Swen (computer worm)

Swen

Common name	Swen worm
Technical name	Win32/Swen
Aliases	• Win32/Swen.worm.106496 (AhnLab) • W32/Swen.A@mm (Authentium Command) • I-Worm/Swen.A (AVG) • Win32/Swen.A@mm (BitDefender) • Win32/Swen.A.Worm (CA) • Win32/Swen.A (ESET) • Email-Worm.Win32.Swen (Kaspersky) • W32/Swen@MM (McAfee) • W32/Swen.A@mm (Norman) • W32/Gibe.C.worm (Panda) • W32/Gibe-F (Sophos) • Email-Worm.Win32.Swen (Sunbelt Software) • W32.Swen.A@mm (Symantec) • WORM_SWEN.A (Trend Micro) • I-Worm.Swen.A1 (VirusBuster)
Type	Computer worm
Subtype	Mass mailer
Point of isolation	September 18, 2003
Operating system(s) affected	Windows 95 to Windows XP
Filesize	106-496 bytes

Swen is a mass mailing computer worm written in C++. It sends an email which contains the installer for the virus, disguised as a Microsoft Windows update, although it also works on P2P filesharing networks, IRC and newsgroups' websites. It was first analyzed on September 18, 2003, however, it might have infected computers before then. It disables firewalls and antivirus programs.

Infection

Self-installation

The virus first sends itself via email with an attachment, posing as an update for Windows. The attachment can have a .com, .scr, .bat, .pif, or .exe file extension. If its file name starts with the letters P, Q, U, or I, It displays a fake Microsoft Update dialogue box, asking if the user wants to install a Microsoft Security Update with the two choices "Yes" and "No". If the user presses "Yes", it displays a fake progress bar while installing the fake update. When finished, it displays another dialogue box saying: Microsoft Internet Update Pack This has been successfully installed. The malware then re-executes itself, followed by yet another dialogue box saying: Microsoft Security Update Pack This update does not need to be installed on this system. If the user chooses "No", the malware will still install itself silently in the background. Next, it checks for certain criteria by opening another dialogue box, prompting the user for their email address, username, password, SMTP and POP3 server addresses. After completing the said fields, the worm then makes a copy of itself in the `C:\Windows` folder as `<random characters>.exe`. The virus finally moves all information to the copy and terminates.

Autostart

The worm creates the following registry entry to execute upon startup: `{{{1}}}`

References

Retrieved from "https://en.wikipedia.org/w/index.php?title=Swen_(computer_worm)&oldid=1052904739"