MUST READ Cracka hackers who doxed CIA Chief, now hit the FBI Deputy Director

Mabouia: The first ransomware in the world targeting MAC OS X

November 5, 2015 By Pierluigi Paganini

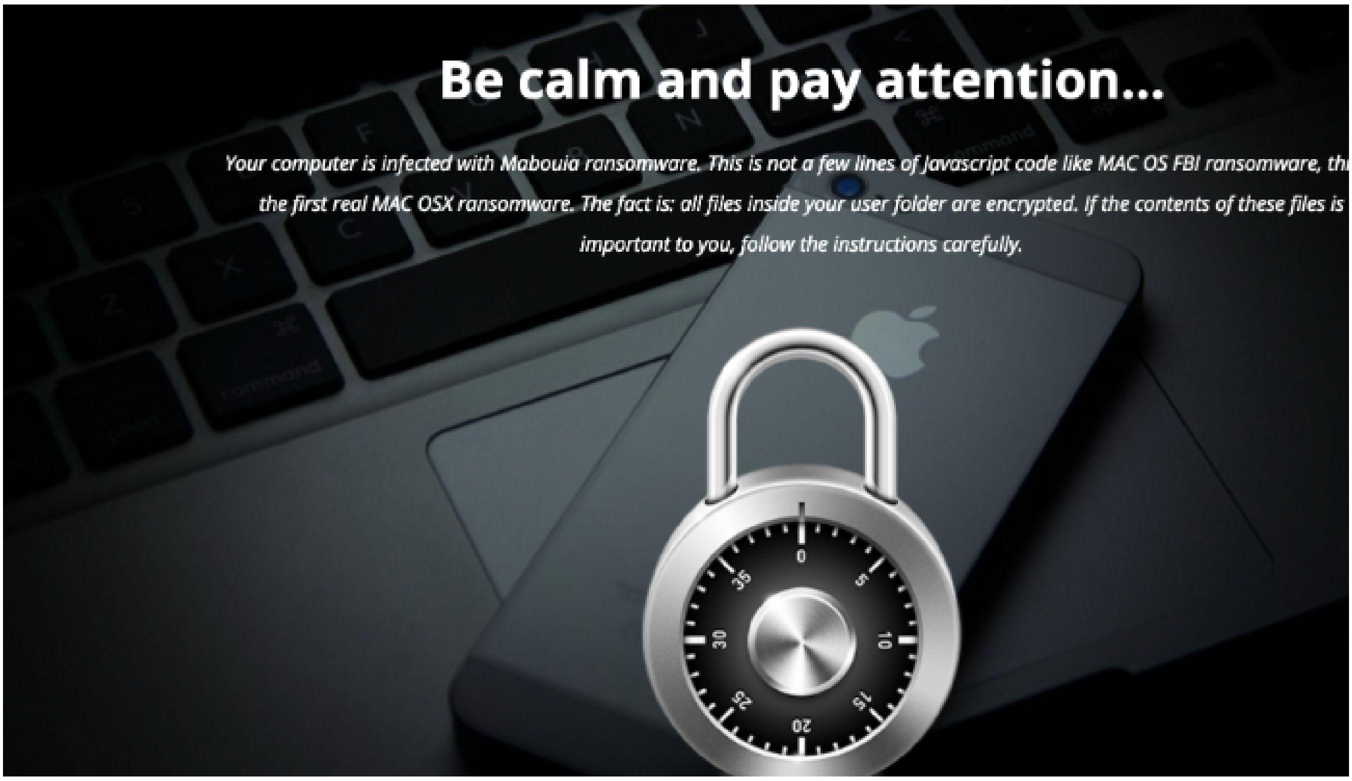
Rafael Salema Marques, a Brazilian researcher, published a PoC about the existence of Mabouia ransomware, the first ransomware that targets MAC OS X.

Imagine this scenario: You received a ransom warning on your computer stating that all your personal files had been locked. In order to unlock the files, you would have to pay $500.

This is the “modus operandi” imposed usually used by ransomware (ransom +software).

Ransomware encrypts files that are virtually impossible to decrypt with the computing means available to ordinary users. The only way to decrypt the files is paying to the malware creator to retrieve the password that unlocks the files… Which is exactly what you would do if I had not held up important files.

The definition of ransomware according to Wikipedia is as follows: “type of malware that restricts access to a computer system that it infects in some ways, and demands that the user pay a ransom to the operators of the malware to remove the restriction.” There are several actives ransomware in the world today, but no one had ever been designed to target Mac OS X until yesterday.



Be calm and pay attention...

Your computer is infected with Mabouia ransomware. This is not a few lines of Javascript code like MAC OS FBI ransomware, th
the first real MAC OSX ransomware. The fact is: all files inside your user folder are encrypted. If the contents of these files is
important to you, follow the instructions carefully.

Rafael Salema Marques (@pegabizu), a Brazilian Cybersecurity Researcher, published yesterday a proof of concept about the existence of Mabouia ransomware, the first ransomware that targets MAC OS X.

The researcher’s goal is to alert the 66 million users of Mac OS X about the myth that there is no malware aimed at Apple’s personal computers.

The creator of the malicious code also mentions that Mac users are a good target for ransomware, because generally have a higher purchasing power and use the computer in a superficial way, usually by editing images and texts.

The malware name Mabouia refers to a kind of endemic lizard found on the island of Fernando de

Noronha – Brazil. Is coded in C++ and uses the cryptographic algorithm XTEA with 32 rounds to encrypt the user files. Furthermore, it does not need superuser privileges for the execution of malicious code, considering that the ransomware will only modify the user's personal files. Thus

About the Author Rafael Salema Marques (@pegabizu)

Rafael Salema Marques is a Brazilian Cybersecurity Researcher. He is a developer who is always seeking knowledge related to programming and Cybersecurity.

Edited by Pierluigi Paganini

(Security Affairs – Mabouia ransomware, malware)

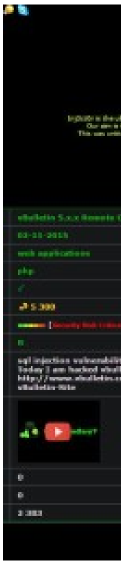
Share it please ...

Share this:

Email | Twitter 50 | Print | LinkedIn 71 | Facebook 96 | More

Cybercrime | Hacking | Mabouia | Mabouia ransomware | Mac OS X | malware

MORE S



vBulleti

day exp

Rumors

hackers

website e
company

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
vBulletin security patches and zero-day exploit available online

YOU MIGHT ALSO LIKE

vBulletin security patches and zero-day exploit available online

November 5, 2015 By Pierluigi Paganini

Offline Ransomware is spreading among Russian users

November 5, 2015 By Pierluigi Paganini

Promote your solution on Security Affairs