



🏠 [Home \(/connect/\)](/connect/)

💬 [Forums \(/connect/forums/community-forums\)](/connect/forums/community-forums)

📄 [Blogs \(/connect/blogs/discover\)](/connect/blogs/discover)

🔍 [Search \(/connect/search\)](/connect/search)

🏠 [Connect Community \(/connect/\)](/connect/) > [Blogs \(/connect/blogs\)](/connect/blogs)

> [Security Response \(/connect/symantec-blogs/symantec-security-response\)](/connect/symantec-blogs/symantec-security-response)

📄 Security Response



<https://twitter.com/threatintel>



<http://www.symantec.com/connect/item-feeds/blog/2261/feed/all/en/all>

+3

3 Votes



Symantec Official Blog

Proof-of-concept threat is reminder OS X is not immune to crypto ransomware

Symantec analysis confirms that in the wrong hands, Mabouia ransomware could be used to attack Macs.

By: [Symantec Security Response \(/connect/user/symantec-security-response\)](/connect/user/symantec-security-response)

SYMANTEC EMPLOYEE

Created 09 Nov 2015



0

🌐 Translations: [日本語 \(/connect/ja/blogs/os-x\)](/connect/ja/blogs/os-x)

🔗 [Share](#)



Analysis by Symantec has confirmed that the proof-of-concept (PoC) threat known as Mabouia works as described and could be used to create functional OS X crypto ransomware if it fell into the wrong hands.

Mabouia (detected by Symantec as OSX.Ransomcrypt (https://www.symantec.com/security_response/writeup.jsp?docid=2015-110912-2037-99)) was developed by Brazilian cybersecurity researcher Rafael Salema Marques (<https://www.linkedin.com/pulse/mabouia-born-first-mac-osx-ransomware-poc-rafael-salema-marques>), who wrote the PoC malware to highlight the fact that Macs may not be immune to the threat of ransomware.

Marques shared a sample of the ransomware with Symantec and Apple. Symantec's analysis has confirmed that the PoC is functional. Marques said he has no intention of publicly releasing the malware.

Mabouia follows the tried-and-tested model used by many ransomware variants of encrypting files on the infected computer and sending the encryption key to a command-and-control (C&C) server. The malware displays payment instructions on the infected computer, including a unique ID the victim would need to use to retrieve a decryption key. This key can potentially be sent to the victim upon payment of a ransom.

In the case of Mabouia, because it's a proof of concept, it only encrypts files saved in a directory called "ransom". Most Mac users will not have a directory with this name on their computer.


Mabouia is the first case of file-based crypto ransomware for OS X, albeit a proof-of-concept. Macs have nevertheless already been targeted by ransomware in the form of browser-based

threats. For example, in 2013, [researchers at Malwarebytes discovered](https://blog.malwarebytes.org/fraud-scam/2013/07/fbi-ransomware-now-targeting-apples-mac-os-x-users/) (<https://blog.malwarebytes.org/fraud-scam/2013/07/fbi-ransomware-now-targeting-apples-mac-os-x-users/>) browser-based ransomware that targeted Safari for Mac users through a malicious website. The website directed Windows users to a drive-by download, while Mac users were served JavaScript that caused Safari to display persistent pop-ups informing the user their browser had been “locked” by the FBI for viewing illegal content.

Protection

[Norton Security](https://us.norton.com/) (<https://us.norton.com/>), [Symantec Endpoint Protection](https://www.symantec.com/endpoint-protection/) (<https://www.symantec.com/endpoint-protection/>), and other [Symantec security products](http://www.symantec.com/products-solutions/) (<http://www.symantec.com/products-solutions/>) detect this threat as [OSX.Ransomcrypt](https://www.symantec.com/security_response/writeup.jsp?docid=2015-110912-2037-99) (https://www.symantec.com/security_response/writeup.jsp?docid=2015-110912-2037-99).


Tags: [Security](/connect/communities/security/) (</connect/communities/security/>), [Security Response](/connect/named-blogs/symantec-security-response/) (</connect/named-blogs/symantec-security-response/>), [Endpoint Protection \(AntiVirus\)](/connect/products/endpoint-protection-antivirus/) (</connect/products/endpoint-protection-antivirus/>), [Apple](/connect/blog-tags/apple/) (</connect/blog-tags/apple/>), [Mabouia](/connect/blog-tags/mabouia/) (</connect/blog-tags/mabouia/>), [mac](/connect/blog-tags/mac/) (</connect/blog-tags/mac/>), [os x](/connect/blog-tags/os-x/) (</connect/blog-tags/os-x/>), [OSX.Ransomcrypt](/connect/blog-tags/osxransomcrypt/) (</connect/blog-tags/osxransomcrypt/>), [proof of concept](/connect/blog-tags/proof-concept/) (</connect/blog-tags/proof-concept/>), [Ransomcrypt](/connect/blog-tags/ransomcrypt/) (</connect/blog-tags/ransomcrypt/>), [Ransomware](/connect/blog-tags/ransomware/) (</connect/blog-tags/ransomware/>)

 [Subscriptions \(0\)](#)



[\(/connect/user/symantec-security-response/\)](/connect/user/symantec-security-response/)

[Symantec Security Response](/connect/user/symantec-security-response/) (</connect/user/symantec-security-response/>)

 [View Profile](/connect/user/symantec-security-response/) (</connect/user/symantec-security-response/>)

[Login](https://www-secure.symantec.com/connect/user/login?destination=node%2F3537401) (<https://www-secure.symantec.com/connect/user/login?destination=node%2F3537401>) or **[Register](https://www-secure.symantec.com/connect/user/register?destination=node%2F3537401)** (<https://www-secure.symantec.com/connect/user/register?destination=node%2F3537401>) to post comments.



Please take a
minute to complete
our Security
Response survey.
Click here.

<https://www.surveymonkey.com/r/G7KVZWQ>

Community Stats

Total Posts

1 , 4 1 4 , 7 0 9

Members

4 3 2 , 0 6 7

[Contact Us \(/connect/contact\)](/connect/contact) [Privacy Policy \(http://www.symantec.com/about/profile/policies/privacy.jsp\)](http://www.symantec.com/about/profile/policies/privacy.jsp) [Terms and Conditions \(/connect/legal\)](/connect/legal) [Earn Rewards \(/connect/points\)](/connect/points) [Rewards Terms and Conditions \(/connect/blogs/symantec-connect-rewards-program-terms-and-conditions\)](/connect/blogs/symantec-connect-rewards-program-terms-and-conditions)

© 2015 Symantec Corporation



[_ \(https://twitter.com/symantec\)](https://twitter.com/symantec)



[_ \(https://www.facebook.com/Symantec\)](https://www.facebook.com/Symantec)



[_ \(https://www.linkedin.com/company/symantec\)](https://www.linkedin.com/company/symantec)