

## 侵入の痕跡 (Indicators of Compromises, IoCs)

iOS App Store で特定された偽のアプリの一部 (IOS\_Chameleon.A として検出)

| アプリ名/ラベル名                   | バンドル名                          | バージョン名 |
|-----------------------------|--------------------------------|--------|
| グローバルホリデー情報— 28 元の登録        | com.luther.worldholiday        | 1.6    |
| グローバルホリデー情報— 28 元の登録        | com.gavinjeremy.publicholidays | 1.1    |
| 微醺                          | KK.WeiXun                      | 1.0.1  |
| semsiye                     | com.semsiye.semsiye            | 1.2    |
| HappyEnglishTOKorean        | com.HappyEnglishTOKorean       | 1.2    |
| No Hit                      | com.NoHit.cw                   | 1.0.2  |
| TeaAssistant                | com.wuzhongxin.teaassistant    | 1.1    |
| SkyMadness                  | sky.madness.com                | 1.0.1  |
| Simon Color Match           | com.jda.Color-Match            | 1.3    |
| Classic Poems               | com.abcd.Poems                 | 1.2    |
| Employee attendance tracker | com.emp.att                    | 1.1    |

Google Play で特定された偽のアプリの一部 (AndroidOS\_Gambling.HRX として検出)

| パッケージ名                   | SHA256 値   | バージョン名 |
|--------------------------|--|--------|
| com.hh.ii.d587           | B8409F8D625AACEF0DA1C50075443833781FD935DEF608FE<br>396B11D4EEC619AE | 1.0    |
| com.hh.ii.p557           | AD791FBAD2C3F06FE7C8CA9820D7D6F62C5C0BAAA83502<br>3472ADA1276C80CF7E | 1.0    |
| com.hh.ii.c603           | 4D7F591760EF07A2F240A6EF0AF4F9544437833A83C68B03E<br>8E04F0E662B38F4 | 1.0    |
| com.liuhe.fenxi.ruanjian | 98F4C2CAB302C1B5954D8EC3B0658D83958D522DE6157B1<br>4171AAA6BB45F5798 | 1.0    |
| com.jz.shequ.jiaoliu     | 8DB2AD04FD93704954CEE498F2431E98CAAD9D1E9BB836D<br>EBD5BBF982A2FD246 | 1.0    |
| com.tain.jing.ssc        | B7DCF23836919EC4CF5E71D313E4866CDAD0C8D514BFF0D<br>E8C3147E65D3EEA93 | 1.0    |
| com.jiu.ou.id2957        | 6C368EF20A419C3E792435C9DAF3CE9CD239611BDD6D408<br>40CA70E56669B5A24 | 1.0    |

|                   |  |     |
|-------------------|--|-----|
| com.jiu.ou.id2969 | 1338C22DE793CF4C6F523A6C1A42C9EEFE5886F3C345ADF2<br>D469C90323CC0691 | 1.0 |
| com.jiu.ou.id2968 | 35B16C8A575B586BA10D0CEF9DB0356E7EBEDF93F887F3A5<br>E90BD971557204D2 | 1.0 |
| com.jiu.ou.id3001 | DAF9E73A4B256D15D9A231B12A0DCDBD4BB152F6557BFF<br>76D184A9286A2DB456 | 1.0 |
| com.jiu.ou.id3006 | C8355E6A056884CD781A36302CC8CE66CE1A912100AE37B<br>28DBE44D3FDD2D702 | 1.0 |
| com.jiu.ou.id3007 | 375EB929AF991AFA92769DE5D285BC7E4085150BD585335<br>D4BDC460101849970 | 1.0 |
| com.jiu.ou.id3000 | 6ADCD1D37D0024EA9E3C443BE029A774D845E2A9EFF48D<br>D43988B05161454077 | 1.0 |
| com.jiu.ou.id3002 | 42F90F0B9B635057170933AA8E73E869728B797010C6CA48<br>91FA59E4D63F377C | 1.0 |
| com.jiu.ou.id3010 | 4DD441A5559E9F17B3A275AFDD73E18FEB27BFB37E9F9C02<br>7CEE8D62A268E846 | 1.0 |

関連する不正なドメイン／URL の一部は以下の通りです。

- app[.]kaiguan1700[.]com
- xx1700.com
- 1700c5.com
- 1700c6.com
- 1700c7.com

## 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](http://www.trendmicro.com)

