Hackers target European governments via Adobe bug: researchers

Jim Finkle, Reuters

(Reuters) - Hackers targeted dozens of computer systems at government agencies across Europe in a series of attacks that exploited a recently discovered security flaw in Adobe Systems Inc's software, security researchers reported on Wednesday.

Russia's Kaspersky Lab and Hungary's Laboratory of Cryptography and System Security, or CrySyS, said the targets of the campaign included government computers in the Czech Republic, Ireland, Portugal and Romania.

They also said that a think tank, research institute and healthcare provider in the United States were among those targeted by the malicious software, which they have dubbed "MiniDuke".

The MiniDuke hackers attacked their victims by exploiting recently discovered security bugs in Adobe's Reader and Acrobat software. They sent their targets PDF documents tainted with malware, an approach that hackers commonly use to infect PCs.

The two research groups declined to elaborate on the identity of the victims, but said they have reported the case to relevant authorities.

Boldizsár Bencsáth, a cyber security expert who runs the malware research team at CrySyS, told Reuters he believed the attackers installed "back doors" at dozens of victim organizations that would enable them to view information on those systems, then siphon off data they found interesting.

He said researchers have yet to uncover evidence that the operation had moved on to a second stage, where the operators had begun to exfiltrate data from their victims.

"This is a unique, fresh and very different type of attack," said Kurt Baumgartner, a senior security researcher with Kaspersky Lab. "The technical indicators show this is a new type of threat actor that hasn't been reported on before."

He said he would not speculate on who that actor -- the hackers -- might be.

Bencsáth, however, said he believed a nation state was behind the attack because of the level of sophistication and the identity of the targets, adding that it was difficult to identify which country was involved.

The MiniDuke hackers exploited security bugs in Reader and Acrobat software that were first identified two weeks ago by Silicon Valley security firm FireEye. The firm

reported that hackers were infecting machines by circulating PDFs tainted with malicious software.

Adobe last week released an update that fixes the security bugs in Reader and Acrobat.

Bencsáth said that the hackers discovered by FireEye had used tainted PDFs that appeared to be applications for visas to enter Turkey.

The MiniDuke hackers also employed several seemingly innocuous documents, including research papers on Ukraine's foreign policy and one on a human rights seminar.

(Editing by Jeremy Laurence)

Source URL (retrieved on *12/20/2013 - 6:50pm*):
http://www.ecnmag.com/news/2013/02/hackers-target-european-governments-adobe-bug-researchers?qt-video_of_the_day=0