APT37: Final1stspy Reaping the FreeMilk

intezer.com/apt37-final1stspy-reaping-the-freemilk/

October 3, 2018

Written by Jay Rosenberg - 3 October 2018

Get Free Account

Join Now

Researchers at Palo Alto Networks recently published a report regarding the NOKKI malware, which has shared code with KONNI and, although not in the report by Palo Alto, KimJongRAT (discovered by Paul Rascagnères of Cisco Talos in 2013), and another report on how there is evidence of the NOKKI malware connecting to the North Korean threat actor known as APT37, Reaper, or Group123.

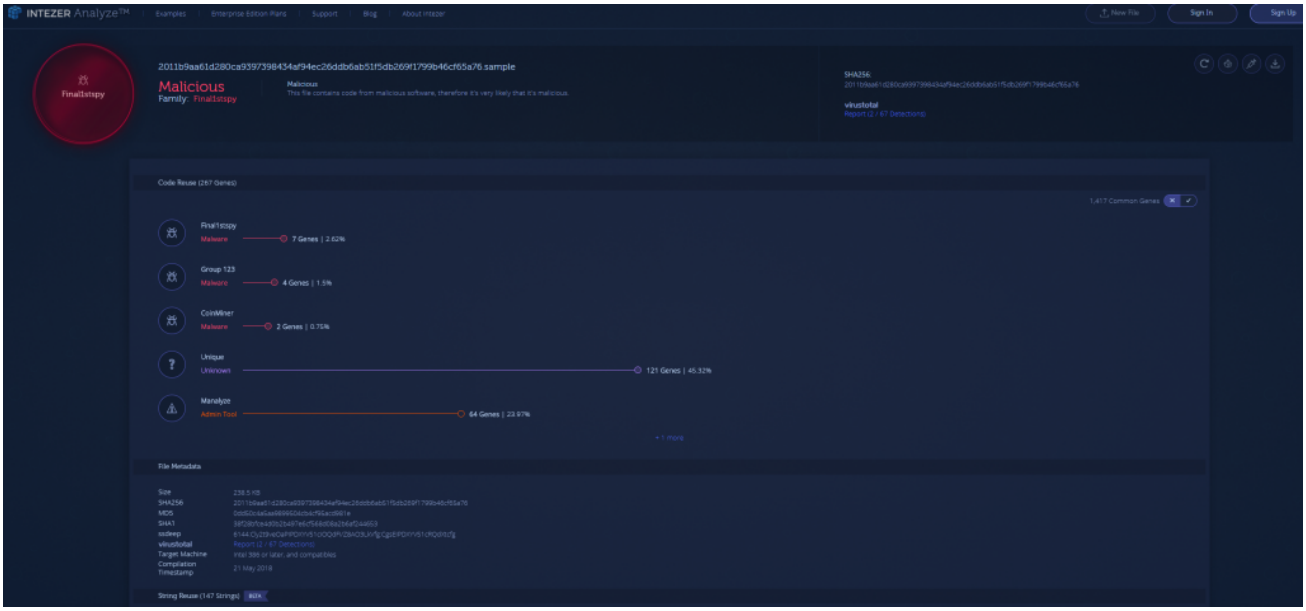
> New report by @PaloAltoNtwks on #NOKKI malware with similarities to #KONNI also has code relations to #KimJongRAT in a report from 2013 by @r00tbsd https://t.co/Rc0T8a4o6h pic.twitter.com/QkjiaQJ2wF
>
> — Jay Rosenberg (@jaytezer) September 28, 2018

The malicious document related to NOKKI, using VBScript, downloads a newly discovered malware named Final1stspy, due to the PDB string inside. As noted by Palo Alto Networks, Final1stspy comes in 2 components, the EXE named “LoadDll” with the sole purpose of loading up a DLL payload, internally named “hadowexecute.” After collecting information

about the infected computer, the end result is that the DOGCALL malware, also known as ROKRAT, is downloaded as the final payload, thus being **one of the links between NOKKI and APT37**.

LINKS THROUGH CODE REUSE

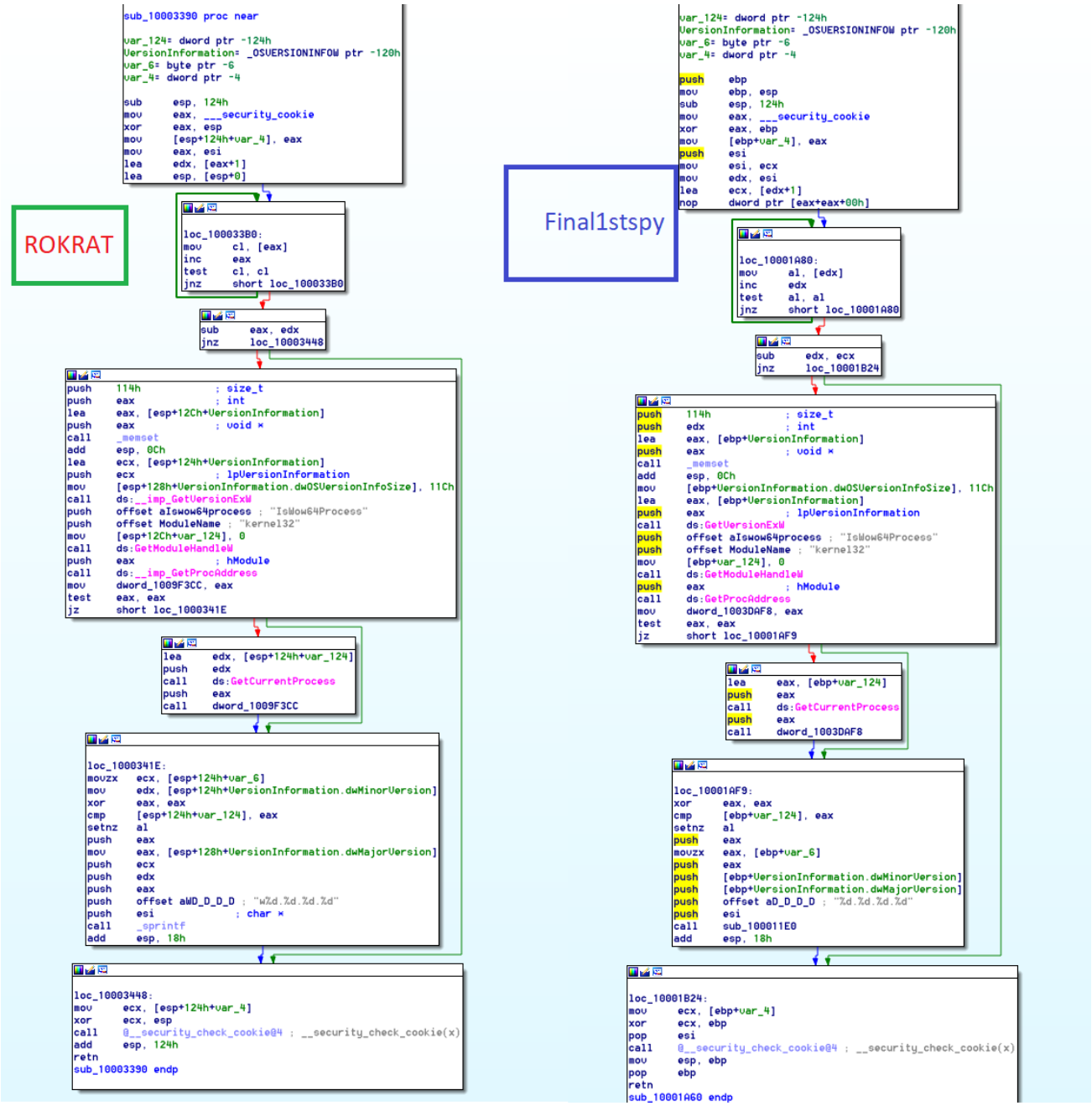
The DLL payload component under the hash that was listed in the report was not available on VirusTotal. We created some YARA signatures from the code of “LoadDll” and did a hunt via VirusTotal. Since the EXE component shares code with the DLL, the YARA hunt led us to find an earlier version of the DLL component of Final1stspy with 2/67 detections, compilation timestamp of May 21, 2018, and first upload to VirusTotal date of July 11, 2018. This is an earlier version than described in the Palo Alto report. After obtaining the hadowexecute DLL component, we checked to see if there was any code reuse in the Intezer Analyze™ system.



Intezer Analyze™

We see that there is some code shared between the EXE component of Final1stspy and other code that has been seen before in the FreeMilk campaign which utilized ROKRAT.

Let’s see the shared code between ROKRAT and Final1stspy by doing comparison of these functions in IDA. If you take a look, there is an identical match between them.



(ROKRAT & Final1stspy hadowexecute function comparison)

This function is unique code that has only been seen before in Group123's ROKRAT and the DLL component of Final1stspy. The identical function gathers information about the operating system and stores it in the same format.

CONCLUSION

The evidence in Group123 being the threat actor involved here does not only lie in the final delivered payload, but in the code itself. This code reuse provides more evidence towards the relationship of KimJongRAT, KONNI, NOKKI, Final1stspy, ROKRAT, and APT37.

IoCs

Final1stspy

2011b9aa61d280ca9397398434af94ec26ddb6ab51f5db269f1799b46cf65a76 (DLL)

0669c71740134323793429d10518576b42941f9eee0def6057ed9a4ba87a3a9a (DLL)

fb94a5e30de7afd1d9072ccedd90a249374f687f16170e1986d6fd43c143fb3a (EXE)

Group 123 (FreeMilk / ROKRAT Samples)

99c1b4887d96cb94f32b280c1039b3a7e39ad996859ffa6dd011cf3cca4f1ba5

01045aeea5198cbc893066d7e496f1362c56a154f093d1a8107cecad8d4e4df2

26ad5f8889d10dc45dcf1d3c626416eb604f5fe4a7268e044f17a3ab6ff14e53

65ec544841dbe666d20de086495158128ddffb8b076ddb801a3f2dc250481135

7f35521cdbaa4e86143656ff9c52cef8d1e5e5f8245860c205364138f82c54df

ef40f7ddff404d1193e025081780e32f88883fa4dd496f4189084d772a435cb2

Jay Rosenberg