SONICWALL

EXECUTIVE BRIEF: IN THE WAKE OF WANNACRY

Anatomy of a ransomware attack

Abstract

Lack of initiative in taking best practices for network security frequently leads to devastating results. One recent headline-grabbing ransomware attack had a global impact. This brief examines how cyber criminals executed this attack, the ongoing challenges it still presents for IT and lessons learned to avoid future attacks.

A common story

It was an all-too-common story. Recently, cyber criminals breached a company's network via phishing a email that contained WannaCry ransomware. The email attachment was opened on an unpatched computer, which led to devastating consequences. When questioned about the unpatched system, the company's owner responded, "I didn't think the patch was very important."

Anatomy of an attack

When you consider how easily this company could have avoided the breach, it just makes you "*WannaCry*." That particular massive ransomware attack infected more than 250,000 systems in more than 150 countries, including several large healthcare institutions in the United Kingdom and even a couple of notable telecommunications companies in Spain.

WannaCry is just one example of threats that are a combination of ransomware and a worm that leverages an SMB file-sharing protocol exploit. It is speculated that initially, certain government agencies created an exploit kit (in this case, EternalBlue) which cyber criminals then allegedly stole.

In April 2017, Shadow Brokers leaked EternalBlue to the public as part of a bigger dump of NSA-developed exploits. Criminals then leveraged elements of that exploit kit in a new, extremely

While they are increasingly in the headlines, ransomware attacks are nothing new. Exploits are a daily occurrence. The "I didn't know" defense can only play out for so long.

aggressive form of ransomware that leverages a worm-like attack against connected network machines, using various read/write functions of the Windows Operating System. This particular exploit affects various versions of Microsoft Windows operating systems, including a number of versions that are in end-of-life status. Although Microsoft released a large number of patches to address this vulnerability, the attack remains dangerous, as many organizations have not applied the patch.

The first version of the worm/ransomware package had a kill switch that was accidently used to disable the worm feature, which slowed its advance. However, the more than 20 versions after the first do not have this weakness. Furthermore, it is important to employ technology that stops all known versions of ransomware as well as technology that can detect new ransomware attacks.

Conclusion

There are more than 114 new viruses and variants created every sixty seconds. *WannaCry* is certainly not the first exploit to leverage this form of attack and it certainly will not be the last. Organizations need to wake up to the new realities of the global cyber battlefield.

Learn more. Read our Solution brief: 7 best practices for stopping ransomware.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com

ExecBrief-InTheWakeOfWannaCry-US-VG-29362