APT Dataset Unattributed Sample Information

APT Hash	Current OSINT Knowledge	Potential Group label	Features	VT Community
71b201a5a7dfdbe91c0a7783f845b71d066c62014b944f488de5aec6272f907c	None	APT3	Bitcoin-related data in the string pattern	No additional information
bff6270b7c6240c394515dc2505bb9f55d7b9df700be1777a8469143f78d0eb6	Has been called Crimson RAT but has no reliable source	Transparent Tribe	Similar IP data such as ASNs, country codes, and BGP prefixes	Crimson RAT and Transparent Tribe
f659b269fbe4128588f7a2fa4d6022cc74e508d28eee05c5aff26cc23b7bd1a5	Identified as China-based APT but has no reliable source	APT40	Similar IP data, ASNs, country codes, and BGP prefixes	China-based APT
4a9efdfa479c8092fefee182eb7d285de23340e29e6966f1a7302a76503799a2	Identified as Russian-based APT	APT28	Similar embedded string patterns	No additional information
12e1b00af73101cb297387b6ee5035c4cae04211d995ddd233fb375deb492b0a	Associated with OceanSalt which is known to have links with the Chinese hacking group, comment crew.	APT15	A similar IP address	OceanSalt
fa71eee906a7849ba3f4bab74edb577bd1f1f8397ca428591b4a9872ce1f1e9b	NCSC-MAR-Devil-Bait.pdf	Kimsuky	Macro-enabled document with specific URL accessed: [http://xeoskin.co.kr, http://schemas.openxmlformats.org]	No additional information
eae62bb4110bcd00e9d1bcaba9000defcda3d1ab832fa2634d928559d066cb15 b3cee881b2f9d115c98d431b70a75709aade2317a82a0792c15dce2ffa892679	One sample associated with APT28 in Reuter's threat report: Rewterz Threat Alert - APT -28 Fancy Bear - Active IOCs - Rewterz)	APT28	Similar IP data	APT28
df5f1b802d553cddd3b99d1901a87d0d1f42431b366cfb0ed25f465285e38d27	None	APT10	Similar IP data and distinct file copyright information	APT3