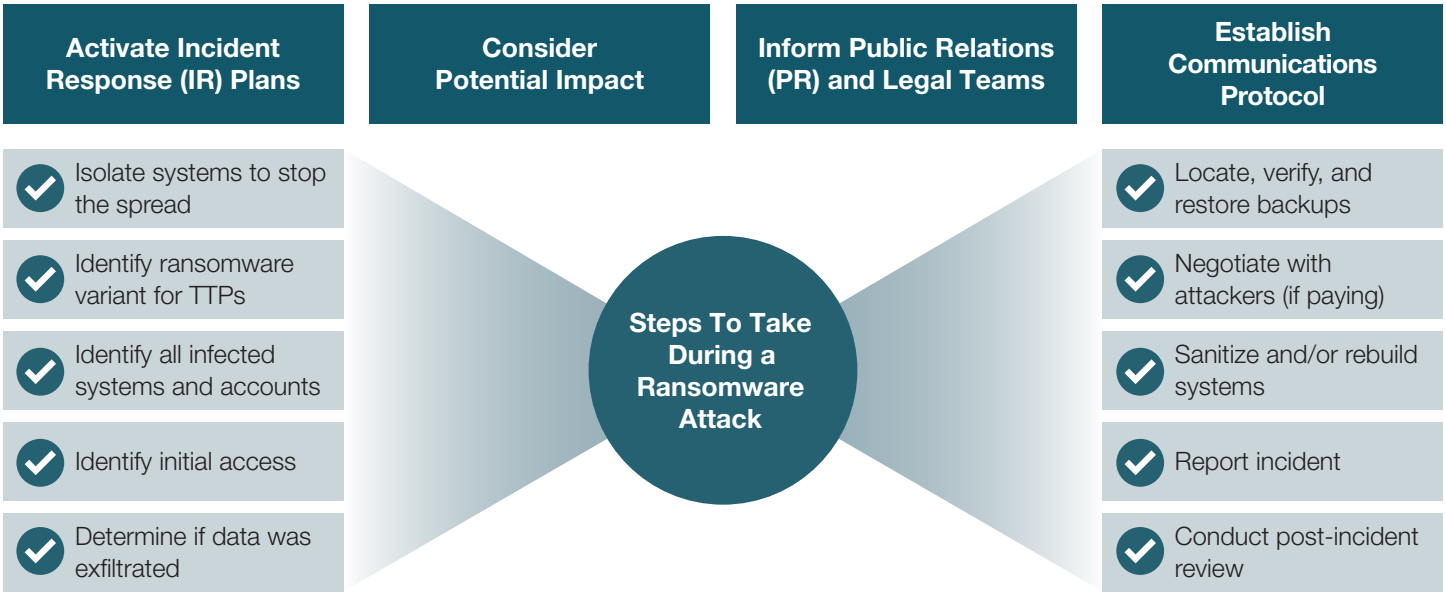
CHECKLIST

What To Do if You're in the Midst of a Ransomware Attack



There were over 187 million ransomware attacks in 2019. That's over 500,000 attacks on businesses every single day. If you have not yet been a victim of a ransomware attack, the odds are that it is just a matter of time. And if you have already been breached, you're not immune. When that day comes, it is essential that you know what to do to minimize the impact to you, your team, and your business.

Here is a quick overview of the steps your organization will need to take to deal with an active ransomware attack:

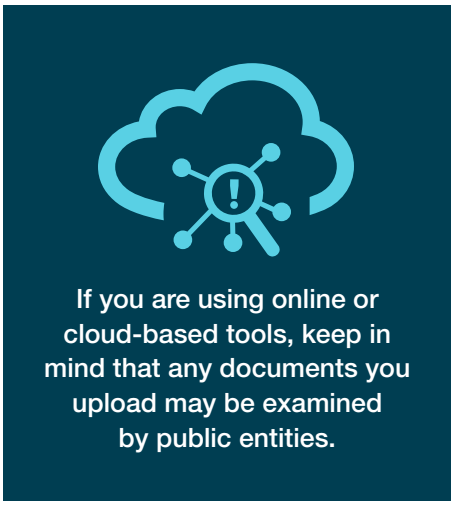
Steps To Take During a Ransomware Attack

First: Don't Panic!

- You will need to act quickly, but methodically. Stay calm, and begin to execute your planned incident response (IR) steps, if you have them. If you don't, the steps below can help. Alternately, reach out to your security vendor for help. It's worth noting when you report the incident to your insurance company, they may already have a list of expert providers who are trained to help you that you can choose from.
- Start thinking about the potential impact the security incident may cause. Take into consideration not only those areas that are obviously compromised, such as data being encrypted and applications being down, but also additional areas of potential compromise.
- Inform your internal public relations and legal teams so they can begin to prepare. Let them know you will establish a more formal communications and reporting structure as you gather additional information.
- Establish a communications and update protocol with a designated contact for each business vertical. For example, commit to updating all relevant team leads every three hours on the situation. This is an important step to avoid people constantly asking for updates and preventing your team from focusing on containment.

Isolate Your Systems and Stop the Spread

- You have multiple options for isolating the threat to stop it from spreading. If the incident is already known to be widespread, you may choose to implement blocks at the network level, such as isolating traffic at the switch or the firewall edge, or temporarily take down the internet connection. If the incident scope is already confirmed to be more narrow, infecting only a few systems, you could isolate them at the device level by possibly pulling the Ethernet or disconnecting the Wi-Fi. If you have technology such as endpoint detection and response (EDR) available, you could also be more surgical and block the attack at the process level, which would be the best immediate option with the least amount of business disruption. Remember to try and keep all systems powered on to ensure no forensic evidence is lost. And keep in mind that once you disrupt an attacker's activity, you are tipping them off and they may go dormant, making it harder to identify the entire attack scope.
- If the situation calls for it, capture forensic images of the data drives and memory of the infected systems. However, do not attempt this if you have never done it before. This should not be the first time your team attempts to collect this information, no matter how confident they might be.



Identify the Ransomware Variant

- Many of the tactics, techniques, and procedures (TTPs) of an attack are publicly documented for each ransomware variant. Determining which attack you are dealing with can give you clues on where to look for the threat and how it is spreading, as well as details around persistence.
- Depending on the variant, some decryption tools may already be available for you to decrypt your ransomed files. A good reference for finding decryption tools is available at the No More Ransom website. Oftentimes, the ransom note itself will give you a good indication of the ransomware group and/or variant being used. Also, uploading the ransomware to ID Ransomware may help identify the variant.
- If you are using online or cloud-based tools, keep in mind that any documents you upload may be examined by public entities.

Identify Initial Access

- Determining the initial access point, or patient zero, will help ensure you are able to close the hole in your security. Common initial access vectors are phishing, exploits on your edge services (such as Remote Desktop services), and the unauthorized use of credentials. Other initial access vectors could be drive-by compromises, exploits on public-facing websites and applications, removable media, hardware additions, and supply chain compromises.
- This step is sometimes difficult, and you may need expertise from digital forensics or IR experts and consultants in determining the initial point of access.

Identify All Infected Systems and Accounts (Scope)

- Even after an attack is over, it is more than likely that your attackers still have a foothold in your network. It is critical that you identify any active malware, or persistent leftovers that are still communicating to the command-and-control (C2) server. Common persistence techniques include:
  - Creating new processes running the malicious payload
  - Using run registry keys
  - Creating new scheduled tasks

- In addition, your attackers have most likely compromised a number of accounts, both non-privileged and privileged, such as Active Directory (AD) accounts, so disable any of those. Also ensure there are no new rogue account creations in process. Other AD components, such as Group Policy Objects (GPOs), should be reviewed to determine if anything has been newly created or modified. This is a common tactic used by attackers to push the ransomware payload out to all systems.
- Document your findings before taking action. Taking action may alert the attacker and cause them to launch a much more serious attack. It may also limit your ability to recover your data or determine the full impact of the data breach.

Determine if Data Was Exfiltrated

- Oftentimes, ransomware attacks not only encrypt your files but they also exfiltrate your data. They will do this to increase the chances that you pay the ransom by threatening to post things like proprietary or embarrassing data online. Look for signs of data exfiltration, such as large data transfers, on your firewall edge devices. Also look for odd communications from servers going to cloud storage applications, such as Dropbox or AWS. If you have a cloud access security broker (CASB) solution, this will be your primary source for this information, along with firewall logs.
- This step can also be difficult and may be another situation to consider bringing in a digital forensics team or IR expert consultants for a more thorough investigation.

Locate Your Backups and Determine Availability

- A ransomware attack will attempt to wipe your online backups and volume shadow copies to decrease the chances of you recovering your data and ultimately not paying the ransom. Because of this, ensure your backup technology was not affected by the incident and is still operational. Second, verify if you have either online or offline backups available for recovery.
- Many times, attackers will try to corrupt any online backups. Verify that not only does a backup exist but that its data is accurate and recoverable.

Verify the Integrity of Your Backups and Restore To Last Known Good

- With many ransomware attacks, attackers have usually been in your network for days, if not weeks, before deciding to encrypt your files. This means that you may have backups that contain malicious payloads that you do not want to restore to a clean system. Through your investigation of the incident, you should gain a good idea of the initial access date and time. You should then try to restore from the day before. Either way, you will need to scan your backups to determine their integrity.

Sanitize Systems or Create New Builds

- If you feel confident in your ability to identify all of the active malware and incidents of persistence in your systems, then you may be able to save some time by not rebuilding. However, it may just be easier and safer to create new, clean systems. You may even consider building a totally separate, clean environment that you can then migrate to. This should not take too long if you are running a virtual environment. Just make sure when you rebuild or sanitize your network or network segment, you have security controls installed and are following best practices to ensure devices do not become reinfected.

Report the Incident

- Now it's time to revisit the legal team. It's important to report to all entities, such as your legal team and insurance company. You should also determine if reporting to law enforcement is needed and required.
- Your legal team can help address any legal obligations around regulated data, such as PCI, HIPAA, etc. Whether you have cyber insurance or not, it's possible your insurance company may help pay for some of the costs of recovery. In addition, if you need an outside IR organization, they will most likely have a preferred list of IR companies you can hire to assist with the investigation.

- Determine if you will publicly disclose the attack. In some cases, you may be legally required to disclose some or all details around the network. Determine the time frame within which you must disclose the attack, if required. Your legal resources should be able to help with this research once you have determined the type of data that may have been compromised. Keep in mind that informing law enforcement about the attack may create a public record and may be the same as a public disclosure.
- If the attack is severe, and your business spans multiple geographical regions, you may need to contact national law enforcement services instead of a local or regional-based law enforcement agency. In the United States, this means contacting your nearest FBI regional office.
- If you are a member of the FBI's InfraGard program, utilize those resources if your organization is going to disclose an incident to law enforcement. If you are not part of InfraGard, or do not know how to use those services, use the FBI's Internet Crime Complaint Center.
- Depending on your circumstances, contacting law enforcement may be beneficial, especially with regard to the additional resources they can provide to assist with addressing the security incident. In some cases, they may also be able to help locate your data if it was exfiltrated. In addition, filing a police report is a formality that may be needed for cyber insurance. (Your legal team should determine if it is required or not.)

It's essential that you review your incident response to understand what went right and to document opportunities for improvement.

Paying the Ransom? Negotiate First

- Law enforcement frowns on anyone paying a ransom. However, if you are considering paying the ransom, you should hire a security company with specialized skills to help you negotiate the ransom down. The bad actors are usually willing to negotiate. Your legal team or outside counsel will often have a list of recommended negotiators for you to choose from. Be aware that paying ransom demands to some specific threat actors (such as nations under economic sanctions) may violate Office of Foreign Assets Control (OFAC) regulations, resulting in additional fines. More information can be found here.
- Keep in mind that ransomware negotiations will take time. You should only negotiate to get your data back. You should also remember that there is never a guarantee that negotiating with the attacker will stop them from deleting data or releasing your data publicly.
- When negotiating, if the attackers claim they have stolen your data, ask them to provide you with a verifiable sample of the stolen data, such as a directory structure. They will typically provide that proof.
- Keep in mind that paying the ransom is not going to remediate the vulnerabilities that the attackers exploited, so still ensure you have identified the initial access and patched the vulnerabilities.

Conduct a Post-incident Review

- There is a famous saying in the military: "No plan survives contact with the enemy." No plan is ever perfect, especially if it has never been tested in a real-world environment. So, it's essential that you review your incident response to understand what went right and to document opportunities for improvement. This "lessons learned" step helps ensure the continuous improvement of your response and recovery capabilities. It is worth noting that this review should be done as soon as possible after the recovery phase, while it's all fresh in everyone's mind.
- Consider simulating the technical and nontechnical details of the attack in red team and table-talk exercises so you can review your options.
- Consider contracting with the third party to assess your entire attack surface to identify any missing security controls. These outside consultants should leverage common frameworks, such as the National Institute of Standards and Technology (NIST), so you have standards that you can measure your progress against.

Everyone Gets Attacked. Everyone Needs a Plan. Get Started Today.

- If you are reading this because you have been the victim of a ransomware attack, follow these steps carefully. Especially the first one. Panicking leads to mistakes and can make the problem worse. Remember, there are professionals available to help.
- If you have not been attacked, this is the time to build an IR plan and a business continuity plan (BCP). These steps are just a baseline. There are a lot of things to plan and document, such as identifying your critical response team, knowing who does what, establishing chains of command, designating a spokesperson, stockpiling and isolating critical recovery resources, building an effective set of backups off-network, running red team/blue team threat simulations, and much, much more.
- There are plenty of organizations that can help. Start by talking with your most trusted security vendors. Many have teams of experts in place designed to test your network, build an IR plan, and provide forensics and recovery services. But whatever you do, don't wait. That's exactly what the cyber criminals targeting your organization are counting on.

There are plenty of organizations that can help. Start by talking with your most trusted security vendors.

Disclaimer: The external websites cited in this document, and the information they provide, have been deemed to be reliable by FortiGuard Labs. However, they have not been independently validated by us, nor do these citations imply any sort of endorsement, as all networks and deployments are unique.

January 8, 2021 1:42 PM

863720-0-0-EN

D:\Fortinet\Work\2021\0108\sb-ransomware-attack