August 28, 2011, 1:20PM

New Worm Morto Using RDP to Infect Windows PCs (/en_us/blogs/new-worm-morto-using-rdp-infect-windows-pcs-082811)

by Dennis Fisher (/author/DennisFisher)

A new worm called Morto has begun making the rounds on the Internet in the last couple of days, infecting machines via RDP (Remote Desktop Protocol). The worm is generating a large amount of outbound RDP traffic on networks that have infected machines, and Morto is capable of compromising both servers and workstations running Windows.

Users who have seen Morto infections are reporting in Windows help forums (http://socialtechnet.microsoft.com/Forums/en-US/winserversecurity/thread/31cf740c-818c-4863-8df9-0d9a1d6de6fc) that the worm is infecting machines that are completely patched and are running clean installations of Windows Server 2003.

"In a new windows 2003 R2 server, I'm noticing every few minutes, svshost.exe [sic] is opening a ton of outgoing TCP 3389 connections. I ran an a/v scanner over it and it's clean. Can it be hacked already??? has anyone seen this before?," one user asked in Microsoft's TechNet forum.

Editor's Pick

Weaknesses in Webkit Becoming Problematic (/en_us/blogs/weaknesse-webki-becomin-problemati-082811)

Microsoft Releases New Versions of Software Security Tools (/en_us/blogs/microso-release-

On Sunday, the SANS Internet Storm Center (http://isc.sans.edu/diary.html?storyid=11452&rss) reported a huge spike in RDP scans in the last few days, as infected systems have been scanning networks and remote machines for open RDP services. One of the actions that the Morto worm takes once it's on a new machine is that it scans the local network for other PCs and servers to infect.

"A few weeks ago a diary (http://isc.sans.edu/diary.html?storyid=11299) posted by Dr. J pointed out a spike in port 3389 (https://isc.sans.edu/port.html?port=3389) traffic.

new-version-software-security-tools-08251)

PHP 5.3.8 Released, Fixes Crypto Bug (/en_us/blogs/php-538-released-fixes-crypto-bug-08241)

Threatpost Newsletter Sign-up (/en_us/node/1690)

Since then the sources have spiked ten fold. "This is a key indicator that there is an increase of infected hosts that are looking to exploit open RDP services." SANS handler Kevin Shortt said in a blog post.

Researchers at F-Secure said that Morto is the forst Internet worm to use RDP as an infection vector. Once it's on a new machine and has successfully found another PC to infect, it starts trying a long list of possible passwords for the RDP service.

"Once a machine gets infected, the Morto worm starts scanning the local network for machines that have Remote Desktop Connection enabled. This creates **a lot of traffic for port 3389/TCP**, which is the RDP port," F-Secure Chief Research Officer Mikko Hypponen (http://www.f-secure.com/weblog/archives/00002227.html) said in a blog post.

"Once you are connected to a remote system, you can access the drives of that server via Windows shares like **tsclient\c** and **tsclient\d** for drives **C:** and **D:**, respectively. Monto uses this feature to copy itself to the target machine. It does this by creating a temporary drive under letter A: and copying a file called **a.dll** to it. The infection will create several new files on the system including **windows\system32\sens32.dll** and **windows\offline web pages\cache.txt**. Morto can be controlled remotely. This is done via several alternative servers, including **jaifr.com** and **qfsl.net."**

It's been quite a while since there was a large-scale Internet worm attack. Once upon a time, worms such as Blaster, Code Red and SQL Slammer (http://threatpost.com/en_us/blogs/insidestory-sql-slammer-102010) were all the rage and found success clogging networks with enormous amounts of scanning traffic and other activity. But those kinds of events have become an anachronism as attackers have turned the attention to for-profit attacks.

Comments

Submitted by Anonymous (not verified) on Sun, 08/28/2011 - 4:08pm.

\\tsclient\c d etc are the connecting CLIENT not the server...

Submitted by Anonymous (not verified) on Sun, 08/28/2011 - 7:00pm.

"Once it's on a new machine and has successfully found another PC to infect, it starts trying a long list of possible passwords for the RDP service."

So brute force password guessing is the only infection method?

There is no serious flaw in the M$ RDP server we need to know about?

Sounds as if picking passwords like: "$Tr{}|\|GP@$$^^()rd" and not "strongpassword" will protect your server from this worm.

Submitted by Anonymous (not verified) on Sun, 08/28/2011 - 7:16pm.

Obvious vector is obvious: Weak passwords are weak.

Submitted by Anonymous (not verified) on Sun, 08/28/2011 - 7:17pm.

Obvious vector is obvious: Weak passwords are weak.