Worm:Win32/Morto.A

Published Aug 27, 2011 | Updated Sep 15, 2017

Learn about other threats

Detected by Microsoft Defender Antivirus
Aliases: Trojan horse Generic24.OJQ (AVG) Trojan.DownLoader4.48720 (Dr.Web) Win-Trojan/Helpagent.7184 (AhnLab) Troj/Agent-TEE (Sophos) Backdoor:Win32/Morto.A (Microsoft)

Summary

Microsoft Defender Antivirus detects and removes this worm.

This threat is a worm that allows unauthorized access to an affected computer. It spreads by trying to compromise administrator passwords for Remote Desktop connections on a network.

Worms automatically spread to other PCs. They can do this in a number of ways, including by copying themselves to removable drives, network folders, or spreading through email.

Find out ways that malware can get on your PC

Additional information for Enterprise users

In the wild, we have observed this threat infecting computers by targeting accounts that have weak passwords.

To help prevent infection, and consequent reinfection, make sure that your organization uses strong passwords for system and user accounts, and verifying that you do not use passwords like those being used by the malware in order to spread. **Changing your password will significantly decrease your chance of re-infection.**

To thwart this and similar threats, it helps to adhere to best password practices, defined and enforced by appropriate policies. Good polices include, but are not limited to:

- Ensuring there are rules around password complexity, so that passwords meet basic strong password requirements, such as minimum length (long passwords are usually stronger than short ones)

- Ensuring passwords are not used for extended periods of time; consider setting an expiry every 30 to 90 days. You might also consider enforcing password history, so that users can not re-use the same password within a pre-defined time frame
- Ensuring passwords contain a combination of:
    - Uppercase letters
    - Lowercase letters
    - Numerals, and
    - Symbols

For general information about password best practices, please see the following articles:

To help prevent re-infection after cleaning, you may also want to consider changing the password for every account on the network, for every user in your environment.

Use the following free Microsoft software to detect and remove this threat:

You should also run a full scan. A full scan might find hidden malware.

Disable Autorun

This threat tries to use the Windows Autorun function to spread via removable drives, like USB flash drives. You can disable Autorun to prevent worms from spreading:

> Disable Windows Autorun

Scan removable drives

Remember to scan any removable or portable drives. If you have Microsoft security software, see this topic on our software help page:

> How do I scan a removable drive, such as a USB flash drive?

Use cloud protection

The Microsoft Active Protection Service (MAPS) uses cloud protection to help guard against the latest malware threats. It's turned on by default for Microsoft Security Essentials and Windows Defender for Windows 10.

> Check if MAPS is enabled on your PC

Get more help

You can also see our advanced troubleshooting page for more help.

If you're using Windows XP, see our Windows XP end of support page.
