Trojan-Downloader:W32/Chymine.A | F-Secure

Archived: 2026-04-05 22:52:59 UTC

Classification

Type:Trojan-Downloader

Aliases:

Trojan.Autorun.ATA, Trojan-Downloader.Win32.Tiny.cmq , Trojan-Dropper:W32/Agent.DKBV, Backdoor.Trojan (Symantec), Trojan:Win32/Chymine.A (Microsoft)

Summary

Trojan-Downloader:W32/Chymine.A exploits a recently discovered vulnerability (CVE-2010-2568) in Microsoft Window's handling of shortcut icons in order to execute a file and drop a keylogger component on the affected machine. The keylogger is capable of capturing keyboard strokes entered into the infected system.

For more information on the vulnerability, please refer to Microsoft Security Bulletin 2286198 (http://www.microsoft.com/technet/security/advisory/2286198.mspx).

Removal

Based on the settings of your F-Secure security product, it will either move the file to the **quarantine** where it cannot spread or cause harm, or **remove** it.

A False Positive is when a file is incorrectly detected as harmful, usually because its code or behavior resembles known harmful programs. A False Positive will usually be fixed in a subsequent database update without any action needed on your part. If you wish, you may also:

- **Check for the latest database updates**

  First, check if your F-Secure security program is using the latest updates, then try scanning the file again.

- **Submit a sample**

  After checking, if you still believe the file is incorrectly detected, you can submit a sample of it for re-analysis.

  Note: If the file was moved to **quarantine**, you need to collect the file from quarantine before you can submit it.

- **Exclude a file from further scanning**

If you are certain that the file is safe and want to continue using it, you can exclude it from further scanning by the F-Secure security product.

Note: You need administrative rights to change the settings.

Technical Details

Execution

The actual exploit is performed by a shortcut (.LNK) file detected as Exploit:W32/Wormlink.B. On execution, the exploit loads the downloader component (the actual file detected as Trojan-Downloader:W32/Chymine.A) from a shared folder shared over the Internet:

- \205.209.171.[...]\DlaT\GdWbpvo.dll

Which in turn downloads an EXE file (detected as Trojan-Spy:W32/Chymine.A) from a remote site:

- http://205.209.171.[...]/bin.exe

To a temporary file. During execution, the malware creates a file on the system, where the downloaded bin.exe file drops a DLL file, the actual keylogger component. In the sample we analyzed, the created file was:

- %windir%\system32\[5250].dll

The file name, in this instance [5250], may be a random number. This DLL component (and its file) is also detected as Trojan-Spy:W32/Chymine.A.

Registry

In order to run, the keyloggger component makes changes to a number of registry keys and injects code into a number of processes. The malware also creates the following launchpoints, which are involved in launching the keylogger component:

- HKLM\SYSTEM\CurrentControlSet\Services\Iprip\Parameters ServiceDll = .\5250~1\ by %windir%\system32\rundll32.exe [Launchpoint: ServiceDll]
- HKLM\System\CurrentControlSet\Services\Iprip ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs by %windir%\system32\services.exe [Launchpoint: Service]

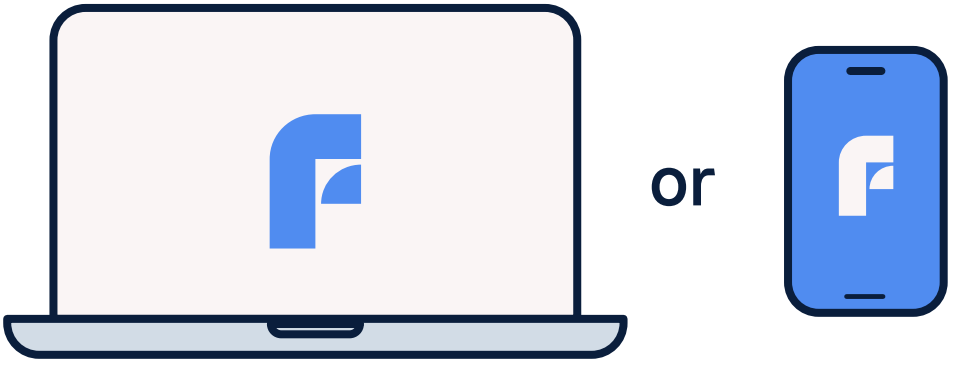
Protect your devices from malware with F-Secure Total

Protecting your devices from malicious software is essential for maintaining online security. F-Secure Total makes this easy, helping you to secure your devices in a brilliantly simple way.

- Award-winning antivirus and malware protection
- Online browsing, banking, and shopping protection
- 24/7 online identity and data breach monitoring
- Unlimited VPN service to safeguard your privacy

- Password manager with private data protection

Choose how many devices you want to protect to get started.



- Free customer support
- Cancel anytime
- The trial does not obligate you to buy the product

Try Total 30 days for freeAfter 30 days your subscription will renew automatically for one year at €69.99.

- Free customer support
- Cancel anytime
- The trial does not obligate you to buy the product

Try Total 30 days for freeAfter 30 days your subscription will renew automatically for one year at €89.99.

- Free customer support
- Cancel anytime
- The trial does not obligate you to buy the product

Try Total 30 days for freeAfter 30 days your subscription will renew automatically for one year at €99.99.

More Support

Contact Support

Chat with with or call an agent.