侵入の痕跡（Indicators of Compromise, IoCs）

Files

SHA-256	詳細	検出名
fd1aac87399ad22234c503d8adb2ae9f0d950b6edf4456b1515a30100b5656a7	The trojanized version of the Syria eGov Application	AndroidOS_StrongPity.HRX
374d92f553c28e9dad1aa7f5d334a07dede1e5ad19c3766efde74290d0c49afb	Sample repackaged from Kingoroot	AndroidOS_StrongPity.HRX
a9378a5469319faffc48f3aa70f5b352d5acb7d361c5177a9aac90d9c58bb628	Sample repackaged from net.cybertik.wifi	AndroidOS_StrongPity.HRX
be9214a5804632004f7fd5b90fbac3e23f44bb7f0a252b8277dd7e9d8b8a52f3	Repackaged from Snaptube	AndroidOS_StrongPity.HRX
596257ef017b02ba6961869d78a2317500a45f00c76682a22bbdbd3391857b5d	Repackaged from Snaptube	AndroidOS_StrongPity.HRX
75dc2829abb951ff970debfba9f66d4d7c6b7c48a823a911dd5874f74ac63d7b	Fake Samsung Security Service sample	AndroidOS_StrongPity.HRX

Network C&C Infrastructure

SHA-256	ドメイン名	検出名
fd1aac87399ad22234c503d8adb2ae9f0d950b6edf4456b1515a30100b5656a7	Internetwideband[.]com	AndroidOS_StrongPity.HRX
374d92f553c28e9dad1aa7f5d334a07dede1e5ad19c3766efde74290d0c49afb	upeg-system-app[.]com	AndroidOS_StrongPity.HRX
a9378a5469319faffc48f3aa70f5b352d5acb7d361c5177a9aac90d9c58bb628	networktopologymaps[.]com	AndroidOS_StrongPity.HRX
be9214a5804632004f7fd5b90fbac3e23f44bb7f0a252b8277dd7e9d8b8a52f3	networktopologymaps[.]com	AndroidOS_StrongPity.HRX
596257ef017b02ba6961869d78a2317500a45f00c76682a22bbdbd3391857b5d	upeg-system-app[.]com	AndroidOS_StrongPity.HRX
75dc2829abb951ff970debfba9f66d4d7c6b7c48a823a911dd5874f74ac63d7b	upn-sec3-msd[.]com	AndroidOS_StrongPity.HRX