侵入の痕跡（Indicators of Compromises、IoCs）

SHA256 値	パッケージ名	アプリのラベル名
332e68d865009d627343b89a5744843e3fde4ae870193f36b82980363439a425	ufD.wykyx.vlhvh	SEX kr porn
403401aa71df1830d294b78de0e5e867ee3738568369c48ffafe1b15f3145588	ufD.wyjyx.vahvh	佐川急便
466dafa82a4460dcad722d2ad9b8ca332e9a896fc59f06e16ebe981ad3838a6b	com.dhp.ozqh	Facebook
5022495104c280286e65184e3164f3f248356d065ad76acef48ee2ce244ffdc8	ufD.wyjyx.vahvh	Anshin Scan
a0f3df39d20c4eaa410a61a527507dbc6b17c7f974f76e13181e98225bda0511	com.aqyh.xolo	佐川急便
cb412b9a26c1e51ece7a0e6f98f085e1c27aa0251172bf0a361eb5d1165307f7	jp.co.sagawa.SagawaOfficialApp	佐川急便

不正な URL
hxxp://38[.]27[.]99[.]11/xvideo/
hxxp://apple-icloud[.]qwe-japan[.]com
hxxp://apple-icloud[.]qwq-japan[.]com/
hxxp://apple-icloud[.]zqo-japan[.]com/
hxxp://files.spamo[.]jp/佐川急便.apk
hxxp://mailsa-qae[.]com

hxxp://mailsa-qaf[.]com
hxxp://mailsa-qau[.]com
hxxp://mailsa-qaw[.]com
hxxp://mailsa-wqe[.]com
hxxp://mailsa-wqo[.]com
hxxp://mailsa-wqp[.]com
hxxp://mailsa-wqq[.]com
hxxp://mailsa-wqu[.]com
hxxp://mailsa-wqw[.]com
hxxp://nttdocomo-qae[.]com
hxxp://nttdocomo-qaq[.]com
hxxp://nttdocomo-qaq[.]com/aa
hxxp://nttdocomo-qar[.]com
hxxp://nttdocomo-qat[.]com
hxxp://nttdocomo-qaw[.]com
hxxp://sagawa-reg[.]com/
hxxp://www[.]711231[.]com
hxxp://www[.]759383[.]com
hxxp://www[.]923525[.]com
hxxp://www[.]923915[.]com
hxxp://www[.]975685[.]com

不正な Twitter アカウント
hxxs://twitter[.]com/lucky88755
hxxps://twitter[.]com/lucky98745
hxxps://twitter[.]com/lucky876543
hxxps://twitter[.]com/luckyone1232
hxxps://twitter[.]com/sadwqewqeqw
hxxps://twitter[.]com/gyugyu87418490
hxxps://twitter[.]com/fdgoer343
hxxps://twitter[.]com/sdfghuio342
hxxps://twitter[.]com/asdqweqweqeqw
hxxps://twitter[.]com/ukenivor3

不正な Instagram アカウント
hxxps://www[.]Instagram[.]com/freedomguidepeople1830/

不正な Tumblr アカウント
hxxps://mainsheetgyam[.]tumblr[.]com/
hxxps://hormonaljgrj[.]tumblr[.]com/
hxxps://globalanab[.]tumblr[.]com/

C&C サーバ
104[.]160[.]191[.]190:8822
61[.]230[.]204[.]87:28833
61[.]230[.]204[.]87:28844
61[.]230[.]204[.]87:28855
61[.]230[.]205[.]122:28833
61[.]230[.]205[.]122:28844
61[.]230[.]205[.]122:28855
61[.]230[.]205[.]132:28833
61[.]230[.]205[.]132:28844
61[.]230[.]205[.]132:28855

TREND MICRO ™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thought-provoking research that can shape strategic industry direction.

www.trendmicro.com