APT Groups and Operations

	A	B
1	**General Information**	
2	Topic	Comment
3	Motive	Cyber security companies and Antivirus vendors use different names for the same threat actors and often refer to the reports and group names of each other. However, it is a difficult task to keep track of the different names and naming schemes. I wanted to create a reference that answers questions like "I read a report about the 'Tsar Team', is there another name for that group?" or "Attackers used 'China Chopper' webshell, which of the APT groups did use that shell too?" or "Did he just say 'NetTraveler'? So, does he talk about Chinese or Russian attackers?"
4	Hints	- Each active country / region has its own tab - The "Other" tab contains actors from certain regions not covered by the main tabs - The "Unknown" tab is used for groups and operations with no attribution - Cells with overlaps are highlighted in gray - overlaps are no error per se but necessary to visualize that groups tracked by one vendor are divided into two different groups by another vendor
5	Disclaimer	Attribution is a very complex issue. This list is an intent to map together the findings of different vendors and is not a reliable source. Most of the mappings rely on the findings in a single incident analysis. Groups often change their toolsets or exchange them with other groups. This makes attribution of certain operations extremely difficult. However, we decided that even an uncertain mapping is better than no mapping at all. Be aware that information published here may be wrong, quickly outdated, or may change based on evolving information. People tend to comment on the sheet. Sometimes they add threat intel that isn't TLP:WHITE but taken from some fee-based platform. Please let me know if confidential information has been disclosed.
6	Known Issues	- Groups named after the malware (families) they've used - Groups named after a certain operation - Lists / tables are not normalized to allow a better overview by avoiding too many spreadsheets - Some groups have now been discovered to be "umbrella" terms for sub-groups. (e.g. Lazarus has subgroups; Winnti's "Burning Umbrella" report)
7	Search	Press CTRL+F or Command+F and then use the Symbol with the three dots to bring up the search dialogue that looks in the full workbook for your keywords
8	Overlaps	Names that appear multiple times are shaded in a light grey
9	First Release	12/26/2015
10	License	CC Creative Commons - Attribution 4.0 International (CC BY 4.0) https://creativecommons.org/licenses/by/4.0/
11	Access Rights	Everyone: READ / COMMENT Invited Editors: READ / COMMENT / WRITE
12	Support	Please contact me (@cyb3rops) if you would like to modify or add content to these lists. I will gladly give you write access to this list if: - I know you personally or from my Twitter stream - you are a threat intel researcher / malware analyst with some reference - you are a vendor representative - you are an author of the listed sources (see '_Sources' work sheet) Please provide you email address if you are interested in helping me (preferably Gmail - this allows native access via the connected Google account)
13	Search Engine	https://cse.google.com/cse/publicurl?cx=003248445720253387346:turlh5vi4xc
14	Short URL	https://apt.threattracking.com
15		

README | China | Russia | North Korea | Iran | Israel | NATO | Middle East | Others | Unknown | _Download | _Taxonomies | _Mal