

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

### 検体 1 :

| ファイル名                   | SHA256   | 検出名                      |
|-------------------------|--|--------------------------|
| plugin                  | 6fe741ef057d38dd6d9bbe02dacbcb4940dac6c32e0f50a641<br>e73727d6bf60d9 | Trojan.SH.GMERA.<br>A    |
| stock                   | 6f48ef0d76ce68bbca53b05d2d22031aec5ce997e7227c3dcb<br>20809959680f11 | Trojan.SH.GMERA.<br>A    |
| Stockfoli               | efd5b96f489f934f2465a185e43fddf50fcde51b12a8fb91d5d9<br>3b09a21706c7 | Trojan.MacOS.GM<br>ERA.A |
| Trial_Stockfol<br>i.zip | 18e1db7c37a63d987a5448b4dd25103c8053799b0deea5f45f<br>00ca094afe2fe7 | Trojan.MacOS.GM<br>ERA.A |

### 不正な URL :

- [hxxps://appstockfolio.com/panel/upload\[.\]php](https://appstockfolio.com/panel/upload[.]php)
- [gmzera54l5qpa6lm\[.\]onion](https://gmzera54l5qpa6lm[.]onion)

検体 2 :

| ファイル名               | SHA256  | 検出名                      |
|---------------------|---|--------------------------|
| com.apple.upd.plist | be8b6549da925f285307b17c616a010a9418af70d090ed960ade575ce27c7787            | Trojan.MacOS.GM<br>ERA.B |
| run.sh              | d50f5e94f2c417623c5f573963cc777c0676cc7245d65967ca09a53f464d2b50            | Trojan.SH.GMERA<br>.B    |
| Stockfoli           | 83df2f39140679a9cfb55f9c839ff8e7638ba29dba164900f9c77bb177796e03 (sample 2) | Trojan.MacOS.GM<br>ERA.B |
| Trial_Stockfoli.zip | faa2799751582b8829c61cbfe2cbaf3e792960835884b61046778d17937520f4 (sample 2) | Trojan.MacOS.GM<br>ERA.B |

不正な URL およびサーバ :

- **hxxp://owpqkszz[.]info/link.php?{ユーザ名}&{IP アドレス}**
- **193[.]37[.]1212[.]176 (C&C サーバ)**

## 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)



©2019 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.