Cyber Weapon 'Flame' required world-class cryptanalysis

by Lucian Constantin via lynx - ComputerWorld *Friday, Jun 8 2012, 11:59am*
international / mass media / other press

narrows the field of responsibility to a large extent

> Flame's authors used a previously unknown MD5 collision attack variant, cryptoanalysts say.

The Flame cyber-espionage malware makes use of a previously unknown cryptographic attack variant that required world-class cryptanalysis to develop, experts from the Dutch national research center for mathematics and computer science (CWI) said on Thursday.

The cryptographic attack, known as an MD5 chosen prefix collision, was used by Flame's creators to generate a rogue Microsoft digital code-signing certificate that allowed them to distribute the malware to Windows computers as an update from Microsoft.

Microsoft's security engineers explained how the MD5 collision attack worked in a blog post on Wednesday. In their article, they referenced older chosen prefix collision research by cryptanalysts Marc Stevens, Arjen Lenstra, and Benne de Weger.

Stevens, Lenstra and de Weger were part of a larger international team of researchers who, in 2008, demonstrated a practical MD5 collision attack which allowed them to create a rogue SSL certificate trusted by all browsers.

Stevens, who is a scientific staff member in the cryptology group at CWI, analyzed the rogue Microsoft certificate used by Flame's authors and determined that they used a different MD5 collision attack than the one devised by him and his colleagues in 2008. "The design of this new variant required world-class cryptanalysis," Stevens said in a blog post on Thursday.

Ronald Cramer, the head of the cryptology research group at CWI and professor at the Mathematical Institute of Leiden University in the Netherlands agreed with Stevens' assessment. "This is not a job done by amateurs," he said.

Furthermore, the fact that Flame's creators used an MD5 collision attack different than the one developed by Stevens and his colleagues, suggests that the two variants might have been designed in parallel.

From a practical point of view it would have made no difference had they used Stevens' attack instead, Cramer said.

Both attacks could have generated rogue Microsoft code-signing certificates that would have tricked

Windows systems. The difference between them lies in the math used, not the end result.

One reasonable explanation why Flame's creators didn't used Stevens' attack is that they developed their own variant before Stevens and his colleagues published their research in 2008, Cramer said.

This theory is also supported by other evidence, according to which Flame was developed in the second-half of 2008, and enforces the idea that Flame was created by a professional team of developers with a lot of resources.

Interestingly, the attack would have failed a long time ago if Microsoft had been more diligent. "We, at the time, notified Microsoft and all other parties affected in this context, so they could take measures," Cramer said.

In December 2008 Microsoft issued a security advisory which recommended that administrators and certificate authorities cease using MD5 as an algorithm to sign digital certificates because of collision attacks. However, the company failed to disable the use of MD5 in parts of its own operating system, which is what Flame exploited, Cramer said.

Following the discovery of the Flame attack Microsoft revoked three of its Terminal Server certificate authorities and announced other changes to the Terminal Service certificate infrastructure to prevent similar abuse in the future.

http://tinyurl.com/77qeqvv
