What to Do First When Ransomware Attacks

The Top 5 Priorities When Dealing With Ransomware

Ecuron Inc. • 2929 Allen Parkway, Suite 200 • Houston, TX 77019 • 833.973.1034 • www.ecuron.com

10062020 What to Do First When Ransomware Attacks

What to Do First When Ransomware Attacks

For many companies, it would be a nightmare to discover that they are the latest unwitting victim of a ransomware attack, capable of crippling computer systems and locking up data if a payment isn't made to cybercriminals.

There's no magic wand that can make a ransomware attack simply disappear - with no impact at all on an organization. However, you can lessen the problem by carefully following tried-and-trusted steps in the immediate aftermath of an attack.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing & Analysis Center (MS-ISAC) have jointly released an in-depth guide that not only includes recommendations on how you can reduce the chances of being the next ransomware victim, but also provide a step-by-step checklist for how to respond to a ransomware attack.

We believe that the ransomware response checklist could be a valuable addendum to organizations' incident response plans. Your company does have a cyber incident response plan, right?

And the advice couldn't be timelier, with more and more organizations hit by ransomware attacks that cripple their ability to operate normally or at all.

So, let's take a look at the checklist step-by-step, focusing specifically on the very first things you should do:

"1. Determine which systems were impacted, and immediately isolate them.

If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.

If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection."

If it's one or two computers that have been infected by the ransomware then you may be able to get away with just disconnecting those PCs and dealing with them

individually. But if the infection has distributed itself more widely then you may have to take more significant action to prevent the ransomware from spreading further.

So clearly, it's important to attempt to determine the scale of the problem as quickly as possible, as this will influence the nature of your response.

"After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods like phone calls or other means to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken."

In some instances, organizations have used personal email accounts or instant messaging services like WhatsApp to communicate if they fear corporate communications systems may be being monitored by the attackers.

Obviously, response teams should be careful to ensure that out-of-band communications they receive are genuinely from fellow workers rather than from malicious actors themselves.

"Not doing so could cause actors to move laterally to preserve their access — already a common tactic — or deploy ransomware widely prior to networks being taken offline."

But what if you cannot temporarily shut down your network or disconnect affected computers from the network?

In that case, the response guide offers the following advice:

"2. Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection."

However, it should be noted that if you do this you may lose potential evidence about the attack which would be useful to the authorities.

Law enforcement agencies, as well as CISA and MS-ISAC, may be interested in gathering a wide variety of other information that could be useful in their investigation.

This includes, but is not limited to, the following:

- Recovered executable files
- Copies of any readme file (this should not be removed as it often assists decryption)

- Live memory (RAM) capture from systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)
- Images of infected systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)
- Malware samples
- Names of any other malware identified on systems
- Encrypted file samples
- Log files (Windows Event Logs from compromised systems, Firewall logs, etc.)
- Any PowerShell scripts found having executed on the systems
- Any user accounts created in Active Directory or machines added to the network during the exploitation
- Email addresses used by the attackers and any associated phishing emails
- A copy of the ransom note itself
- Ransom amount and whether or not the ransom was paid
- Bitcoin wallets used by the attackers
- Bitcoin wallets used to pay the ransom (if applicable)
- Copies of any communications with attackers

Even if there is little chance that an attacker might be identified and caught, details like the above – if shared with other companies – could help prevent them from becoming the next victim of the ransomware.

And it is only after the first two response steps that the guide recommends victims attempt to restore critical systems.

"3. Triage impacted systems for restoration and recovery.

Identify and prioritize critical systems for restoration and confirm the nature of data housed on impacted systems.

– Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.

Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner."

While these first three steps are being considered in order, there is additional work that can be taking place in parallel.

"4. Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis."

This clearly is a document that will grow over time as more information is found out about the ransomware, and what systems have been attacked and which have not.

"5. Engage internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident."

The guide provides contact information for CISA, MS-ISAC, as well as the FBI and US Secret Service.

"Share the information you have at your disposal to receive the most timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leaders."

The guide also references the "Public Power Cyber Incident Response Playbook", which although targeted at power utilities contains advice that would be appropriate for any organization needing step-by-step guidance on how to engage teams and co-ordinate messaging to customers and the public.

Ideally you do not wait until you are suffering a ransomware attack to read guidance like this but build a playbook of your own in advance that is specific to your organization.

There are many more steps detailed, and good advice offered, in the full MS-ISAC Ransomware Guide and we would strongly recommend it to anyone responsible for securing an organization against an attack.

APPENDIX

Current Cost of a Data Breach (Data as of July 2019)

Average cost of a breach worldwide:	$3.92 million
Average cost in the United States:	$8.19 million
Most expensive sector:	Healthcare with $6.45 million per breach
Average size of data breach:	25,575 records
Average cost per record:	$150

PCI Fines (companies dealing with credit card data):

- $5,000 - $100,000 per month, depending on size of business

HIPAA Fines (companies dealing with healthcare and medical records):

- $100-$50,000 per violation with a max penalty of $1.5 million per year for violations that are identical.

Graham Leach Bailey Act (GLBA) (applies to financial institutions, not just banks):

- Up to $100,000 per violation for the company
- Officers and directors can be fined up to $10,000 per violation
- Also includes criminal penalties of up to 5 years in prison and the possibility of revocation of licenses

Sources:

- https://www.ibm.com/security/data-breach
- https://www.lbmc.com/blog/pci-compliance-fees-fines-penalties/
- https://compliancy-group.com/hipaa-fines-directory-year/
- https://www.shredit.com/en-us/blog/compliance/the-gramm-leach-bliley-act
- https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act

About Ecuron

Ecuron is a boutique cybersecurity consulting company that specializes in preparing companies to face cyber threats. Our mission is to create a partnership with you, securing your data and protecting your organization every step of the way. For help developing and implementing an information- and cybersecurity strategy for your organization and for more information visit https://www.ecuron.com .