APTs Target Mac Users

The facts are in, and the malware myth that Mac users are not at risk from advanced persistent security threats has been busted.

By Sean Michael Kerner | October 03, 2012

TORONTO: Seth Hardy sees more than his fair share of malware in any given day. Hardy, who works for The Citizen Lab at the Munk School of Global Affairs, tracks security attacks on vulnerable non-governmental organizations (NGOs).

In a talk delivered at the SecTor security conference here, Hardy revealed that despite myths to the contrary, Mac users are being specifically targeted by Advanced Persistent Threats (APTs).

"The question 'Are Mac users no longer safe' is a trick question, because you were not safe to begin with," Hardy told the capacity audience.

He explained that The Citizen Lab looks at targeted threats against human rights organizations. As such they have somewhat limited visibility, though the attacks he has seen are highly targeted. "Citizen Lab's visibility is deep but not wide. But we are getting malware directly from sources that receive it along with the context of how they were delivered," he said. At a high level, Hardy defined APT as "something we weren't able to see, block or deal with."

Revir/IMULER Malware

One of the APT malware attacks Hardy has seen over the past year is the Revir/IMULER attack, which involves a zip file with content relevant to the receiving organization. Hardy noted that the file contained legitimate information with a link to a real website. It also had an application in it that showed an image of a t-shirt. When clicked, the image contacts a command and control server and drops a malicious payload.

Hardy said Revir/IMULER follows a common APT pattern of using real information to get people to click on files that appear to be coming from real people.

What was particularly troubling is that most virus scanners were not able to pick up the payload or the attack. Hardy noted that only 14 out of 43 anti-virus scanners on VirusTotal were able to detect the Revir/IMULER malware.

While initial detection of Revir/IMULER isn't easy, figuring out what the payload does is another story. Hardy showed the code for the malware, which included real function names, as opposed to some form of obfuscation. That is, the APT authors for Mac have done nothing to hide what their code is doing.

"All the Mac malware stuff we look at keeps additional information about what the code is doing, making reverse engineering really easy," Hardy said.

More Mac Attacks

The Olyx/Lamadai/Sadpab Mac APT family is directly related to CVE-2011-3544, which is an Oracle Java

vulnerability. Apple did not patch the flaw until some four months after Oracle has already provided a public fix. Hardy noted that with Sadpab, the victim gets a link that directs the user to Web pages with Java .jar files that take advantage of the Java vulnerability.

"Sabpab is seen by organizations that are regularly targeted," Hardy said. "We'll probably see more of this one in the future."

The Maccontrol APT attack is another piece of malware that has been bundled into a zip file. It is similar to other forms of Mac malware in that it has a hardcoded link to the APT author's command and control center. Hardy said Maccontrol is still an ongoing threat, with multiple generators sending out material.

A piece of malware called Davinci is a bit different than other Mac attacks in that it is sold to law enforcement. Hardy described Davinci as "the best Mac malware that $200,000 can currently buy." Hardy warned that even though it is only sold to law enforcement, it is active and can be used for potential harm.

Hardy's key takeaway was that more Mac APTs are coming. "This is a new space, people are building up their tools and authors, and just getting started," he said. "Targeted groups will not stop being targeted."

Hardy suggests that Mac users (and everyone else) should always remain vigilant when clicking on any attachment or link. In his view, a good best practice is to use a trusted service such as Google Drive to open and share items.

Sean Michael Kerner is a senior editor at eSecurity Planet and InternetNews.com, the news service of the IT Business Edge Network. Follow him on Twitter @TechJournalist.