JSSLoader: the shellcode edition

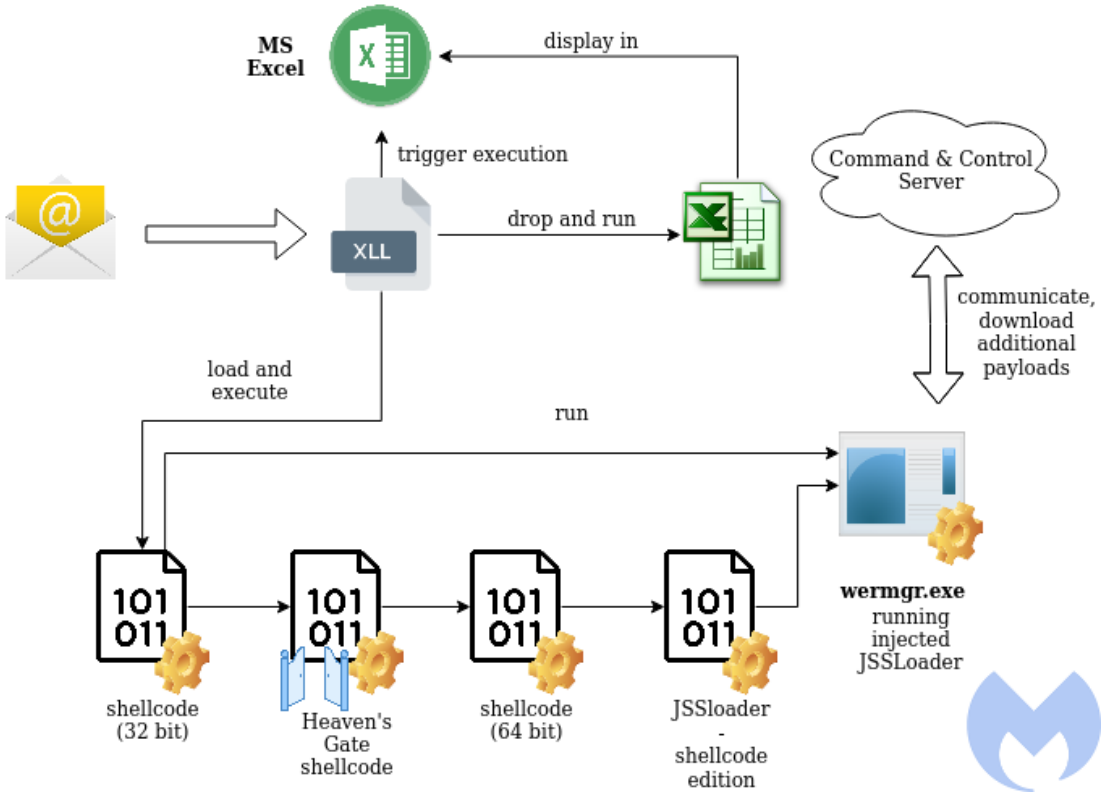
malwarebytes.com/blog/threat-intelligence/2022/08/jssloader-the-shellcode-edition

Posted: August 15, 2022 by Threat Intelligence Team

The Malwarebytes Threat Intelligence team observed a malspam campaign in late June that we attribute to the FIN7 APT group. One of the samples was also reported on Twitter by Josh Trombley; during execution, it was observed to drop a secondary payload, written in .NET.

Details about FIN7 campaigns were described by Mandiant in the article "FIN7 Power Hour: Adversary Archeology and the Evolution of FIN7". Earlier this year Morphisec and Secureworks described a new component used by this group, delivered

in XLL format. That element was the first step in the attack chain leading to another malware, dubbed JSSLoader.



During our analysis, we found out that the current malware used by FIN7 is yet another rewrite of JSSLoader with expanded capabilities as well as new functions that include data exfiltration.

In this white paper, we will focus on the implementation details of the new observed sample, and provide a deep dive in the code, as well as compare it with earlier samples analyzed by other vendors.

Download the white paper.

COMMENTS

RELATED ARTICLES

ABOUT THE AUTHOR

Threat Intelligence Team