cybereason

FakeSpy: Indicators of Compromise

June 29th, 2020

IOC	Type	Description
ad1ad43fdb2f6759b1a32b47dea41cd98afd74f6 00e26db52f692c5bea849f92a137991da484f907 7456e4ae32d574273656ce2350b28a745a33f806	SHA1	FakeSpy Japan Post samples
6165039d703b74a99c0640950305e62cc88412d8		FakeSpy Japan Post unpacked JAR
f4524e97b979a59a56c4414f1835e236ce460a93 558575c4357295acf08d49df3fb85da42829e2ed		FakeSpy Yamato Post samples
81ffd6e272d9b141530f8d3a52bbd2942c77fc0d		FakeSpy Yamato Post unpacked JAR
47e8d207966478f0bac718a117bc51b96632a5d1 0cfb6920c952a6f072021de0cc7c832208940b73		FakeSpy Chunghwa Post samples
a1cecf4f3f3a54dd78fb836738a9806fa720a89b		FakeSpy Chunghwa Post unpacked JAR
d818e3525cc8d74f391b93ec23f8dc235d156834 b7c4e93aaa09954c9f39e3128faed67155bac6f4 50cf9b9eddd095e81f6f08c2866fdc392551936d		FakeSpy Royal Mail samples
fe4942f434fff8650fff6fb7c766f96d4c50f362		FakeSpy Royal Mail unpacked JAR
4a17b45712f9701e00bc67382c022bc395cb391c e6ff0d3f5a745e5feda39ff22f66c0692cf6e714 4b1af28747217dbe888edba998d7dbb171c99278		FakeSpy LaPoste samples
983e8af3a6a83413085915f40c4a28df285768f8		FakeSpy LaPoste unpacked JAR
dd0f6b6d7ad521cd4496abf09985d0564bf97576		FakeSpy Swiss Post samples

81ffd6e272d9b141530f8d3a52bbd2942c77fc0d		FakeSpy Swiss Post unpacked JAR
4f8abb95a5836f73e2feab23e01bd3d5b4476d00 73d4c01ca239b339fcf64d498b14df0598e5c212		FakeSpy Deutsche Post samples
1f040347318736b3c34cb94089c042287119374c		FakeSpy Deutsche Post unpacked JAR
54910d4015660e13ef11fed78083ca5c210b3ba0 3844d06e5bef43b5fcaafb562551bdd942527b9f 4bbf3cce7d3a3a2844b9d6a34883e5a88d69a6a6		FakeSpy US Post samples
d9c5b3dddcbcf0322c3162aefcb58c47aca75b50		FakeSpy US Post unpacked JAR
doukt[.]club genmaa[.]club swizz[.]club frenchkt[.]club	Domains	C2 servers FakeSpy sent the data to