Researcher Reveals 2-Step Vista UAC Hack

May 17 2007

The technique uses social engineering to trick the victim into downloading an innocent-looking file that includes a Trojan horse attack.

A Web application developer has uncovered a two-step process (PDF) for exploiting Windows Vista's User Account Control, essentially by having a Trojan piggyback on what could be a legitimate download.

Robert Paveza, a senior Web application developer with Terralever, a Web-based marketing company based in Tempe, Ariz., published details of the vulnerability in a paper titled "User-Prompted Elevation of Unintended Code in Windows Vista."

Paveza said in the paper that the vulnerability uses a two-part attack vector against a default Vista installation. The first step requires that malware called a proxy infection tool be downloaded and run without elevation. That software can behave as the victim expects it to while it sets up a second malicious payload in the background.

"For instance, if users believe they are downloading a 'Pac-Man' clone, such a game could be run while the malicious software did its work in the background," Paveza said. He noted that the infection succeeds, for all intents and purposes, with the installation of the proxy infection tool.

"This pattern of infection follows the typical Trojan horse model, piggybacking on what may be otherwise legitimate software," he said.

News of the vulnerability first broke May 15. When eWEEK that day contacted Microsoft, based in Redmond, Wash., a spokesperson said the company is aware of demonstrations that "purport" to show how a Vista system can be attacked. But, the spokesperson said, the demonstration provided by Paveza is of actions an attacker can take on a system that already has been compromised by another means.

"With this in mind, it is important to note that user interaction is required for the initial infection of the Trojan to occur," the spokesperson said. "The user must open the attacker's malicious executable. Furthermore, the successive social engineering attempt will only be successful if the user inadvertently clicks on the malicious shortcut. In fact, at this point, the user must be part of the local administrator's group or provide administrator credentials at the UAC prompt."

The spokesperson went on to point to Microsoft's previous communications regarding running as a standard user. "Remember that running as a standard user does not prevent malicious software from copying itself to locations controlled by this user, such as the user's profile directory," Michael Howard and David LeBlanc noted in "Writing Secure Code for Windows Vista."

As far as UAC being vulnerable to social engineering attacks goes, that's old news. Joanna Rutkowska offered constructive criticism of UAC in her blog on Feb. 4, and Ollie Whitehouse, a research scientist for Symantec, based in Cupertino, Calif., followed with a Feb. 20 posting titled An Example of Why UAC Prompts in Vista Can't Always Be Trusted.

Shortly thereafter, a Microsoft spokesperson told eWEEK that UAC was indeed susceptible to social engineering attacks.

But as Whitehouse said to eWEEK at the time, UAC isn't a security boundary - not a hard one, at any rate. "UAC is not like a firewall, which is a hard security boundary, between your PC and the untrusted Internet," he said. "UAC seems to be more of a security function, but not a boundary. It's useful as a tool to help users but - shouldn't be - seen as impervious."