Array Networks Blog

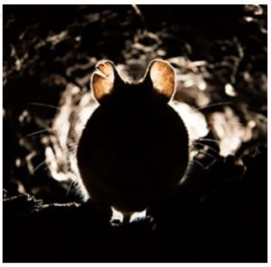
01
DEC, 16

0
COMMENT

RDP Under Attack: How To Protect Against Trojan.Sysscan

POSTED IN SSL VPN BY EVELYN MILLER

Share Share 0 print



The cat-and-mouse game of network security is constantly evolving, as hackers come up with new ways to get to the 'cheese' – the lucrative personal and corporate financial, tax and banking information that can pay off handsomely for the bad guys, while wreaking havoc on unwitting victims.

One of the latest malware/attack variants, disclosed just last month, is Trojan.sysscan. The scheme begins with brute-force attacks against Microsoft Remote Desktop Protocol (RDP) servers to steal credentials. Once successfully logged in, the Trojan itself is installed and then sets all RDP ports to remain open, thus allowing at-will access for theft of credentials, personal and corporate financial information, and more. Reports indicate the Trojan can easily evade detection, making this exploit even more dangerous.

In addition, there have been several recent reports of hackers leveraging RDP ports to deliver ransomware.

RDP is very popular as a means of giving users access to their desktop PCs anywhere, anytime via their mobile or other remote endpoint. However, this means that RDP ports are left open, often 24/7, to allow access by staff as needed. Compounding the problem, RDP servers are often connected directly to the Internet, without a front-end protection mechanism.

Various news articles on Trojan.sysscan advocate simply enforcing strong passwords to 'declaw' the entry method for this hack: the brute-force attack. However, the human factor of network security comes into play with this strategy. All it takes is one – just one – slip by an end user, and you could be spending hours or days remediating this Trojan.

Fortunately, there are a couple of methods that can eliminate the threat of RDP Trojans completely. If you're using an SSL VPN to authenticate and control access to your network, simply put your RDP servers behind it. As a bonus, Array's AG Series SSL VPN adds a couple of extra layers of protection. First, it doesn't expose the standard RDP port, thus veiling it from attackers. Second, once users authenticate with the AG Series, connections are proxied to the now-internal RDP server, meaning that RDP resources are neither exposed to nor connected directly to the Internet.

Another tactic to consider is eliminating Microsoft RDP entirely from your network. Array's DesktopDirect remote desktop access solution, an add-on module for the AG Series SSL VPN, protects data in transit via a custom remote desktop protocol as well as SSL encryption. With DesktopDirect, data never leaves the corporate network, and never resides on the remote device, so it is always secure. Users can see and work with their files and network resources similar to how they use Microsoft RDP, and the interface is so simple to use that no training is required.

DesktopDirect can also eliminate many of the headaches associated with managing and using Microsoft RDP. For example, user self-registration makes it easy for network administrators to roll out. Users can power up their office computer remotely via DesktopDirect's Wake-on-LAN technology.

In the old Tom and Jerry cartoons, the mouse almost always outsmarted the cat. By adopting a few new tactics, you can easily outsmart and defeat Microsoft RDP Trojans and other malware.

Stay Connected

Subscribe by Email

E-mail

□ unsubscribe

Submit

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 exhibiendo la #AVXSeries y otras #tecnologías de #ciberseguridad en... https://t.co/kCHUJznxC3