Quadrox Security Bulletin

KB-0075-W32.Downadup (Conflicker)

GENERAL

Distribution	**OEM/Partner/Distributor**	**Installer**	**Customer**
	YES	YES	YES
Last Update	30-03-2009		
Product	All OS		
Version	All		

DESCRIPTION

Quadrox wants to inform/warn you about a possible critical external threat for all WebCCTV/Guard systems.

W32.Downadup (Conflicker) is a worm that propagates on local and network drives by taking advantage of the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability. W32.Downadup can create its own Service on Windows to run itself each time Windows is started.

More information:

- http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
- http://en.wikipedia.org/wiki/Conficker
- http://discuss.50plus.com/ipb/index.php?showtopic=20389 (Source: NY Times)
- http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9126205

This article informs you about the proper actions to take in order to prevent/solve the problem. Please don't wait and take immediate action…

SOLUTION

How can you check if your system has been infected?

- Open your browser and open one of the following three sites:
  - http://microsoft.com
  - http://symantec.com
  - http://mcafee.com

  If the sites load without problems, it seems your system is not affected.

Which steps do you need to take?

- Your system is **not affected**:
  - Run Microsoft Windows Auto Update
  - If you don't want to do a full Auto Update, please run KB958644 from Microsoft (http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx)

- Your system is **affected**:
  - Enigma's Conflicker removal tool:
    http://www.enigmasoftware.com/conficker_removal_tool_more_info.php
  - BitDefender Conflicker removal tool:
    http://www.f-secure.com/v-descs/worm_w32_downadup_a.shtml
  - Microsoft's removal tool:
    Microsoft's removal tool http://onecare.live.com/site/en-us/default.htm

The Enigma, BitDefender and Microsoft tools work because Conflicker doens't have their URL blacklisted inside the worm. This may change as Conflicker mutates, but for now the removal tool is available (and free).