APT Dataset Unattributed Sample Information

Hash	Current OSINT Knowledge	ADAPT clustering	Features	VT Community
71b201a5a7dfdbe91c0a7783f845b71d066c62014b944f488de5aec6272f907c	Nan	Cluster 1: Grouped with one other sample from APT3	Embedded Bitcoin pattern	No additional information
bff6270b7c6240c394515dc2505bb9f55d7b9df700be1777a8469143f78d0eb6	Nan (Has been called Crimson RAT but no reliable source)	Cluster 2: Grouped with 2 other samples from Transparent Tribe	The same ASNs, country codes, and BGP prefixes	Crimson RAT and Transparent tribe
f659b269fbe4128588f7a2fa4d6022cc74e508d28eee05c5aff26cc23b7bd1a5	Nan (China-based APT but no reliable source)	Cluster 3: Grouped with three other samples from APT40 → including a document sample	Similar BGP prefixes and ASNs	China-based APT
4a9efdfa479c8092fefee182eb7d285de23340e29e6966f1a7302a76503799a2	Nan (Russian-based APT but no definite attribution)	Cluster 4: Grouped with 6 other samples from APT28	Embedded string patterns are similar but nothing too conspicuous	No additional information
12e1b00af73101cb297387b6ee5035c4cae04211d995ddd233fb375deb492b0a	Nan (One source mentioning OceanSalt. OceanSalt APT seems to have links with the Chinese hacking group Comment Crew)	Cluster 5: Grouped with 6 samples from APT15; a Chinese threat group	IP address	OceanSalt

fa71eee906a7849ba3f4bab74edb577bd1f1f8397ca428591b4a9872ce1f1e9b	NCSC-MAR-Devil-Bait.pdf The report calls the malware 'Devil Bait' but doesn't say it's linked to Kimsuky. However, the techniques used, like persistence and using 'Update' in file names, are similar to those used by Kimsuky.	Cluster 6: Grouped with two other document files from Kimsuky	Macro-enabled documents Similar URLs accessed: [http://xeoskin.co.kr, http://schemas.openxmlformats.org]	No additional information
Eae62bb4110bcd00e9d1bcaba9000defcda3d1ab832fa2634d928559d066cb15 b3cee881b2f9d115c98d431b70a75709aade2317a82a0792c15dce2ffa892679	Nan (no concrete source information. However, one sample is linked to a Reuter's threat report identifying APT 28 (Fancy Bear) as the potential actor: Rewterz Threat Alert - APT -28 Fancy Bear - Active IOCs - Rewterz)	Cluster 7: Grouped with 4 other samples from APT28	Shares a similar BGP prefix and ASN with one of the samples in APT28	APT28
df5f1b802d553cddd3b99d1901a87d0d1f42431b366cfb0ed25f465285e38d27	Nan	Cluster 8: Grouped with 4 other samples from APT10	Distinct file copyright information in metadata	APT3