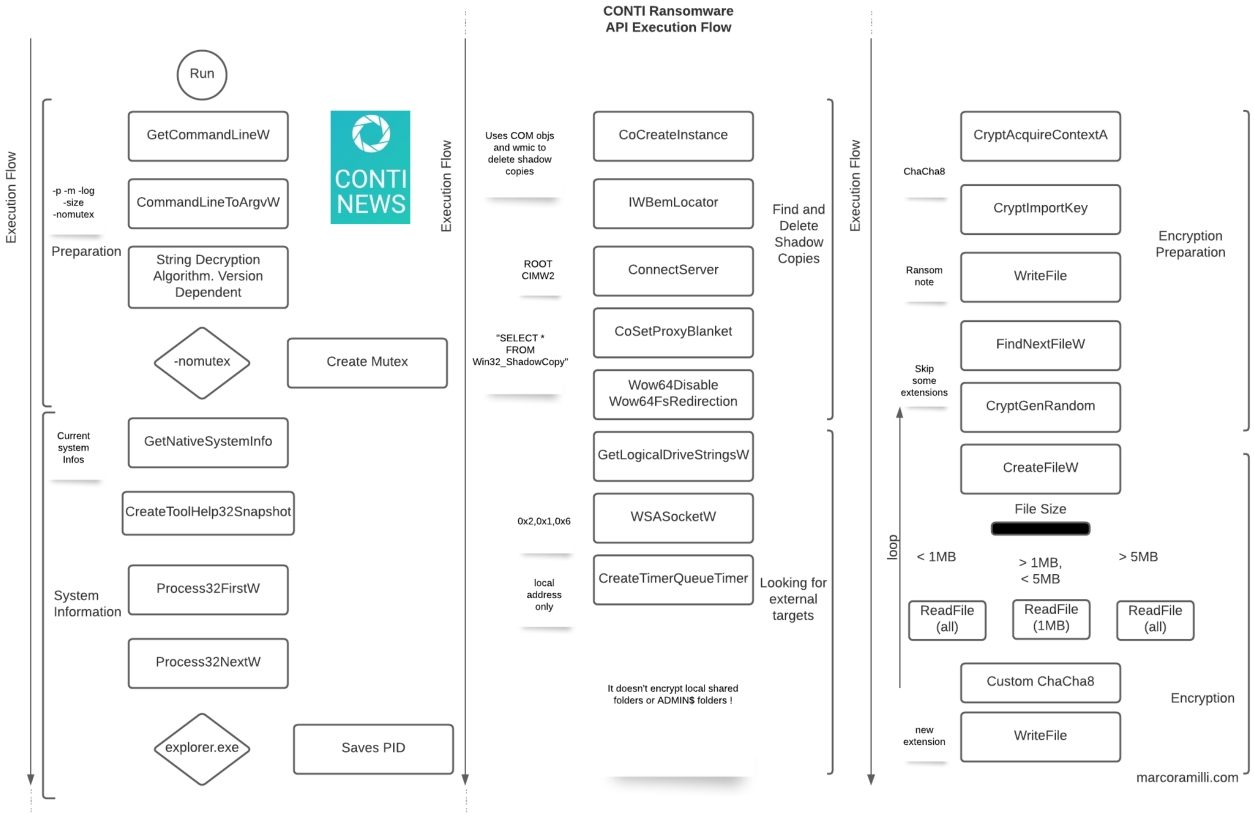
CONTI Ransomware: Cheat Sheet

marcoramilli.com/2021/11/07/conti-ransomware-cheat-sheet/

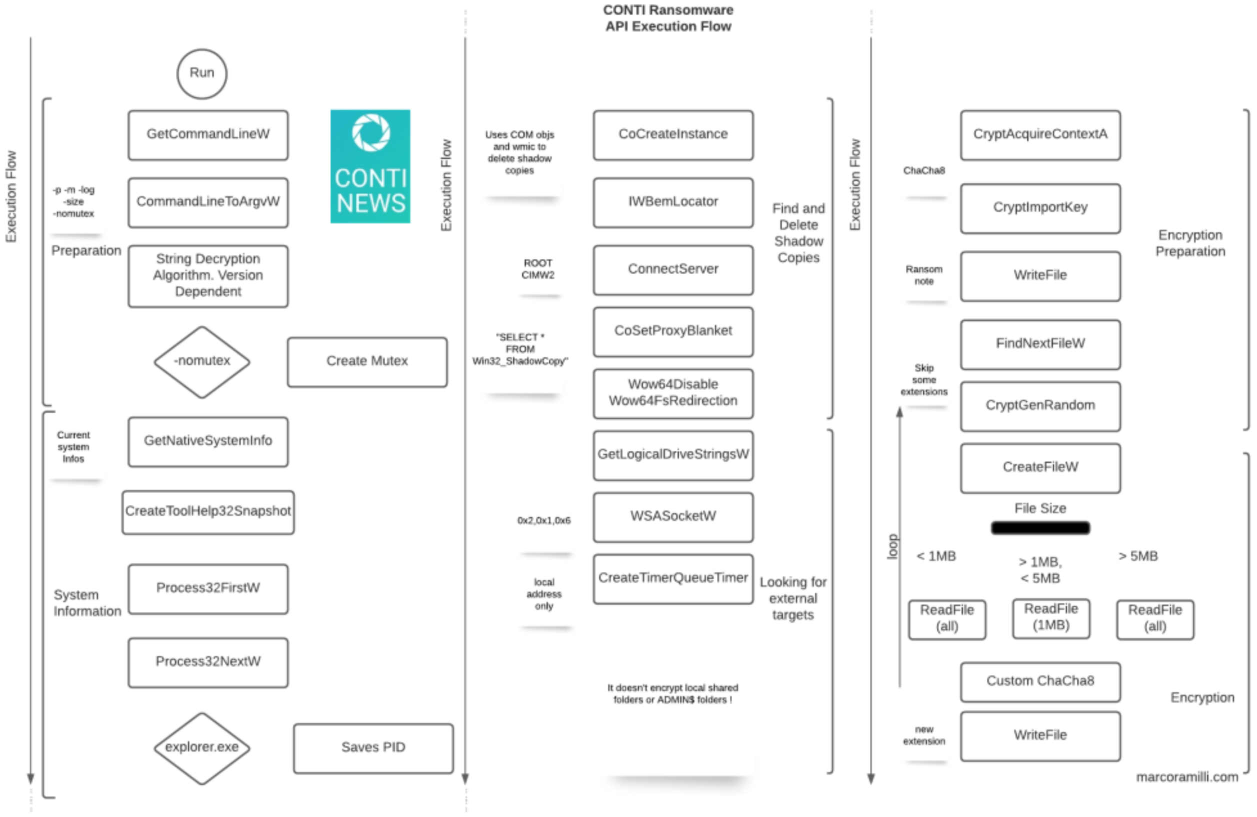
View all posts by marcoramilli

November 7, 2021



Ransomware are today very effective and they cause serious problems in many companies, we hear almost everyday entire businesses under ransom and companies who loose turnover and opportunities since have no available data to deal with. For such a reson I feel like I have to contribute in somehow to the community by giving what I can on this topic. So, this is my little contribution to fight CONTI ransomware: an **API block cheat sheet**. In other words by reading such a flow you should have the main CONTI functionalities mapped by API call blocks. It might help you in the following ways:

- To learn how the current CONTI ransomware works (if you had no chance to reverse it)
- To extract behavioural models for your Manchine Learning engine
- To synthetize API call signatures for your dynamic detection engine
- Extract behavioural patterns for your SIEM



CONTI Ransomware Cheat Sheet

The Execution flow is represented by the long up-to-down raws and it runs from left to right. The main API calls are included into rectangles while the conditional jumps are mapped into diamonds. Next to specific rectangles (API Calls) a little note is giving further details on the analyzed step. Square brackets wraps API calls into blocks so that you might easily read the six logic CONTI steps, that are: Preparation, System Information, Find and Delete Shadow Copies, Looking for External Targets (shared folders), Encryption Preparation (ransom note included) and Encryption Execution.

If you think this content is helpful, please consider to make a little donation. It would help me in building and writing additional contributions to community. By donation you will contribute to community as well. Thank you !

If you think this content is helpful, please consider to make a little donation. It would help me in building and writing additional contributions to community. By donation you will contribute to community as well. Thank you !

DonateDonate monthly
I hope you might enjoy it !