SOPHOS

FIREWALL BEST PRACTICES TO BLOCK RANSOMWARE

A Sophos whitepaper August 2020

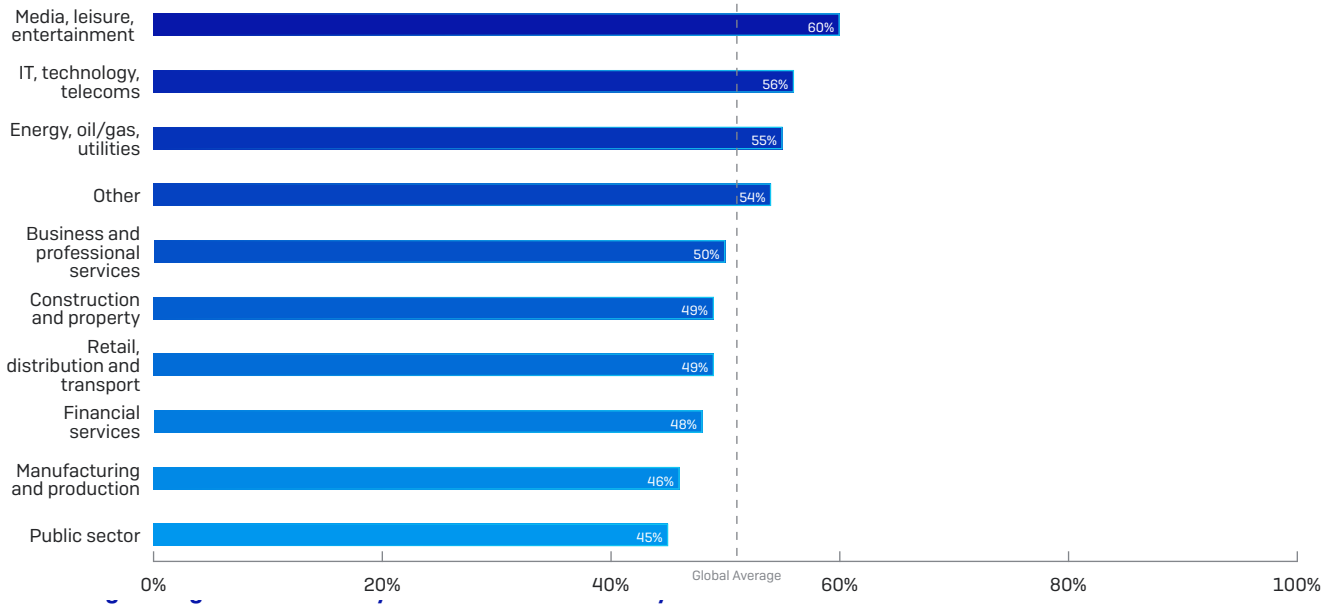
Firewall Best Practices to Block Ransomware

Ransomware continues to plague organizations, with over half of companies surveyed across 26 countries revealing that they were hit by ransomware in the last year*. Such attacks are ever increasing in complexity and are getting more efficient at exploiting network and system vulnerabilities, leaving organizations with a significant clean-up bill: a global average of an eye-watering US$761,106.

Modern firewalls are highly effective at defending against these types of attacks, but they need to be given the chance to do their job. In this whitepaper, we will discuss how these attacks work, how they can be stopped, and best practices for configuring your firewall and network to give you the best protection possible.

Who hackers are targeting

Who are hackers targeting? The short answer: everyone. In a recent survey, 51% of respondents said they had been hit by ransomware in the last year and it seems that organization size is not a significant factor. Forty-seven percent of the organizations had fewer than 1,000 employees while 53% had more than 1,000. No country, region, or vertical market segment is immune.



In the last year, has your organization been hit by ransomware? Base: 5,000 respondents.

If you search the news for "ransomware attack" you will find several new successful attacks occurring every week. The effects are devastating: huge ransomware demands, significant down-time and business disruption, reputation damage, loss of data, and in an increasing number of cases, sensitive company data is being auctioned off by attackers.

*The State of Ransomware 2020 - An independent survey of 5,000 IT managers in 26 countries, commissioned by Sophos and conducted by Vanson Bourne.

How ransomware attacks get on the network

In 2020, there has been an increasing trend toward server-based attacks. These are highly-targeted, sophisticated attacks that take more effort to deploy. However, they are typically far more deadly due to the higher value of assets that get encrypted, which can cripple organizations with multi-million-dollar ransom demands. Fortunately, these kinds of attacks are preventable with proper security best-practices in place.

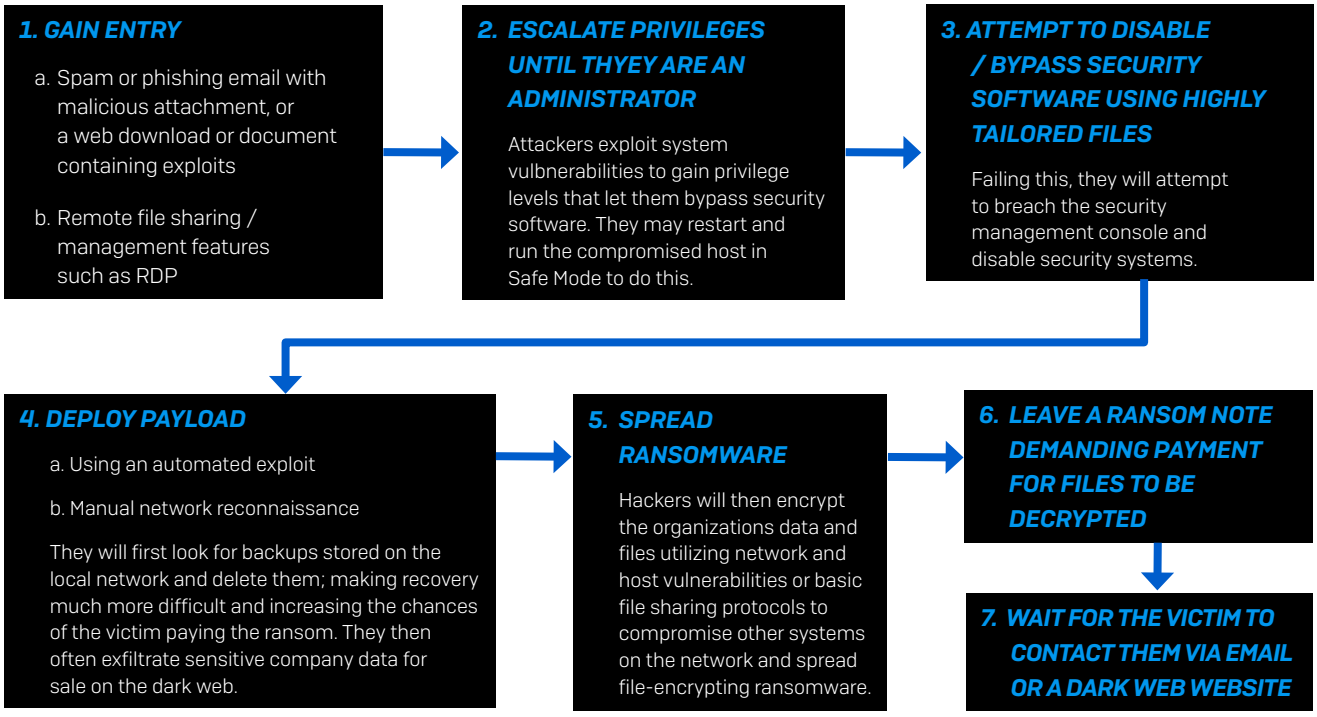
HOW THE RANSOMWARE GOT INTO THE ORGANIZATION	% INCIDENTS
Via a file download/email with malicious link	29%
Via remote attack on server	21%
Via email with malicious attachment	16%
Misconfigured public cloud instances	9%
Via our Remote Desktop Protocol (RDP)	9%
Via a supplier who works with our organization	9%
Via a USB/removable media device	7%
Other	0%
Don't know	0%
Total	100%

How did the ransomware attack get into your organization? Question asked to respondents whose organization had been hit by ransomware in the last year. Base: 2,538 respondents.

However, as you can see from the survey responses in the table above, the top entry point for ransomware is through files downloaded or sent to users in spam or phishing attacks. Don't leave security in the hands of your users. For these types of attacks, it's best to safeguard your organization with strong firewall protections.

How a ransomware attack works

A typical targeted ransomware attack looks like this:



RDP - Remote Desktop Protocol or Ransomware Deployment Protocol?

Remote Desktop Protocol (RDP) and other desktop sharing tools like Virtual Network Computing (VNC) are innocuous and highly useful features of most operating systems that allow staff to access and manage systems remotely. Unfortunately, without the proper safeguards in place, they 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 remote tools can leave you wide open to attackers. Attackers often use brute-force hacking tools which try hundreds of thousands of username and password combinations until they get the right one.

How to stay protected from ransomware

To properly protect your organization from ransomware, there are three major initiatives you should undertake.

1. Upgrade your IT security

Your firewall and endpoint security can protect against attacks getting onto the network in the first place, and if an attack should somehow penetrate your network, they can prevent it from spreading and infecting other systems. But not all firewalls and endpoint security solutions can do this effectively, so make sure you have an IT security system that does.

Ensure you have:

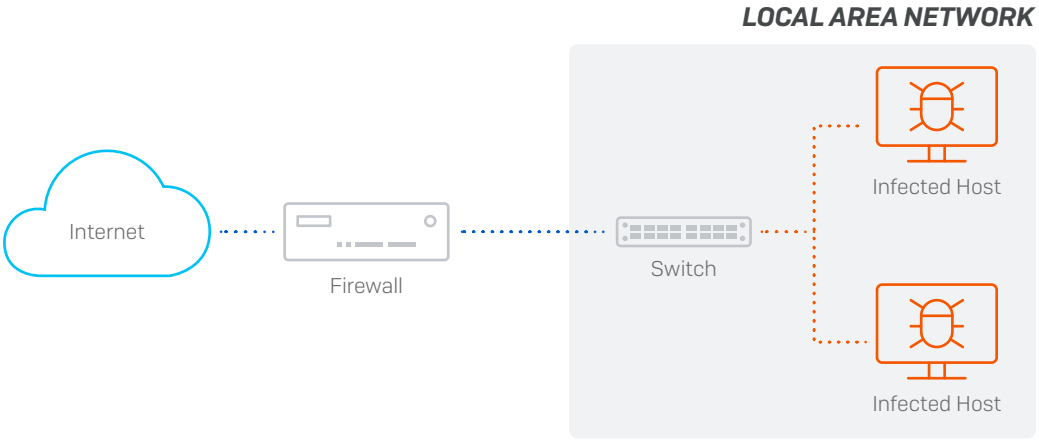
- Affordable sandboxing to analyze file behavior as it's run before it gets on your network
- The latest machine learning technology to identify new zero-day variants in any files coming through the firewall
- Firewall IPS with live signature updating to block network exploits
- Free and easy remote access VPN to enable management of your network remotely without compromising on security
- Endpoint protection with anti-ransomware capabilities

2. Lock down remote access and management

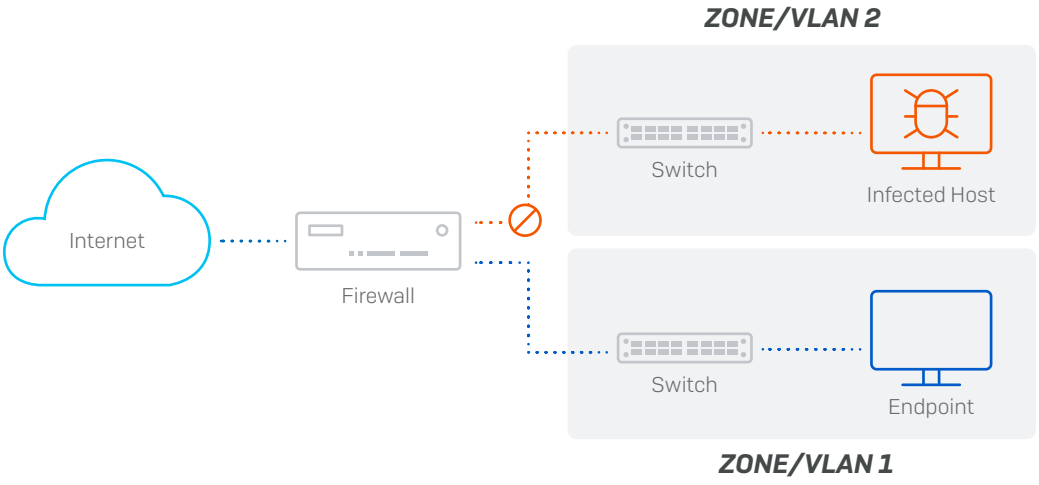
When it comes to networks, every opening to the outside world is a potential vulnerability waiting to be exploited by a ransomware attack. Locking down your organization's Remote Desktop Protocol access, open ports, and other management protocols is one of the most effective steps you can take to secure against targeted ransomware attacks. There are numerous ways you can do this. One popular method is to require all users be on a VPN before they can access resources such as RDP and restrict VPN access to known IP addresses. Also, properly secure and harden your servers, use complex passwords that are changed frequently, and leverage multi-factor authentication.

3. Segment your network

Unfortunately, many organizations operate with a flat network topology: all of their endpoints connect into a common switch fabric. This topology compromises protection by enabling easy lateral movement or propagation of attacks within the local network since the firewall has no visibility or control over the traffic flowing through the switch.



A best practice is to segment the LAN into smaller subnets using zones or VLANs and then connecting these together through the firewall to enable the application of anti-malware and IPS protection between segments. This can effectively identify and block threats attempting to move laterally on the network.



Whether you use zones or VLANs depends on your network segmentation strategy and scope, but both offer similar security capabilities by providing the option to apply suitable security and control over traffic movement between segments. Zones are ideal for smaller segmentation strategies or networks with unmanaged switches. VLANs are the preferred method for segmenting internal networks in most cases and offer the ultimate in flexibility and scalability. However, they require the use (and configuration) of managed Layer 3 switches.

While it's a best practice to segment your network, there's no "best" way to segment a network. You can segment your network by user type (internal, contractors, guests), by department (sales, marketing, engineering), by service, device, or role type (VoIP, Wi-Fi, IoT, computers, servers) or any combination that makes sense for your network architecture. But generally, you'll want to segment less trusted and more vulnerable parts of your network from the rest. You'll also want to segment large networks into smaller segments, all with the aim of reducing the risk of threat penetration and propagation.

Best practices for firewall and network configuration

- **Ensure you have the best protection**, including a modern high-performance next-gen firewall with IPS, TLS Inspection, zero-day sandboxing, and machine learning ransomware protection.
- **Lock down RDP and other services** with your firewall. Your firewall should be able to restrict access to VPN users and whitelist sanctioned IP addresses.
- **Reduce the surface area of attack** as much as possible by thoroughly reviewing and revisiting all port-forwarding rules to eliminate any non-essential open ports. Every open port represents a potential opening in your network. Where possible, use VPN to access resources on the internal network from outside rather than port-forwarding.
- **Be sure to properly secure any open ports** by applying suitable IPS protection to the rules governing that traffic.
- **Enable TLS Inspection** with support for the latest TLS 1.3 standards on web traffic to ensure threats are not entering your network through encrypted traffic flows.
- **Minimize the risk of lateral movement** within the network by segmenting LANs into smaller, isolated zones or VLANs that are secured and connected together by the firewall. Be sure to apply suitable IPS policies to rules governing the traffic traversing these LAN segments to prevent exploits, worms, and bots from spreading between LAN segments.
- **Automatically isolate infected systems.** When an infection hits, it's important that your IT security solution be able to quickly identify compromised systems and automatically isolate them until they can be cleaned up (such as with Sophos Synchronized Security).
- **Use strong passwords and multi-factor authentication** for your remote management and file sharing tools so that they're not easily compromised by brute-force hacking tools.

How Sophos can help

Sophos offers the ultimate IT security solution for defending against the latest ransomware. Not only do you get the best protection at every point, but you also benefit from years of integration between firewall and endpoint. This offers tremendous advantages in terms of visibility into network health, and the ability to automatically respond to security incidents.

With our award-winning XG Firewall, the focus is first and foremost to prevent attacks from getting onto the network. In the event ransomware does happen to get on your network, though, you're doubly covered. XG Firewall can automatically stop ransomware dead in its tracks thanks to integration with Sophos Intercept X, our industry-leading endpoint protection platform. It's like putting your network on auto-pilot – a huge force multiplier to your team.

We call this technology Sophos Synchronized Security. Synchronized Security merges our endpoint and network protection features into a powerful, deeply-integrated cybersecurity system. And the best part: it's all super easy to manage – along with all your other Sophos products - from our Sophos Central cloud management console.

Key XG Firewall and Sophos technologies that are designed specifically to combat ransomware

- XG Firewall's Sandstorm sandboxing and machine learning analysis of files entering the network help ensure that even previously unseen ransomware variants, exploits, and malware don't spread via spam, phishing, or web downloads.
- XG Firewall's intrusion prevention system catches the latest network exploits and attacks that hackers may be utilizing to find vulnerabilities in your defenses.
- XG Firewall's extensive but simple VPN options enable you to close all the holes in your network and remove your reliance on vulnerable RDP connections while still providing full access to your network by authorized users.
- XG Firewall offers high-performance Xstream TLS 1.3 inspection with flexible policy controls that ensure you can strike the perfect balance between privacy, protection and performance and ensure threats are not entering your network unseen over encrypted traffic flows.
- Sophos Synchronized Security integrates XG Firewall with our Intercept X endpoint protection to automatically respond to ransomware attacks by detecting the first signs of compromise, stopping them, and notifying you.
- Sophos Intercept X endpoint protection with CryptoGuard can detect a ransomware attack in progress, stop it, and roll it back automatically. XG Firewall includes CryptoGuard technology in the sandboxing environment to catch ransomware red-handed before it gets on your network.

Conclusion

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

In summary:

- Ensure you have the best protection
- Lockdown RDP and other services with your firewall
- Reduce the surface area of attack as much as possible
- Secure any open ports by applying suitable IPS protection
- Apply sandboxing and machine learning analysis to downloads and attachments
- Minimize the risk of lateral movement within the network by segmenting LANs
- Automatically isolate infected systems
- Use strong passwords and multi-factor authentication for your remote management and file sharing tools

Try Sophos XG Firewall for free at www.sophos.com/xgfirewall

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

200804 WPEN (TN)

SOPHOS