APT Dataset Unattributed Sample Information

Hash	Current Knowledge	ADAPT cluster-info	Feature	VT Community
71b201a5a7dfdbe91c0a7783f845b71d066c62014b944f488de5aec6272f907c	Nan	Cluster 1: Grouped with one other sample from APT 3	Bitcoin pattern, embedded	No additional information
bff6270b7c6240c394515dc2505bb9f55d7b9df700be1777a8469143f78d0eb6	Nan (Has been called Crimson RAT) but no reliable source	Cluster 2: Grouped with 2 other samples from Transparent Tribe	Exactly the same ASNs, country codes, and BGP prefixes	Crimson RAT and transparent tribe
f659b269fbe4128588f7a2fa4d6022cc74e508d28eee05c5aff26cc23b7bd1a5	Nan (Call china based APT no reliable threat report)	Cluster 3: grouped with three other samples from APT 40 → This one has a document sample	Similar BGP prefixes and ASNs	Chinese basted apt
4a9efdfa479c8092fefee182eb7d285de23340e29e6966f1a7302a76503799a2	Nan (Says russian based APT but not the exact name)	Cluster 4: Grouped with 6 other samples from APT28	Embedded string patterns are similar but nothing comes too conspicuous	No info
12e1b00af73101cb297387b6ee5035c4cae04211d995ddd233fb375deb492b0a	Nan (only one report saying The Oceansalt APT Group seems to	Cluster 5: We grouped it with other 6 samples from APT 15 another chinese group actor	IP address	OceanSalt

	have links with the Chinese hacking group Comment Crew (aka APT1).)			
fa71eee906a7849ba3f4bab74edb577bd1f1f8397ca428591b4a9872ce1f1e9b	NCSC-MAR-Devil-Bait.pdf This report names it as Devil Bait but doesn't the attribute it to Kimsuky although says something like this: "Masquerading as AhnLab, a popular endpoint security product in South Korea, for persistence is a technique previously used by Kimsuky actors. The use of the string 'Update' in autorun names (e.g. AhnlabUpdate) is also associated with this group."	Cluster 6: Grouped in a cluster with two other document files from Kimsuky	Macro enabled documents Similar file paths accessed and URL: [http://xeoskin.co.kr, http://schemas.openxmlformats.org]	No info
Eae62bb4110bcd00e9d1bcaba9000defcda3d1ab832fa2634d928559d066cb15 b3cee881b2f9d115c98d431b70a75709aade2	2 Nan samples no reliable source but for sample there is threat report saying APT 28 : Rewterz Threat Alert - APT -	Cluster 7: Grouped with 4 other samples from APT 28	Shares a similar BGP prefix and ASN with one of the samples in APT28	APT28

317a82a0792c15dce2ffa892679	28 Fancy Bear - Active IOCs - Rewterz but nothing else			
df5f1b802d553cddd3b99d1901a87d0d1f42431b366cfb0ed25f465285e38d27	Nan (Just says some hacking tool) no attribution	Cluster 8: Grouped with 4 other samples from APT 10	Looks like it grouped based on some distinct file copyright information in metadata	APT3