

# Worm:Win32/Morto.A threat description - Microsoft Security Intelligence

By Microsoft Corporation

Archived: 2026-04-05 20:46:37 UTC

Published Aug 27, 2011 | Updated Sep 15, 2017

[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:

- [http://technet.microsoft.com/en-us/library/cc784090\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc784090(WS.10).aspx)
- [http://technet.microsoft.com/en-us/library/cc756109\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc756109(WS.10).aspx)

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.

---

Source: <https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Morto.A>