Internet Explorer users are warned against Poison Ivy

18 September 2012, by Nancy Owano

(Phys.org)—More than a few Internet Explorer users stand vulnerable to fresh attacks of Poison Ivy. In the latest headline in the "Internet Explorer has a flaw" saga, a security hole in Internet Explorer 7,8, and 9 is being exploited. Attackers can spring a back-door Trojan on an IE browser victim's computer. The Trojan is known as Poison Ivy. Security researchers say the IE hole is new to them. They say the attacks have already taken place. Eric Romang, a security researcher, spotted the flaw a few days ago and blogged that a potential Microsoft Internet Explorer 7 and 8 zero-day is actually exploited in the wild.

Rapid7, a security company, said it was a zero-day exploit making Internet Explorer 7, 8, and 9 vulnerable on Windows XP, Vista and 7 systems. Computer users can experience attacks if they visit a malicious website, which hands over privileges to the attacker. The attacker can run code of his choice in the context of the user. The attacker can delete or add files or change registry values. Security experts, like Rapid7, are advising business and general consumer users to avoid Internet Explorer until Microsoft issues a patch. Rapid 7 offered advice for Internet users to switch to other browsers such as Chrome or Firefox while waiting for a security update. HD Moore, CSO of Rapid7, said, though, that avoiding the browser might not even be enough, as many applications rely on the IE engine to render HTML.

The exploit had already been used by malicious attackers in the wild but Rapid7 on Monday released an exploit module for Metasploit to allow security teams to get closer to the situation. Security experts can use it to simulate attacks that exploit the security flaw in Internet Explorer. They can see if their own corporate networks are vulnerable. Metasploit is a collaboration between the open source community and Rapid7.

"We have added the zero-day exploit module to Metasploit to give the security community a way to test if their systems are vulnerable and to develop counter-measures," according to Rapid7.

Security watchers believe that the attacks are being made by the same people who previously figured out how to exploit a vulnerability in Oracle's Java framework. Security sleuths peg the IE exploits on the China-based group called Nitro, a group that first made news last year when Symantec said they had done their mischief at 48 businesses.

Romang said the zero-day season is not over yet. Microsoft said it is investigating reports of the bug.

In the near term, as an interim step, Microsoft is urging Windows users to install free software designed to protect the Internet Explorer browser. The tool is called Enhanced Mitigation Experience Toolkit, or EMET. Microsoft says it as designed to help prevent hackers from gaining access to your system. "The toolkit includes several pseudo mitigation technologies aimed at disrupting current exploit techniques," according to Microsoft. "These pseudo mitigations are not robust enough to stop future exploit techniques, but can help prevent users from being compromised by many of the

exploits currently in use."

More information:
www.rapid7.com/downloads/metasploit.jsp
www.microsoft.com/en-us/downlo …
etails.aspx?id=29851