How to configure a firewall to block the WannaCry ransomware attack

The infosec (information security) community has a lot of good security measures to protect against ransomware attacks, including ransomware firewall best practices, antivirus tools, and ransomware protection strategies. .

The massive WannaCry ransomware attack, a form of malware, caused widespread damage globally in May 2017, affecting at least 150 countries and targeting banks, hospitals, and suppliers. telecommunications service providers and government organizations.

Hackers exploited operating system and zero-day vulnerabilities to launch these cyber threats. The infosec (information security) community has a lot of good security measures to protect against ransomware attacks, including ransomware firewall best practices, antivirus tools, and ransomware protection strategies. .

Let's take a closer look at what users need to know and the steps that can be taken to prevent this and other similar ransomware threats in the future!

Some basic information about WannaCry

The vulnerability that attackers are exploiting resides in the SMB component in Windows, part of the Microsoft operating system. Server Message Block (SMB) is a network protocol that provides file and printer sharing services in Windows systems. SMB can be used within a corporate network to share files and printers; however, it should never go beyond this network, especially through remote access over WiFi.

In fact, this is so strongly discouraged that in January 2017, the United States Computer Emergency Readiness Team (US-CERT) recommended blocking 'all instances of Server Message Block (SMB) at the network boundary by blocking TCP port 445 with associated protocols on UDP ports 137-138 and TCP port 139, for all devices in range', following multi-factor authentication best practices. This measure prevents the WannaCry attack and should be deployed on home and business firewalls, as part of Endpoint Protection measures.

How to prevent WannaCry ransomware attack

Configure all Perimeter Firewalls (or routers) (an imaginary virtual digital 'wall', set up on a network to keep out malicious actors) to block all access to port 445, like part of your cyber security strategy.

Some points to consider include:

1. Configure this rule on your Perimeter Firewall (also known as 'boundary' firewall). This will prevent any SMB traffic, including malware and ransomware, from entering or leaving the corporate network.

2. Some firewalls will only provide a 'Port' field - in this case configure the 'Port' field as described in the 'Destination Port' field above. Be sure to follow firewall best practices to block ransomware.
3. For zone-based firewalls and endpoint security measures (such as Palo Alto Networks and Fortinet), as well as firewalls that attach their policies or ACLs to network interfaces (such as Cisco ASA), you should configure 'source ' for external or untrusted zones/interfaces and 'target' to internal zones/interfaces.
4. The best approach is to block all access to TCP 445 at the beginning of the rule base to avoid accidentally opening it with less important rules.
5. You should also block port 445 on your internal firewall to segment your network and prevent lateral movement – ??this will prevent the internal spread of ransomware.
6. Note that blocking TCP 445 will prevent file and printer sharing, including across applications – if this is required for your business, you may need to leave the port open on some internal firewalls. set or use encryption key.
7. If you need to share files externally (for example, for home users), use or Remote Desktop protocol to provide access to it.
8. You may also want to block sensitive data with a host-based firewall like iptables, part of an advanced threat prevention system.