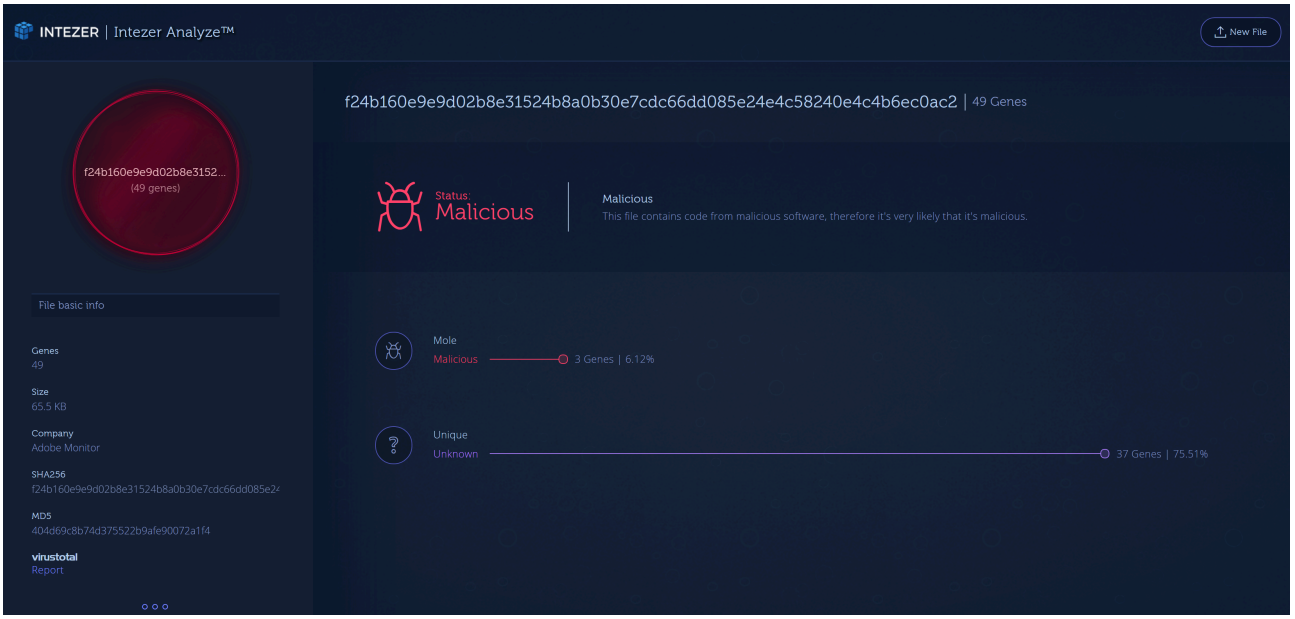
Silence of the Moles

By Jay Rosenberg

Published: 2017-11-01 · Archived: 2026-04-05 14:41:17 UTC

Kaspersky Labs published a technical analysis of a new malware, Silence that is aimed at attacking financial institutions. After uploading the loader of this malware to Intezer Analyze™, we have found a possible connection through code reuse to the loader of another campaign of malware, Mole previously discovered by Unit 42 of Palo Alto Networks.

This connection might be an indicator that these two attacks are originated from the same threat actor, but currently it is too early to tell.

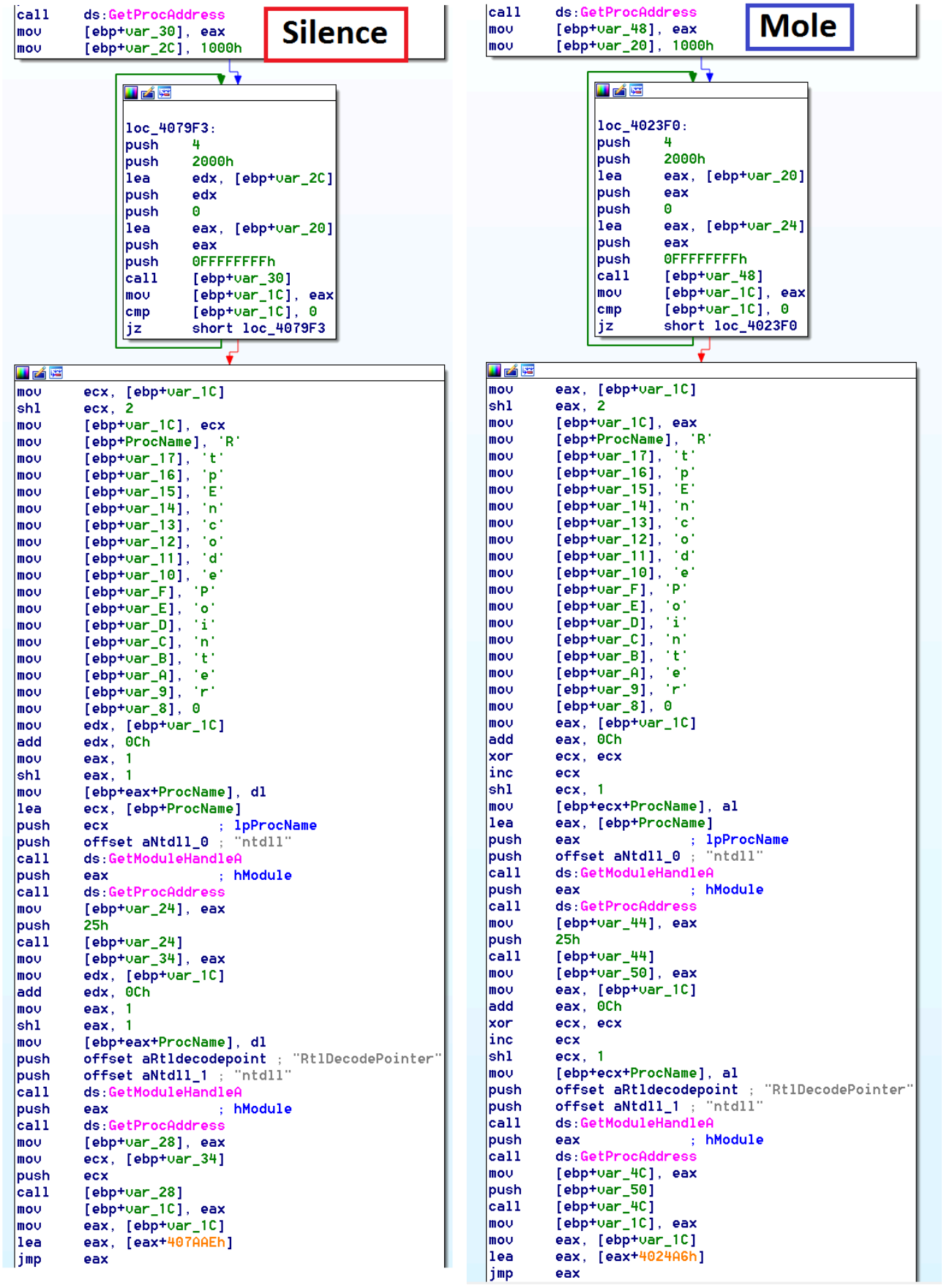


(Intezer Analyze™ public report available here.)

Silence Loader: f24b160e9e9d02b8e31524b8a0b30e7cdc66dd085e24e4c58240e4c4b6ec0ac2

Mole Loader: 50117ce3fe5dba572cf23584dc7541a7cfd4026d4316e69d29cdf536873fdf20

If we look at the code of the two loaders used by both campaigns side by side, we can see that the code is very similar and according to our system is unique to these families of malware.



(sub_4079A0 vs sub_4023A0)

Through the disassembly in the photo above, we can also see there is a string initialized through an array, “RtpEncodePointer,” that is later used for a call to GetProcAddress. This looks like a typo and the author of the code meant to write “RtlEncodePointer” because “RtpEncodePointer” does not exist in ntdll.dll. The evidence suggests that this code was being reused. There are no references to “RtpEncodePointer” available publicly online besides automated reports of a couple unclassified malware from Hybrid Analysis

In addition to the links within the code, there are several other similarities we have witnessed between the Mole and Silence malware, such as the attack vectors (spear phishing, packaging of the malware) and motives — which can be extra evidence for this connection.

Yet again, we see that identifying code reuse can be very valuable in detecting new malware, and in some cases for attribution purposes. We invite you to read more of the posts in our blog and to request an invite to the community edition of our product.

Follow @jaytezer for more updates.

Source: http://www.intezer.com/silenceofthemoles/