SOPHOS

ENDPOINT PROTECTION BEST PRACTICES TO BLOCK RANSOMWARE

A Sophos whitepaper July 2020

Endpoint Protection Best Practices to Block Ransomware

In our survey of 5,000 IT Managers across 26 countries, 51% of respondents revealed that they were hit by ransomware in the last year. In 73% of those incidents, attackers succeeded in encrypting data. Furthermore, the average global cost to remediate these attacks was an eye-watering $761,106.

One of the most effective methods to protect against ransomware attacks is with a properly configured endpoint protection solution. In this whitepaper, we will discuss how ransomware attacks work, how they can be stopped, and best practices for configuring your endpoint solution for the strongest protection possible.

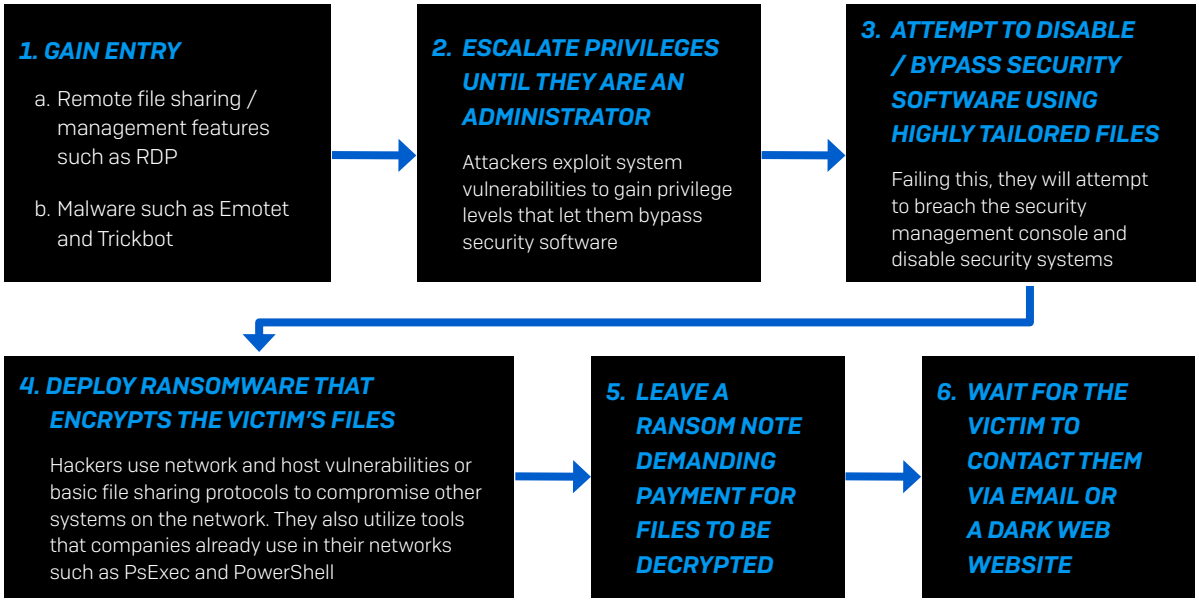
How Ransomware Attacks Are Deployed

In recent years, ransomware attacks have trended away from brute-force, large-scale attacks to focused, planned, and manually executed attacks that are much harder to detect and block. Let's take a look at how different forms of ransomware operate and what your organization should be doing to minimize its vulnerability to an attack.

Targeted Ransomware Attacks

Targeted ransomware attacks are very manual; typically focus on one victim at a time and often demand very high ransoms fees. Attackers gain access to the network and move laterally, identifying high-value systems in the process. Attempting to impact as many systems at once, these attacks are often launched at the worst possible times for defenders: nights, weekends, and holidays. They also leverage several attack techniques in order to sidestep layered protection features, making them particularly effective.

A typical targeted ransomware attack might look like this:



Consequences for falling victim to these attacks can be severe. Hackers are getting bolder, sometimes demanding six-figure payments. Furthermore, our survey revealed that paying the ransom actually doubled the cost of dealing with an attack – in excess of a business-crippling $1.4 million on average globally.

Remote Desktop Protocol or Ransomware Deployment Protocol?

Remote Desktop Protocol (RDP) and other desktop sharing tools like Virtual Network Computing (VNC) are legitimate and highly useful features that allow administrators to access and manage systems remotely. Unfortunately, without proper safeguards in place, such tools also provide convenient in-roads for attackers and are commonly exploited by targeted ransomware.

Not properly securing RDP and other similar remote management protocols behind a virtual private network (VPN) or at least restricting which IP addresses can connect via RDP can leave you wide open to attack. Attackers often use brute-force hacking tools, which try hundreds of thousands of username and password combinations until they find the right one and compromise your network.

General Best Practices to Stay Protected from Ransomware

Staying secure against ransomware isn't just about having the latest security solutions. Good IT security practices, including regular training for employees, are essential components of every single security setup. Make sure you're following these 10 best practices:

1. Patch early, patch often

Malware often relies on security bugs in popular applications. The earlier you patch your endpoints, servers, mobile devices, and applications, the fewer holes there are to be exploited.

2. Back up regularly and keep a recent backup copy off-line and off-site

In our survey, 56% of IT managers whose data was encrypted were able to restore it using backups. Encrypt your backup data and keep it off-line and off-site so you won't have to worry about cloud backups or storage devices falling into the wrong hands. Furthermore, implement a disaster recovery plan that covers the restoration of data.

3. Enable file extensions

The default Windows setting is to hide file extensions, meaning you must rely on the file thumbnails to identify them. Enabling extensions makes it much easier to spot file types that wouldn't commonly be sent to you and your users, such as JavaScript files.

4. Open JavaScript (.JS) files in Notepad

Opening a JavaScript file in Notepad blocks it from running any malicious scripts and allows you to examine the file contents.

5. Don't enable macros in document attachments received via email

Microsoft deliberately turned off auto-execution of macros by default many years ago as a security measure. A lot of infections rely on persuading you to turn macros back on, so don't do it!

6. Be cautious about unsolicited attachments

Cybercriminals often rely an ages-old dilemma: knowing that you shouldn't open a document until you are sure it's legitimate, but not being able to tell if it's malicious until you open it. If in doubt, leave it out.

7. Monitor administrator rights

Constantly review local and domain admin rights. Know who has them and remove those who don't need them. Don't stay logged in as an administrator any longer than necessary, and avoid browsing, opening documents, or other regular work activities while you have admin rights.

8. Stay up to date with new security features in your business applications

For example, Office 2016 now includes a control called "Block macros from running in Office files from the internet," which helps protect against external malicious content without stopping you from using macros internally.

9. Regulate external network access

Don't leave ports exposed to the world. Lock down your organization's RDP access and other remote management protocols. Furthermore, use two-factor authentication and ensure remote users authenticate against a VPN.

10. Use strong passwords

It sounds trivial, but it really isn't. A weak and predictable password can give hackers access to your entire network in a matter of seconds. We recommend making them impersonal, at least 12 characters long, using a mix of upper and lower case, and adding a sprinkle of random punctuation Ju5t.LiKETh1s!

Best Practices for Your Endpoint Protection Solution

Alongside a next-gen firewall, one of the most effective methods for protecting against ransomware attacks is to make use of an endpoint protection solution. However, it needs to be configured correctly in order to provide optimum protection.

Follow these best practices to protect your endpoint devices from ransomware:

1. Turn on all policies and ensure all features are enabled

It sounds obvious, but this is a surefire way that you'll get the best protection out of your endpoint solution. Polices are designed to stop specific threats, and regularly checking they're all turned on will ensure your endpoints are protected – especially against newer strains of ransomware.

Furthermore, enabling features that detect file-less attack techniques and ransomware behavior are critical in stopping criminals from infiltrating your endpoints and deploying harmful ransomware strains. They also enable you to more easily remediate attacks should they somehow get into your environment.

2. Regularly review your exclusions

Exclusions – preventing trustworthy directories and file types from being scanned for malware – are sometimes leveraged to soften complaints from users who feel the protection solution is slowing down their systems. Exclusions can also be used to reduce the risks of potential false positives.

Over time, a growing list of excluded directories and filetypes can end up impacting more and more people across the network. And malware that manages to make its way into excluded directories – perhaps accidentally moved by a user – will likely succeed because it's excluded from being checked.

Be sure to regularly check your list of exclusions within your threat protection settings and keep the number of exclusions as close to zero as you can.

3. Enable multi-factor authentication (MFA) within your security console

Multi-factor authentication, or MFA, provides an additional layer of security after the first factor, which is often a password. Enabling MFA across your applications is generally good IT security practice, and it's critical to enable it for all users who have access to your security console.

Doing so will ensure access to your endpoint protection solution is secure and not prone to accidental or deliberate attempts to change your settings, which could leave your endpoint devices vulnerable to attacks. MFA is also critical in securing RDP.

4. Ensure every endpoint is protected and up to date

Checking your devices regularly to know if they're protected and up to date is a quick way to ensure optimum protection. A device not functioning correctly may not be protected and could be vulnerable to a ransomware attack. Endpoint security tools often provide this telemetry, and an IT hygiene maintenance program is also useful for regularly checking for any potential IT issues.

5. Maintain IT hygiene

Regular IT hygiene ensures your endpoints and the software installed on them run at peak efficiency. Not only does it mitigate your cybersecurity risk, but it can save you a lot of time when it comes to remediating potential incidents in the future.

Implementing a program to maintain IT hygiene is especially critical for safeguarding against ransomware attacks and other cybersecurity threats. For example: ensuring RDP is running only where you need it and expect it, regularly checking for configuration issues, monitoring device performance, and removing unwanted or unneeded programs. An IT hygiene check may highlight the need to update software applications, including your security software. It's also a surefire way to ensure your precious data is backed up regularly.

6. Hunt for active adversaries in your network

In today's threat landscape, malicious actors are more cunning than ever, deploying stealthy techniques to conduct damaging ransomware attacks. Organizations need tools that allow them to ask detailed questions so they can identify advanced threats and active adversaries. Once found, organizations also need tools they can use to quickly take appropriate action to stop such threats.

Technologies within your endpoint solution, such as endpoint detection and response (EDR), provide this functionality, so be sure to enable and make use of EDR features if you have them.

7. Close the gap with human intervention – ransomware is only the endgame

Ransomware is only the endgame for hackers. To deploy ransomware, hackers will have already breached your network and possibly exfiltrated data without your knowledge – sometimes months before an attack even takes place.

Technology alone is often not enough to stop these intrusions. As a real-world example, a security camera lets you see how thieves get into your property, but it's only with security guards in place that you can prevent theft. The same can be applied to cybersecurity. The best way to truly safeguard against these types of intrusions is to add human expertise as part of a layered security strategy.

Managed detection and response (MDR) services are critical here. Pairing your internal IT and security teams with an external team of elite threat hunters and response experts helps provide actionable advice for addressing the root causes of recurring incidents.

Sophos Intercept X Advanced with EDR

Sophos Intercept X Advanced with EDR includes all the features you need to help protect your organization from ransomware attacks like Ryuk, Sodinokibi, Maze, and Ragnar Locker.

Intercept X includes anti-ransomware technology that detects malicious encryption processes and shuts them down before they can spread across your network. Anti-exploit technology stops the delivery and installation of ransomware, deep learning blocks ransomware before it can run, and CryptoGuard prevents the malicious encryption of files, rolling them back to their safe states.

Furthermore, Sophos EDR helps keep your threat hunting and IT operations hygiene running smoothly across your entire estate. Sophos EDR empowers your team to ask detailed questions to identify advanced threats, active adversaries, and potential IT vulnerabilities, and then quickly take appropriate action to stop them. It enables you to detect adversaries lurking in your network and waiting to deploy ransomware that may have gone unnoticed.

Sophos Managed Threat Response (MTR)

The Sophos MTR service adds human expertise to your layered security strategy. An elite team of threat hunters proactively looks for and validates potential threats on your behalf. If authorized, they take action to disrupt, contain, and neutralize threats, and provide actionable advice to address the root causes of recurring incidents.

Conclusion

Despite being a perennial cyberthreat, ransomware will only continue to evolve. While we may never be able to eradicate ransomware completely, following the endpoint protection best practices outlined in this document will give your organization the best odds of staying protected against the latest threats.

In summary:

1. Turn on all policies and ensure all features are enabled
2. Regularly review your exclusions
3. Enable MFA within your security console
4. Ensure every endpoint is protected and up to date
5. Maintain IT hygiene
6. Hunt for active adversaries on your network
7. Close the gap with human intervention – remember: ransomware is only the endgame

Try Sophos Intercept X for free
at www.sophos.com/endpoint

Learn more about Sophos MTR
at www.sophos.com/MTR

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

200702 WPEN (NP)

SOPHOS