ITsMine™

RANSOMWARE SOS GUIDE:

Got Hit With A Ransomware Attack - Now What?

Guy Edri has 20+ years experience in Malware Research, Digital Forensics, Incident Response, and Ransomware attack recovery.

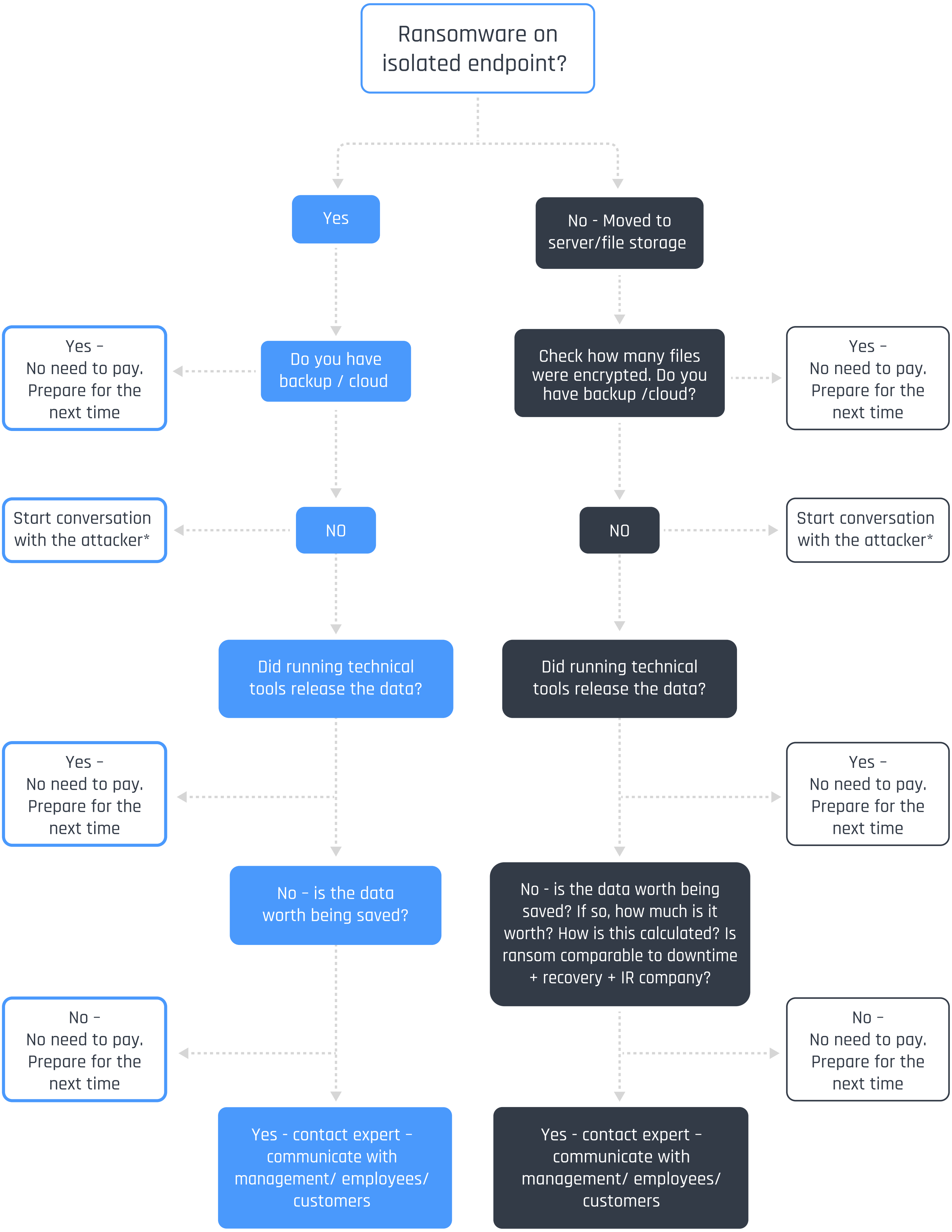
Here, Guy provides specific steps, tips and best practices when it comes to dealing with the aftermath of a ransomware attack.

What To Do After You Get Hit By Ransomware

What follows is a specific, proven step-by-step approach to get you and your organization back on your feet:

1. Disconnect internet access.
2. Isolate the potentially infected machines .
3. Run the below flow chart – time is money, and you need to get the required data fast. If information is not available, assume the worst and move to the next level.
4. Check for backup (see that this too was not hit by the ransomware).
5. How and where: Cloud, local, etc.
6. Run tools like www.nomoreransom.org
7. In parallel to Step 1 start negotiations with the attacker. SEE ALL THE DETAILS IN "TIPS FROM A PROFESSIONAL NEGOTIATOR" BELOW (best practice is to hire a professional negotiator).
8. It will not just "go away" – and you have a couple of hours before the cost will most likely double.
9. To pay or not to pay? Don't make any decisions without consulting a professional.
10. Change your mindset: can you treat this as (expensive) penetration testing?
11. Reinstall every device that had access to the infected device while the ransomware was available.
12. Plan how to recover the systems. If there wasn't enough segregation in the network, now is the best time to remedy that going forward.
13. Call for IR (Incident Response) services to find the point of entry, and to close the holes that let the attacker get inside.

Ransomware Response Flowchart:



Ransomware on isolated endpoint?

Yes

No - Moved to server/file storage

Yes –
No need to pay.
Prepare for the next time

Do you have backup / cloud

Check how many files were encrypted. Do you have backup /cloud?

Yes –
No need to pay.
Prepare for the next time

Start conversation with the attacker*

NO

NO

Start conversation with the attacker*

Did running technical tools release the data?

Did running technical tools release the data?

Yes –
No need to pay.
Prepare for the next time

Yes –
No need to pay.
Prepare for the next time

No – is the data worth being saved?

No - is the data worth being saved? If so, how much is it worth? How is this calculated? Is ransom comparable to downtime + recovery + IR company?

No –
No need to pay.
Prepare for the next time

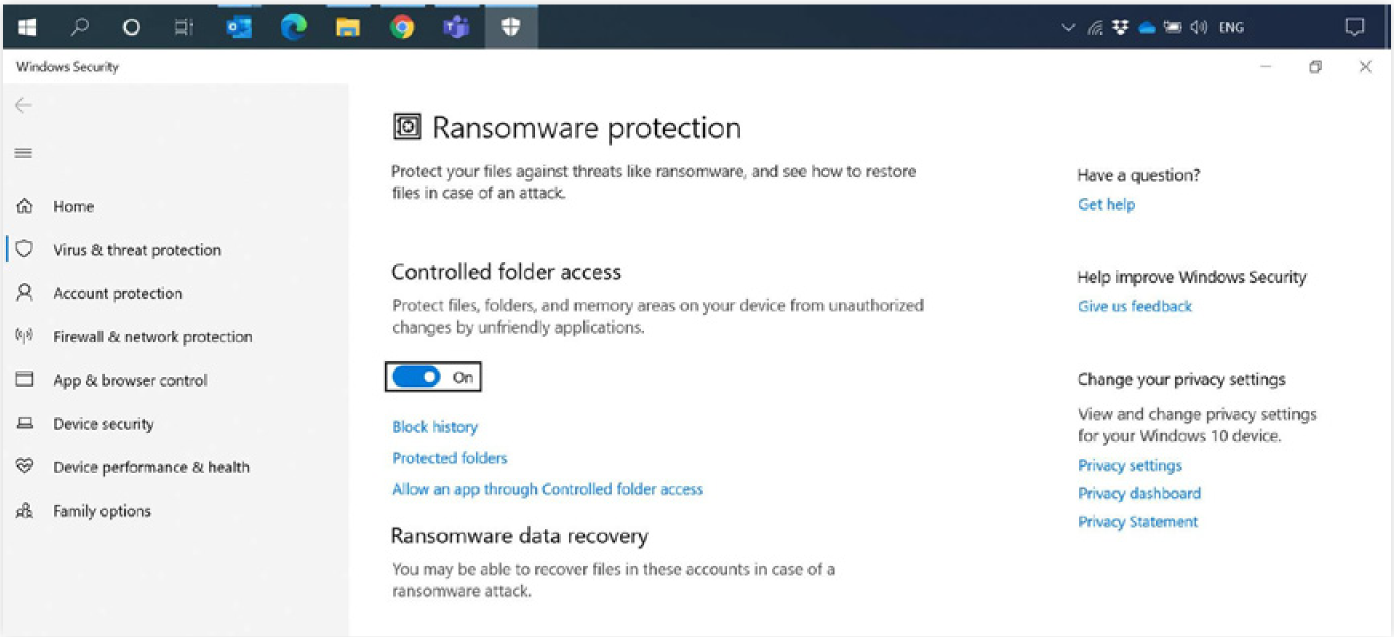
No –
No need to pay.
Prepare for the next time

Yes - contact expert – communicate with management/ employees/ customers

Yes - contact expert – communicate with management/ employees/ customers

After You Recover From The Attack, What Should You Do Next?

1. Protect your managed devices – use tools like Microsoft Defender – and activate the ransomware protection on the devices (whitelist the processes that allow edits to the files).
2. More information on this from Microsoft can be found here for Windows: https://support.microsoft.com/en-us/help/4013550/windows-protect-your-pc-from-ransomware
3.



Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
ENG

Ransomware protection

Protect your files against threats like ransomware, and see how to restore files in case of an attack.

Controlled folder access

Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.

On

Block history
Protected folders
Allow an app through Controlled folder access

Ransomware data recovery

You may be able to recover files in these accounts in case of a ransomware attack.

Have a question?

Help improve Windows Security

Change your privacy settings

View and change privacy settings for your Windows 10 device.

4. And here for Mac: https://support.apple.com/en-il/guide/mac-help/mh40596/mac
5. Upgrade the central logs of your security product (AV, EDR, etc) to the cloud
6. Connect your cloud and file storages to get all access logs in order to easily investigate the changed/deleted/encrypted files from a location/user/PC etc. Keep the data for forensics for at least two years.
7. Backup your files in the cloud/file storage – make sure you do not have leftover critical data on employee endpoints.
8. Plant SoftwareMines™ to make sure that your central file storages are protected from ransomware (even if the unmanaged device was infected).
9. Educate employees to "close the door". Revoke access automatically to areas they do not need access to anymore – as the ransomware uses the same access the users have.
10. Make sure all the systems have been patched to the latest security updates
11. Harden all servers/workstations.
12. Subscribe to Threat Intelligence feeds.
13. Forward all logs from Servers, FW, AV, EDR/XDR, and other devices to a central log server like Splunk/ELK, etc. If there is enough of an InfoSec budget, consider a managed SOC service.
14. Have a proper incident response plan in place and a company on call that knows the entire infrastructure.
15. Perform a full Penetration Test/Gap Analysis once every 3-6 months.

Tips from a Professional Negotiator

Cyber Crisis Negotiation: Do's and Don'ts

Once you've been hit with a classic ransomware attack, with no backup or any technological remediation in sight – and the threat actor has initiated a "dialogue box", be it as a link to a certain TOR window, confidential email account, or DM in social media – it is crucial to remember to following these ground-rules for effective negotiation:

Dialogue is not an agreement to pay. Engage in a conversation to learn more about the threat actor.

Keep messages short. Ask simple questions and expect simple answers.

Hold your emotions. Angry and rude communication will lead you nowhere.

It's "business", nothing is personal – however, there are people communicating with you.

Don't appeal to their logic, appeal to their emotions and human needs.

Never lie. If asked, consult your tech team for the best answer.

Expect no guarantees, but still ask for a "trouble-shooting" mechanism once you decide to pay.

The 3 Cardinal Rules

There are three main rules to bear in mind after being hit by a ransomware attack:

1

Don’t Panic:

This is what the attackers want you to do. At this sensitive time, almost as much damage can be done by doing the wrong thing, than by the attack itself. There are professionals out there who deal with these attacks all the time. Don't panic, relax those shoulders, you're going to get through this.

2

Don’t Pay:

The aim of the attackers of course is to extort money from you. Despite promises to the contrary, in many cases paying won't mean that you get access to your data again. They will threaten, they will tease, but don't be fooled into thinking that these people play fair.

3

Communicate openly with stakeholders:

Update people with what is happening. You don't have to share all information, but it's important to keep lines of communication open – including with stakeholders such as employees, customers, suppliers, regulators, and shareholders.