

Video: Keyloggers 101

Dan Honkanen, GCIH, Security+, ITIL, et al

Keyloggers are usually one of the top picks for a hacker or a spy's best friend. They basically serve as the eyes and ears of the attacker. They can be based on software or hardware and send detailed reports including the user's passwords, chat logs, all typed text, launched applications and visited websites. They can even send screenshots to visually show what the user was viewing as well as any webcam and microphone activity. Most laptops today come with a built-in webcam and microphone and don't usually give any signal that they have been enabled. Any person who uses that computer will have all their activities monitored and recorded in an encrypted log which only the attacker can access.

In this video, I will present the basics of keyloggers and also demonstrate a couple of my favorite keyloggers, their features, how hidden they are and how to prevent and detect keyloggers in general. At the end of this primer, the viewer should be able to fully understand where keyloggers fit into both sides of the equation.

Discuss in Forums {mos_smf_discuss:Special Events}

Resources

Software (commerical) Keyloggers:

All in One - <http://www.relytec.com>

SpyTech SpyAgent - <http://www.spytech-web.com/spyagent.shtml>

Micro Keylogger - <http://www.microkeylogger.com/>

Software (free) Keyloggers:

Ardamax - <http://www.ardamax.com/download.html>

Ghost Keylogger - http://download.cnet.com/Ghost-Keylogger/3000-2092_4-10040186.html

SpyOutSide - <http://www.brothersoft.com/spyoutside-25772.html>

Detection/Prevention Tools:

Key Scrambler - <http://www.qfxsoftware.com/>

Spy Shelter - <http://www.spyshelter.com/>

Prevx 3 - <http://www.prevx.com/freescan.asp>

Dan Honkanen has worked in Technical Support and on the Malware Removal Team with Dell and HP but more recently has been working with the BC Government for the past 4 years as a Technical Analyst (all around Techie working in Tier 3 application support, networking and server work). On the side, he does data recovery jobs and volunteers with www.haltabuse.org as an Internet Safety Advocate. He has attained SANS GCIH, Security+, Network+, A+, MCP, DCSE and ITIL. His main interests are Martial Arts, ocean sports, travel and ethical hacking.