Array Networks Blog

22 JUN, 17

The Dystopian New Normal Of Ransomware

POSTED IN UNCATEGORIZED BY EVELYN MILLER

1 COMMENT

In the IT world, it's become sort of a dystopian new normal to see massive, headline-grabbing network attacks, often on a global scale. The latest of these, just over a month ago, was WannaCry – which was estimated to have infected more than 200,000 computers worldwide in its first wave*. This ransomware/worm is particularly insidious as all it takes is one person on the network clicking on an email attachment or web link to launch it; once inside the network, it quickly spreads to other vulnerable devices on the intranet and internet.

However, ransomware like WannaCry, as well as certain other malwares, share a point of commonality that IT managers can leverage to better defend against them: In many cases, they exploit an operating system vulnerability. In the case of WannaCry, it is a Microsoft Windows vulnerability in the Server Message Block implementation (MS17-010).

Microsoft issued an advisory and patch for MS17-010 more than *two months* before WannaCry was ever detected, meaning that IT managers who were diligent about enforcing patch updates within their organization were for the most part immune.

That's the good news. The not-so-good news is twofold. WannaCry is still out there; there have been reports of new attacks as recently as June 8th and 9th. In addition, remote and mobile workers, contractors, vendors still need access to the corporate network, and often you don't (or can't) control their devices. If they're not patched, any of them can be a conduit that lets WannaCry and other ransomware into the network.

If you're using an enterprise-class SSL VPN like Array's AG Series, however, you have a security tool that can defend against unpatched and insecure devices getting onto your network and exposing your corporate resources to ransomware. The AG Series includes host checking, which can pre-scan devices before they ever connect to the network to ensure that the required service packs, firewalls, antivirus, and/or antispyware are present and up to date. In addition, custom rules can be written, and different communities of interest can be assigned different host check requirements (for example, remote workers versus vendors).

If a device fails the host check, network access is denied. Through the AG Series, ransomware like WannaCry is blocked before it ever gets onto the network.

While an SSL VPN can help protect one vector from ransomware attacks, Trapp Technology, an Array customer and partner, also offers a list of other tips to protect against WannaCry in their recent blog post, How to Keep Your Company Safe from the WannaCry Virus.

Unfortunately, this dystopian 'new normal' of ransomware is not going to go away. Ransomware attacks will continue to cause an untold amount of damage to valuable corporate resources as well as draining IT time and budgets. Fortunately, there are ways to strategically protect against WannaCry as well as against unauthorized and unsecure access.

*In a joint hearing of the U.S. House Oversight and Research and Technology subcommittees, a security industry vendor representative estimated that the number could be as high as one to two million devices worldwide.

Latest Tweets

Array's Management Platform (AMP) latest release offers new enhancements. AMP provides centralized #configuration,... https://t.co/VV5a54c4WJ
6 months ago

Using a #virtual #appliance to process traffic is a key #encryption strategy #enterprises can use to improve... https://t.co/okBrz2HxCf
6 months ago

@Interop attendees...Swing by booth 325 to see how to supercharge software-based #WAF & #NGFW solutions w/ Array's... https://t.co/2Vyu7sf5Cj
6 months ago

RT @cegasecurity: @ArrayNetworks y @CEGASecurity, estarán