SOPHOS

Remote Ransomware

Malicious remote encryption is a popular ransomware technique used in around 60% of human-operated ransomware attacks[1]. Most leading endpoint security solutions struggle to this approach and if you're not using Sophos Endpoint, there's a high chance you're exposed. Read this guide to learn about the risk of remote ransomware and Sophos' industry-leading ransomware protection that stops it.

A Sophos Whitepaper. December 2023

What is remote ransomware?

Remote ransomware, also known as malicious remote encryption, is when a compromised endpoint is used to encrypt data on other devices on the same network.

In human-led attacks, adversaries typically try to deploy ransomware directly to the machines they want to encrypt. If their initial attempt is blocked (for example, by security technologies on the target devices) they rarely give up, choosing instead to pivot to an alternative approach and try again, and again.

Once attackers succeed in compromising a device, they can leverage the organization's domain architecture to encrypt data on managed domain-joined machines. All the malicious activity – ingress, payload execution, and encryption – occurs on the already-compromised machine, therefore bypassing modern security stacks. The only indication of compromise is the transmission of documents to and from other machines.

80% of remote encryption compromises originate from unmanaged devices on the network[2], although some start on under protected machines that lack the defenses needed to stop attackers getting onto the device.

Why is remote ransomware so prevalent?

A key factor driving the widespread use of this approach is its scalability: A single unmanaged or under protected endpoint can expose an organization's entire estate to malicious remote encryption, even if all the other devices are running a next-gen endpoint security solution.

To make matters worse, adversaries are not limited in their choice of ransomware variant for these attacks. A wide range of well-known ransomware families support remote malicious encryption, including Akira, BitPaymer, BlackCat, BlackMatter, Conti, Crytox, DarkSide, Dharma, LockBit, MedusaLocker, Phobos, Royal, Ryuk, and WannaCry.

Another significant reason behind the prevalence of remote ransomware is that most endpoint security products are ineffective in this scenario because they focus on detecting malicious ransomware files and processes on the protected endpoint. However, with remote encryption attacks, the processes run on the compromised machine, leaving the endpoint protection blind to the malicious activity.

In contrast, Sophos Endpoint includes robust protection against malicious remote encryption, powered by our industry-leading CryptoGuard protection.

Sophos CryptoGuard: Industry-leading, universal ransomware protection

Sophos Endpoint contains multiple layers of protection that defend organizations from ransomware including CryptoGuard, our unique anti-ransomware technology that is included in all Sophos Endpoint subscriptions.

Unlike other endpoint security solutions that solely look for malicious files and processes, CryptoGuard analyzes data files for signs of malicious encryption irrespective of where the processes are running. This approach makes it highly effective at stopping all forms of ransomware including malicious remote encryption. If it detects malicious encryption, CryptoGuard automatically blocks the activity and rolls back files to their unencrypted state.

CryptoGuard actively examines the content of all documents as files are read and written, using mathematical analysis to determine whether they have become encrypted. This universal approach is unique in the industry and enables Sophos Endpoint to stop ransomware attacks that other solutions miss, including remote attacks and never-before-seen ransomware variants.

CryptoGuard is one of the unique capabilities in Sophos Endpoint and is included with all Sophos Intercept X Advanced, Sophos XDR, and Sophos MDR subscriptions. What's more, the capability is enabled automatically by default, ensuring organizations enjoy full protection from both local and remote ransomware attacks straight away – no fine tuning or configuration required.

- **Detects malicious encryption by analyzing file content**

  Unlike other solutions that look at ransomware from an anti-malware perspective by focusing on detecting malicious code, CryptoGuard looks for mass rapid encryption of files by analyzing content using mathematical algorithms.

- **Blocks both local and remote ransomware attacks**

  Because CryptoGuard focuses on the content of files, it can detect ransomware encryption attempts even when the malicious process is not running on the victim's device.

- **Automatically rolls back malicious encryption**

  CryptoGuard creates temporary backups of modified files and automatically rolls back changes when it detects mass encryption. Sophos uses a proprietary approach, unlike other solutions that use Windows Volume Shadow Copy, which adversaries are known to circumvent. There are no limits to the size and type of file that can be recovered, minimizing the impact on business productivity.

- **Automatically blocks remote devices**

  In a remote ransomware attack, CryptoGuard automatically blocks the IP address of the remote device attempting to encrypt files on the victim's machine.

- **Protects the master boot record (MBR)**

  CryptoGuard also protects the device from ransomware that encrypts the master boot record (preventing startup) and from attacks that wipe the hard disk.

Discover unprotected devices

A single unprotected endpoint can leave your organization vulnerable to a remote encryption attack. Deploying Sophos Endpoint provides robust universal ransomware protection from malicious encryption, but how can you identify if you have unprotected devices on your network in the first place?

This is where Sophos Network Detection and Response (NDR) can help. Sophos NDR monitors network traffic for suspicious flows and, in doing so, identifies unprotected devices and rogue assets in the environment.

For the strongest protection against remote ransomware attacks, install Sophos Endpoint on all machines in the environment, and deploy Sophos NDR to discover unprotected devices on your network.

Elevate your protection against remote ransomware today

Malicious remote encryption is a popular ransomware technique that most leading endpoint security solutions struggle to stop. If you're not using Sophos Endpoint, there's a high chance you're exposed.

To learn more about Sophos Endpoint and how it can help your organization better defend against today's advanced attacks, including remote ransomware, speak with a Sophos adviser or your Sophos partner today. You can also take it for a test drive in your own environment with a no-obligation 30-day free trial.

1 Microsoft Digital Defense Report. https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

2 Burt, T. (2023, October 5). Espionage fuels global cyberattacks. Microsoft. https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2023-12-06 (WP-DD)

SOPHOS