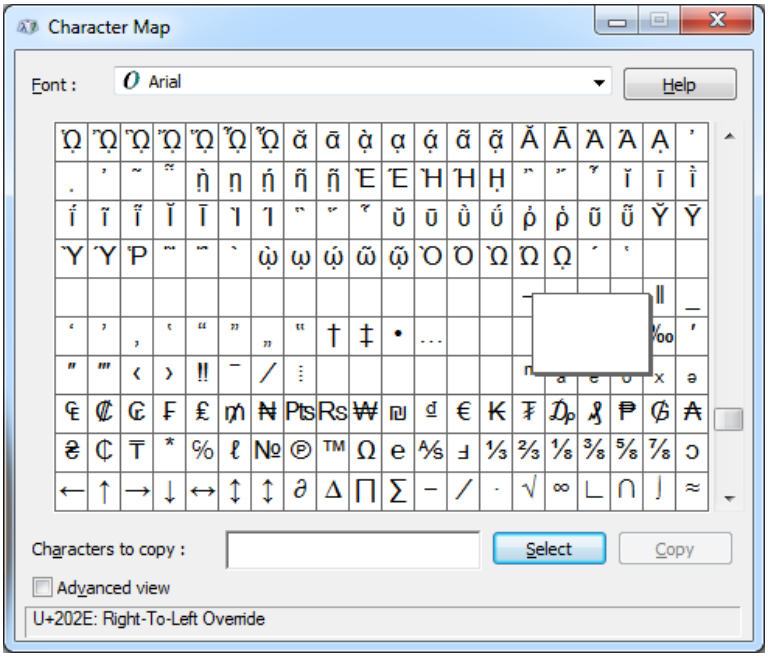
Sophos Discovers ZeroAccess Using RLO

blog.malwarebytes.com/threat-analysis/2013/08/sophos-discovers-zeroaccess-using-rlo/

Joshua Cannell August 1, 2013



Yesterday, analysts at SophosLabs looked at a new ZeroAccess variant using some new tricks to hide itself.

Or should I say old ones, which are seemingly rediscovered.

In his article, Sophos researcher James Wyke describes how ZeroAccess typically stores it's local data, but in this variant explains that "the malware authors are also using the right-to-left override and several other non-printable Unicode characters in both file paths and registry entries to further hinder identification and removal of the ZeroAccess components."

If you recall, ZeroAccess is a notorious rootkit that made it's first debut in 2011 and has since produced many versions. I recently wrote about a self-debugging technique I found when unpacking a ZeroAccess sample.

On the other hand, RLO is a simple trick used by malware to obfuscate text strings, usually for the purpose of masking file extensions. Fellow Unpacked author Jean-Taggart wrote a blog about this here.

We've been seeing a resurgence of the RLO trick as of late in malware samples, namely a signed piece of Mac malware named 'Janicab' which was documented by F-secure. While this technique is far from new, it might be just enough to fool the average user or junior malware analyst.

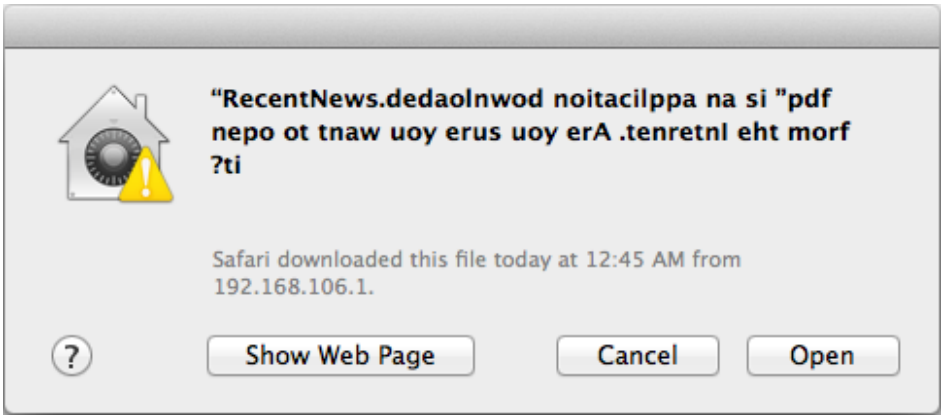


Image: F-Secure

In the ZeroAccess sample discovered by Sophos, the malware obfuscated the registry key value for the malware's service, called 'gupdate'. Implementation of RLO does not make the service binary 'GoogleUpdate.exe' initially appear to be an EXE.

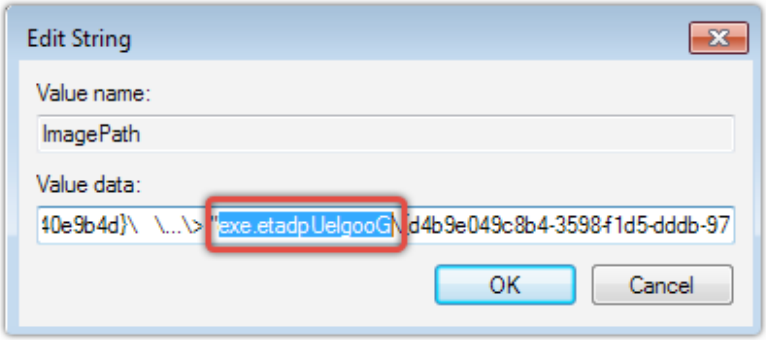


Image: NakedSecurity

Is RLO making a comeback? It certainly seems like it.

Malware authors sometimes get lazy and recycle the same old tricks to hide their dirty deeds. Nevertheless, the method used doesn't always need to be complex if it gets the job done.

Other simple forms of rudimentary obfuscation that's used a lot in malware is ROT13 and base64 encoding, both of which I talked about here.

For the full article from Sophos, click here.

Joshua Cannell is a Malware Intelligence Analyst at Malwarebytes where he performs research and in-depth analysis on current malware threats. He has over 5 years of experience working with US defense intelligence agencies where he analyzed malware and developed defense strategies through reverse engineering techniques. His articles on the *Unpacked* blog feature the latest news in malware as well as full-length technical analysis. Follow him on Twitter @joshcannell