment to help identify critical business functions and the relevant threat and vulnerability risks.

To ensure your response is effective, your organization should run through specific scenarios (e.g. cyber attack, significant power outage, or natural disaster) to help you identify key participants and stakeholders, address the significant risks, develop mitigation strategies, and identify the recovery time and effort. You can conduct a business impact analysis (BIA) to predict how disruptions or incidents will harm your operations, business processes, systems, and finances. During your BIA, you should also assess the data you collect and the applications you use to determine their criticality and choose priorities for immediate recovery. It is also critical to take note of your recovery efforts, documenting what went well and what areas require improvement.

## **Ransomware Protection – Tips to Prevent Ransomware Attacks (CrowdStrike)**

1. Practice Good IT Hygiene
2. Improve Resiliency of Internet Facing Applications
3. Implement and Enhance Email Security
4. Harden Endpoints
5. Ransomware-Proof Data with Offline Backups
6. Restrict Access to Virtualization Management Infrastructure
7. Implement an Identity and Access Management (IAM) Program
8. Develop and Pressure-Test an Incident Response Plan
9. Know When to Ask for Help

**1. Practice Good IT Hygiene**

Minimizing the attack surface is critical for every organization — it’s crucial that you gain visibility into every endpoint and workload running in your environment and then keep any vulnerable attack surfaces updated and protected.

IT hygiene’s primary benefit is to give you complete network transparency. This perspective provides a bird’s eye view, as well as the power to drill down and proactively clean out your environment. Once you achieve this level of transparency, the understanding of “who, what and where” that IT hygiene provides has tremendous benefits for your organization. You’re able to:

Identify gaps in your security architecture. The clarity that IT hygiene provides allows you to see what hosts are running on your environment and whether they are protected. Having complete visibility enables you to effectively deploy your security architecture and ensure no rogue systems are operating behind your walls. The larger and more distributed your environment becomes — such as with workforces going increasingly remote — the harder it is to have visibility across all of your endpoints and identities (including both human and service accounts). Identifying the unmanaged assets in your environment allows you to target vulnerabilities and protect your valuable assets before attackers can reach them.

See what is running in your environment. By proactively identifying outdated and unpatched applications and operating systems, you can manage your application inventory and solve security and cost problems simultaneously. Unpatched operating systems and applications have serious security and cost implications — make sure to identify which applications are running on your network and pinpoint unpatched apps to get ahead of attackers.

See who is running in your environment. Account monitoring allows you to see who is working in your environment and ensure they’re not violating their credential permissions (including detection of tools or behavior trying to subvert those policies). System administrators remain highly targeted, and combined with poor password renewal policies, credential theft is a harsh reality. With insight into password updates, you can prevent credential creep by removing old administrative accounts or making sure users update their passwords regularly. Taking this a step further, visibility into unusual admin behavior or privilege elevation can prevent silent failure by tipping off your security team as soon as something suspicious occurs.

Ensure user compliance. Making sure your users abide by your most up-to-date password policies keeps administrators and users compliant with your security requirements. Consistent and ongoing user education can ensure that password best practices are followed, and ridding your network of old accounts (including service accounts) can mitigate the risk of “credential creep” by former employees.

Add defense-in-depth. Implement real-time detection policies to monitor for anomalous credential behavior use, including detection of lateral movement even on workstations that may not have a Falcon agent installed. In addition, enable risk-based conditional access to trigger MFA for human and service accounts without adding burden to users, ensuring higher compliance.

Once you have full visibility and understanding of your environment, your organization can identify hygiene-related security deficiencies and resolve them immediately. From there, security teams can quickly pivot to address the critical elements of comprehensive endpoint protection: prevention, detection, hunting and threat intelligence. These capabilities are key to a complete solution that can protect your organization from the most motivated, sophisticated attackers.

**2. Improve Resiliency of Internet-facing Applications**

CrowdStrike has observed eCrime threat actors exploiting single-factor authentication and unpatched internet-facing applications. BOSS SPIDER, one of the initial big game hunting (BGH) ransomware threat actors, routinely targeted systems with Remote Desktop Protocol (RDP) accessible from the internet. Less sophisticated threat actors operating ransomware variants such as Dharma, Phobos and GlobeImposter frequently gain access through RDP brute-force attacks.

**3. Implement and Enhance Email Security**

Gaining an initial foothold into a victim organization through a phishing email is the most common tactic for BGH ransomware groups. Typically, these suspicious emails contain a malicious link or URL that delivers the ransomware payload to the recipient’s workstation.

CrowdStrike recommends implementing an email security solution that conducts URL filtering and also attachment sandboxing. To streamline these efforts, an automated response capability can be used to allow for retroactive quarantining of delivered emails before the user interacts with them. In addition, organizations may want to restrict users from receiving password-protected zip files, executables, javascripts or Windows installer package files unless there is a legitimate business need. Adding an “[External]” tag to emails originating from outside of the organization and a warning message on top of the email’s body can help remind users to use discretion when handling such emails.

**4. Harden Endpoints**

Throughout an attack lifecycle that ultimately culminates in a ransomware deployment, threat actors will often leverage a number of endpoint exploitation techniques. These exploitation techniques vary from exploiting poor AD configurations to leveraging publicly available exploits against unpatched systems or applications.

The list below includes some key system-hardening actions for defenders to implement. It is important to note this is not an exhaustive list, and system hardening should be an iterative process.

Ensure full coverage across all endpoints on your network for endpoint security products, and for the endpoint detection and protection (EDR) platform. Each endpoint security platform should have strict anti-tampering protections and alerting in place if and when a sensor goes offline or gets uninstalled.

Develop a vulnerability and patch management program. Doing so will ensure that all endpoint applications and operating systems are kept up-to-date. Ransomware actors leverage endpoint vulnerabilities for many purposes, including but not limited to privilege escalation and lateral movement. Existing Falcon customers can leverage CrowdStrike Falcon Spotlight™ vulnerability management for a near real-time way to understand exposure to a particular vulnerability across the environment, without the need to deploy additional agents and security tools.

Follow Active Directory security best practices. Based on some of the most common AD downfalls observed by CrowdStrike Services during ransomware engagements, we recommend these steps:

* Avoid easy-to-guess passwords with weak authentication methods.
* Avoid having regular domain users with local administrator privileges, and local administrator accounts with the same passwords across the entire enterprise or large portions of the enterprise.
* Limit workstation-to-workstation communication. While this can be achieved using group policy objects (GPOs), it can be also achieved through a number of micro-segmentation software options.
* Avoid sharing privileged credentials. Poor security practices include shared administrative accounts and using administrator accounts for personal or day-to-day business activity that does not require administrator privileges.
* Note that the first two points above can be accomplished using AD with little to no additional costs. At an additional cost, a privileged access management (PAM) solution can provide a much more scalable and robust solution to the same problem and is discussed more later in this blog post.

**5. Ransomware-proof Data with Offline Backups**

In recent years, and since the emergence of ransomware as a top method of monetizing attacks, the developers behind malicious code have become very effective at ensuring victims and security researchers cannot decrypt affected data without paying the ransom for the decryption key. Further, when developing a ransomware-proof backup infrastructure, the most important idea to consider is that threat actors have targeted online backups before deploying ransomware to the environment.

For these reasons, the only sure way of salvaging data during a ransomware attack is through ransomware-proof backups. For example, maintaining offline backups of your data allows for a quicker recovery in emergencies. The following points should be considered when developing a ransomware-proof offline backup infrastructure:

* Offline backups, as well as the indexes (describing which volumes contain which data) should be completely separate from the rest of the infrastructure.
* Access to such networks should be controlled via strict access control lists (ACLs), and all authentications should be performed using multifactor authentication (MFA).
* Administrators with access to both offline and online infrastructures should avoid reusing account passwords and use a jump box when accessing the offline backup infrastructure.
* Cloud storage services, with strict ACLs and rules, can also serve as offline backup infrastructure.
* Emergency situations such as a ransomware attack should be the only time the offline infrastructure is allowed a connection to the live network.

**6. Restrict Access to Virtualization Management Infrastructure**

As mentioned earlier, threat actors engaged in big game hunting ransomware campaigns are continuously innovating to increase the effectiveness of their attacks. The most recent such development includes the ability to attack virtualized infrastructure directly. This approach allows for targeting of hypervisors that deploy and store virtual machines (VMDK). As a result, the endpoint security products installed on the virtualized machines are blind to malicious actions taken on the hypervisor.

To further understand how this attack would unfold, we will use some of VMware’s naming convention as it is the most common virtualizing product found in today’s enterprise environments.

Many ESXi systems (VMware hypervisors) do not have Secure Shell (SSH) protocol enabled by default and are usually managed via vCenter. If SSH is disabled, previously stolen administrative credentials are used to enable SSH on all ESXi systems. Once that is complete, a valid account is used to SSH into each ESXi system being targeted. Before the threat actor deploys the Linux-based ransomware, VMDKs hosted on the ESXi are stopped to allow the ransomware binary to access the files for encryption purposes. Systems impacted by the ransomware through this deployment method will be completely offline and inaccessible to the users.

**7. Implement a Robust Identity Protection Program**

Organizations can improve their security posture by implementing a robust identity protection program to understand on-premises and cloud identity store hygiene (for example, Active Directory, Azure AD). Ascertain gaps, and analyze behavior and deviations for every workforce account (human users, privileged accounts, service accounts), detect lateral movement, and implement risk-based conditional access to detect and stop ransomware threats.

**8. Develop and Pressure-test an Incident Response Plan**

Organizations sometimes become aware of threat actor activity within their environment, but they lack the visibility to address the problem or the right intelligence to understand the nature of the threat. Recognizing the threat and responding quickly and effectively can be the difference between a major incident and a near miss.

Incident response plans and playbooks help facilitate that speedy decision making. Plans should cover all parts of the response effort, across the organization. For the security team, they should provide aids to decision-making so that front-line responders don’t overlook important details while triaging alerts. They should also outline the extent of the security team’s authority to take decisive actions — such as shutting down business-essential services — if a ransomware attack appears imminent.

For the crisis management team, plans should identify who will be involved and what their roles and responsibilities are. It should also tee up important decisions, like when to activate an incident response retainer, whether to notify insurance carriers, when and how to involve in-house or outside counsel, and how to discuss ransom demands with executives.

Consider conducting regular tabletop exercises to test the incident response plan and processes. Some organizations may benefit from simulated exercises such as “purple team” engagements, where red teamers mimic ransomware operators’ actions on objectives, including data exfiltration and ultimately ransomware deployment. CrowdStrike also recommends regular exercising of your incident response plan, both planned and unplanned, such as utilizing a red team to conduct a mock attack operation.

**9. Know When to Ask for Help**

In the event that you believe your organization may be impacted by ransomware, calling in experts to help investigate, understand and improve the situation can make the difference between a minor incident and a major breach. In some instances, organizations become aware of threat actor activity within their environment but may lack the visibility to address the problem or the right intelligence to understand the nature of the threat. Getting educated about the latest threats and seeking help by activating an incident response team or retainer, such as those offered by CrowdStrike Services, may allow for detection and remediation before the threat actor is able to deploy ransomware or exfiltrate data from the environment.

It’s better yet to seek out expert assistance before you truly need it. A technical assessment can help you to proactively identify and understand factors about your organization’s network that could make future ransomware incidents more or less likely. It may take different forms, depending on your current needs and security maturity. For instance, if you experience an intrusion that was confined to a specific network segment or specific business unit, an enterprise-wide compromise assessment can give confidence that the attacker did not move into parts of the environment that were beyond the scope of the initial investigation. Alternatively, an IT hygiene assessment can identify weak passwords, Active Directory configurations or missed patches that could open the door to the next attacker.

### **Develop your backup plan**

Develop and implement a backup plan for your organization. A backup is a copy of your data and systems that can be restored in the event of an incident.

Online, offline, and cloud. Online backups are stored on a remote server or computer that is connected to your network. Unlike online backups, offline backups (“cold backups”) remain unconnected to your network and devices. Cloud backups are stored on a cloud platform maintained by a service provider.

## **Cyber security controls**

When implementing and maintaining a defence-in-depth defence model, it is imperative that your organization layers security controls throughout your networks to protect the security, confidentiality, integrity, and availability of your networks, devices, and information.

In the first stage of a ransomware incident, there are some preventative mitigation measures that can be put in place to protect your organization. The following is a list of cyber security controls that can be implemented at the forefront of your cyber security environment.

* Provide your employees with tailored cyber security training to ensure they are aware of attack vectors like phishing and how to identify suspicious emails or links.
* Use of strong passwords, or preferable passphrases, to attempt to prevent threat actors from being successful in brute force attacks.
* Implement MFA for your organization’s devices.
* Create an application allow list to control who or what is allowed access to your networks and systems. Application allow lists help to prevent malicious applications from being downloaded and infecting your server.
* Scan your hardware, software, and operating system for vulnerabilities and apply patches and updates to mitigate the risk of the vulnerabilities being exploited by a threat actor.
* Segment your network to ensure sensitive and high value information is in a different zone of your network.
* Setup monitoring and logging functionality for your systems and networks and ensure you receive automated alerts if any anomalies are detected.
* Protect your systems that are connected or exposed to the Internet with encryption, firewalls, MFA, and frequent vulnerability assessments.
* Disable macros to decrease the risk of ransomware being spread through Microsoft Office attachments.

In the second stage of a ransomware incident, there are some mitigation measures you can implement to enhance the protection of your systems and networks and prevent ransomware from spreading across your network and connected devices.

* Implement security tools, such as anti-virus and anti-malware software, as well as firewalls, to your networks to add layers of protection to potential entry points for threat actors.
* Apply the principle of least privilege in which you provide individuals only the set of access privileges that are essential for them to perform authorized tasks.

In the third stage of a ransomware incident, the number one mitigation measure you can implement for your organization is your backup plan. Ensure you have multiple copies of your backup stored offline and if possible, in the cloud through a CSP. By having your backups disconnected from your network, threat actors cannot delete them or infect them with ransomware. Ensure you test your backups and restore processes on a regularly scheduled basis and adjust any issues immediately to ensure your backup files are ready for your organization to recover quickly in the event of a ransomware incident.

### **Establish perimeter defences**

Protecting your network, connected systems and devices against cyber threats can seem like a daunting task. Perimeter defences to protect the boundary between two network security zones through which your traffic is routed. If this is defended by basic security protocols like firewalls, anti-virus and anti-malware software, your overall protection is significantly enhanced. Installing anti-phishing software is another option for enhancing your organization’s cyber security. Anti-phishing software blocks phishing emails to prevent attacks from occurring or spreading further.

Ensure your users access your network using your virtual private network ([VPN](https://cyber.gc.ca/en/glossary/VPN)). A VPN acts as a secure tunnel through which you can send and receive data on an existing physical network. Using a VPN provides a secure connection between two points, such as your laptop and your organization’s network.

#### **Zscaler Ransomware Protection**

Ransomware protection options

A whole range of different security solutions provide ransomware detection and remediation tools. Some of these are dedicated solutions that focus on a few specific capabilities, while others are part of broader threat protection suites.

Zscaler offers cloud native [ransomware protection](https://www.zscaler.com/solutions/security-transformation/cyberthreat-protection) to secure organizations against ransomware in three key ways:

* AI-driven sandboxing to quarantine and inspect suspicious content
* Inspection of all SSL/TLS-encrypted traffic
* Always-on protection that follows off-network connections

Let's look at each of these areas in more detail.

Using AI-driven sandbox quarantine

Because today’s ransomware variants are tailored to their targets, effective mitigation measures need to thwart new strains and zero-day threats before they can cause harm. Outdated approaches to ransomware protection rely on out-of-band malware analysis that passes unknown files to the user at the same time they’re being analyzed. Such “passthrough” approaches send an alert if they find a malicious file, but by that time, the file will have already reached its target, creating a significant risk of infection.

With an AI-driven sandbox quarantine built on a cloud native proxy architecture, files can be quarantined and fully analyzed before delivery, virtually eliminating the risk of patient zero infections. In contrast to legacy passthrough approaches, suspicious or never-before-seen files are guaranteed to be held for analysis and will not reach your environment.

A cloud native, AI-driven solution like [Zscaler Cloud Sandbox](https://www.zscaler.com/products/sandboxing) delivers benefits beyond those of legacy anti-malware solutions, including:

* Complete control over quarantine actions with a granular policy defined by groups, users, and content type
* Real-time security verdicts on unknown files powered by machine learning and the [Zscaler Zero Trust Exchange](https://www.zscaler.com/products/zero-trust-exchange)—the world’s largest security platform built for the cloud
* Fast, secure file downloads, with any files identified as malicious marked for quarantine

Essentially, Zscaler Cloud Sandbox prevents ransomware attacks by ensuring that unrecognized or malicious files never make it to your network in the first place.

Inspecting all encrypted traffic

Up to 90% of internet traffic is now encrypted. Attackers are taking advantage of this to hide their attacks, including ransomware. To reduce risk, comprehensive ransomware protection must inspect all encrypted traffic. That said, full SSL inspection can be challenging with legacy technologies. Decryption, inspection, and re-encryption of traffic is compute-intensive, and most appliances (such as next-generation firewalls) lack the processing power to avoid slowing performance to a crawl. Moreover, it doesn’t matter if it’s an appliance or VM in the cloud; either takes a performance hit when inspecting SSL traffic.

So, what can keep up with the demands of top-to-bottom SSL/TLS inspection?

A cloud native proxy architecture like Zscaler's lets organizations perform complete SSL inspection at scale without worrying about impacting performance or expanding the processing power of costly appliances. Using a global cloud distributed across more than 150 data centers on six continents, SSL traffic can be thoroughly inspected for hidden ransomware threats with no dips in performance—even if user bandwidth dramatically increases.

All of this combines to eliminate any security gaps caused by the difficulty of analyzing ransomware hidden in encrypted traffic.

Following off-network connections

Many organizations struggle with always-on security when it comes to ransomware. By today’s standards, always-on security means extending your corporate security policies to keep your network safe even as users drop off VPN, use personal devices, and connect via home or public Wi-Fi networks. Relying on legacy approaches tied to data centers and regional gateways means security policies cannot follow your users off-network. That, in turn, allows attackers to deliver ransomware to those they know are operating outside of your security controls.

Zscaler can deliver the first two aforementioned strategies—AI-driven sandbox quarantine and complete SSL inspection—to users regardless of their location or device. Every connection over any network gets identical protection to uncover and thwart both known and unknown threats, keeping your organization free from patient zero ransomware infections.

This approach to preventing ransomware starts with user connections being secured through the Zscaler Zero Trust Exchange. Off-net users simply add [Zscaler Client Connector](https://www.zscaler.com/products/zscaler-client-connector), our lightweight endpoint agent, to their laptops or mobile devices (with support for Android, iOS, macOS, and Windows operating systems) to enjoy the protection of the same security tools, policy enforcement, and access controls they would get in your headquarters.

#### **Implement logging and alerting**

Implementing continuous monitoring of your networks will help you establish a baseline for acceptable activity patterns within your organization. Establishing monitoring capabilities for your networks and systems can help your organization manage risk. Your monitoring system should generate logs that can be reviewed by IT specialists and management when necessary. Access to your logs should be limited to those who need to review them.

Implementing automatic alerting within your monitoring practices is also necessary in order for anomalies in activity patterns to be flagged and reviewed, as well as potential vulnerabilities and events that need risk mitigation action to be taken. The alerts will indicate something out of the ordinary has occurred and your organization can then review these anomalies to determine what occurred, whether there is a risk to the organization, and what can be done to mitigate the risk. Your organization’s logging and alerting system should not permit modifications to be made to your logs once they have been received from the system. They should be a stamp in time and assist you in understanding what led to an event or an incident.

If your organization becomes a victim of ransomware or another type of cyber incident, your logs could provide you with insight into how the incident occurred and what controls or mitigation measures can be implemented to better protect your networks and systems from future incidents.

#### **Conduct penetration testing**

Penetration testing is a method for gaining assurance of the security of a system. During a penetration test, the tester attempts to breach some or all of the system's security, using the same tools and techniques that an adversary may use. It is not meant to be a primary method of identifying vulnerabilities, rather a method of ensuring your organization’s vulnerability assessment and management processes are effective.

#### **Segment your networks**

When segmenting your network, you divide your networks into smaller sections or zones. With network segmentation, traffic is directed and flows through the different sections of the network. Segmenting your network allows you to stop traffic flow in certain zones and prevent it from flowing to other areas in your network. In the same manner, segmentation also allows you to isolate and stop the spread of malware to different sections of your network, and control and restrict access to your information. When segmenting your network, ensure your information technology (IT) and operational technology (OT) networks are identified, separated, and monitored. In addition to segmenting your IT and OT networks, you should also identify interdependencies between them and implement measures that can be put in place during a cyber incident to protect critical information and functions.

#### **Constrain scripting environments and disable macros**

If your organization is using Windows, you may want to consider constraining your scripting environments. With Windows specifically, Microsoft developed an automated system administration capability through an interface powered by their shell scripting language (PowerShell). It is a powerful and important part of the system administration toolkit. It can be used to fully control Microsoft Windows systems and has many benefits for organizations. Threat actors can exploit PowerShell and inject malicious code into your devices’ memory. More concerning is the fact that PowerShell is a trusted source and therefore the threat actor’s code injection will typically not be blocked by anti-virus or anti-malware software or by your systems’ event logs.

#### **Patch and update**

To protect your connected devices from ransomware, you should ensure you check the operating system, software, and firmware regularly for updates and install security patches. There are a variety of patches available; however, the following three types are most applied:

1. **Bug fix patch**: Repairs functionality issues in software (e.g. error that causes unexpected device behaviour);
2. **Security patch**: Addresses security vulnerabilities to protect the system from threats (e.g. malware infecting devices through security flaws); or
3. **Feature patch**: Adds new functions to the software (e.g. enhancements to application performance and speed).

#### **Use protective domain name system (DNS)**

Domain Name System (DNS) is a protocol that maps domain names easily read by the human eye to Internet Protocol (IP) addresses easily read by machines. It is often referred to as the address book for the Internet. DNS is used for both human-initiated actions (e.g. visiting a website) and machine-initiated actions (e.g. running an update).

Protective DNS is a tool that can be implemented by your organization to block employees using corporately issued devices from visiting potentially malicious domains on the internet. Protective DNS identifies malicious domains against your organization’s blocklist, which is a listing of domains and IP addresses that users are not permitted to visit using corporate assets or while on your organization’s network.

You should also consider implementing protective DNS filtering on any mobile devices used by employees of your organization, especially if they can connect to your network and systems remotely. You can do this by manually configuring DNS settings on your organization’s devices, through a mobile device management (MDM) tool. Canadians can use a free public DNS application called Canadian Shield provided by the Canadian Internet Registration Authority (CIRA) to ensure personal devices always use a trusted DNS and filter out malicious IP addresses Footnote15. Canadian Shield can be set-up on your router or gateway to better protect your entire network. It is recommended to apply their “Protected” DNS resolver as it is designed to offer enhanced malware and phishing blocking functionality. By replacing the default DNS server settings on your devices with a trusted DNS server you can better protect your devices

#### **Apply password management**

When permitted, your organization should consider implementing passphrases in place of passwords, however, most systems are set up to require a username and password to grant access. Using strong passwords is one step in protecting your systems and sensitive information, but it is not enough to prevent a threat actor from gaining access. Password guessing is a common tactic used by threat actors to gain access to networks and systems.

Section 2.1.4 provides details on adopting MFA into your account and access management practices. In conjunction with MFA, implementing the use of a password manager for your staff members can be a beneficial tool in remembering and securing passwords required to access your networks and systems. Password managers can be a useful tool for your organization to keep track of the numerous passwords for individual and administrative accounts.

Your organization should also consider implementing password vaults for administrative accounts. Password vaults ensure a higher level of protection as the passwords are cycled and synched with your systems. This ensures a password can only be used once and provides tracing capabilities that can determine who used a password at a given time for specific access.

#### **Use email domain protection**

Consider implementing technical security measures to protect your organization’s domains from email spoofing, preventing the delivery of malicious messages sent on behalf of your domain, and identify the infrastructure used by threat actors. These measures also help prevent phishing emails from being delivered to your organization. You can reduce a threat actor’s chance of carrying out successful malicious email campaigns by implementing the following three security protocols that act jointly to protect email domains from being spoofed:

* **Sender Policy Framework (SPF):** Consider implementing technical security measures to protect your organization’s domains from email spoofing, preventing the delivery of malicious messages sent on behalf of your domain, and identify the infrastructure used by threat actors. These measures also help prevent phishing emails from being delivered to your organization. You can reduce a threat actor’s chance of carrying out successful malicious email campaigns by implementing the following three security protocols that act jointly to protect email domains from being spoofed:
* **DomainKeys Identified Mail (DKIM):**You can use DKIM to provide a mechanism for email messages to be authenticated using a cryptographic signature. When an email system that supports DKIM receives a DKIM signed message, it retrieves the record associated with the message’s DKIM header and verifies the message’s signature using the published public key. This DKIM check cryptographically confirms that the message was sent by an authorized sender and was not altered in transit. If the signature is not valid, or if no DKIM record is available, the message will fail DKIM. Messages that fail this DKIM check may be rejected.
* **Domain-based Messaged Authentication, Reporting and Conformance (DMARC):**Implementing DMARC policy and verification can enhance your security protocols and protect your email domains from being spoofed. If an email passes through the DMARC validation it will be delivered to the intended recipient. If the email fails DMARC validation, the receiving email system applies the policy specified in the sending domain’s DMARC record, and will either deliver the email, deliver the email marked as suspicious, or reject the email.

## **How to recover from ransomware**

Recovering from ransomware can be a lengthy process and recovering your organization’s brand and reputation can be an even longer process. Working on the assumption that your organization will encounter some form of malware will assist you in developing your planned response and could speed up your recovery processing time. By adhering to the guidance provided in this document, your organization will not only reduce the time it takes to recover from an attack, but it can also reduce the likelihood of an attack occurring or minimize the impact of an infection.

**Immediate response actions**

Threat actors can infiltrate your network and continue to have visibility into your systems, connected devices, and communications. You should assume the threat actor has visibility into your organization and therefore you should implement an alternative communication method (e.g. external email accessed by a device not connected to your network) that is not accessible to them. This will also block the threat actor from gaining insight into your intended incident response plans and recovery actions.

### **Recovery actions**

Despite temporary disruptions to your business, isolating your infrastructure from the Internet is the most important course of action. Isolation will temporarily remove the threat actor’s access to you infrastructure, allowing you to gain control and further your incident investigation, response, and recovery.

### **Remediate the point of entry**

To recover successfully and avoid reinfection, you will need to identify how the threat actor was able to enter your network, systems, and devices and address the vulnerability immediately. Ensure you remediate the point of entry prior to connecting your systems or devices to your network or the Internet to thwart the threat actor’s ability to gain access in the same manner.

### **Implement your backup plan**

Ensure your organization is protected by having a detailed backup plan in place. You will execute this plan if your main systems and data storage are compromised and need to be restored with your copied information. The plan will ensure your organization can restore critical systems and data and get back to business quickly. You should recover your systems using offsite backups that are not connected to your networks. Prior to restoring from a backup, scan and analyze it to ensure it hasn’t been compromised by the threat actor.

### **Restore your systems**

Following your incident response plan, identify the critical systems and data that need to be recovered first. Ensure that these systems and data have not been impacted by the ransomware attack and that they do not have signs of any other malware infection.

There are several options to consider when implementing your recovery strategy. You should choose a recovery strategy that meets your business needs and security requirements.

### **Engage cyber security professional assistance**

Procuring professional services from a highly rated cyber security agency or professional can be a helpful asset when preparing for and responding to a ransomware incident. If your organization has a cyber insurance policy, your provider will often include the assistance of a third-party cyber security professional in the event of an incident like a ransomware attack. They will provide you with incident response expertise and a recovery strategy tailored to your organization. They may also deploy a incident handling team to lead your organization’s response and recovery process. If you do engage professional cyber security assistance, ensure you clearly identify the service expectations, roles, and responsibilities.

### **Inform stakeholders**

When an incident occurs, and especially when it compromises your systems and data, it is imperative you inform key stakeholders, clients, and your staff members. You should consider preparing a statement in advance that can then be tailored to the incident, as well as a contact list of all stakeholders to be notified. Ransomware attacks can jeopardize your organization’s reputation, so your communications plan must be implemented swiftly following an incident to ensure your stakeholders are informed and able to enact their own incident response plans if necessary.

### **Analyze the incident**

Determining the root cause of the incident is key. How did the threat actor gain access to your network and deploy the ransomware? Often the ransomware incident is a symptom of a more serious hack or intrusion by the threat actor. Without identifying how they gained access and applying appropriate security measures to prevent it from happening again, threat actors may continue to exploit the vulnerability.

Determining what systems, accounts, and information have been accessed by the threat actor is a vital step in your incident analysis. This will enable you to determine the extent of the damage, such as what accounts were compromised and what data was exfiltrated, which will inform your approach to control the attack, prepare, and implement a proper response, and execute a successful recovery.

## **List of abbreviations**

**Term and Definition**

**BIA**

Business Impact Analysis

**CIRT**

Cyber Incident Response Team

**CSP**

Cloud Service Provider

**DKIM**

DomainKeys Identified Mail

**DMARC**

Domain-Based Message Authentication, Reporting, and Conformance

**GC**

Government of Canada

**IT**

Information Technology

**MFA**

Multi-Factor Authentication

**MSP**

Managed Service Provider

**OS**

Operating System

**RaaS**

Ransomware as a Service

**RDP**

Remote Desktop Protocol

**SPF**

Sender Policy Framework

**SSO**

Single Sign-On

**VPN**

[Virtual Private Network](https://cyber.gc.ca/en/glossary/Virtual%20Private%20Network)

## **References**

<https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-insightidr-ransomware-playbook.pdf>

<https://cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099#table2>

<https://cyber.gc.ca/sites/default/files/cccs-itsm00099-fig6-v3-en.png>

<https://cyberreadinessinstitute.org/resource/ransomware-playbook/>

<https://xsoar.pan.dev/docs/reference/playbooks/playbook3>

<https://www.crowdstrike.com.br/solucoes/ransomware-protecao/>

<https://www.cisa.gov/stopransomware/ransomware-guide>

<https://www.cisa.gov/stopransomware/ransomware-guide>

<https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf>

<https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident>

<https://csrc.nist.gov/publications/detail/nistir/8374/archive/2021-06-09>

<https://csrc.nist.gov/projects/ransomware-protection-and-response>

<https://www.zscaler.com/resources/security-terms-glossary/what-is-ransomware-protection>

**HISTÓRICO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rev. | Data | Histórico | Atividade | Responsabilidade |
| 0 | 16/05/2021 | Criação | Elaborador  Revisor  Aprovador | Joas/Kleber  Kleber  Gustavo |