■侵入の痕跡（Indicators of Compromise、IoC）

SHA256	検出名
6413be289cf38c2462bd8c6b8bad47f8d953f399e1ccba30126a1fb70d13a733	Trojan.X97M.PANDASTEAL.AA
4ff1f8a052addbc5a0388dfa7f32cc493d7947c43dc7096baa070bfc4ae0a14e	Trojan.Win32.PHOBOS.B
0a9f466fb5526fd512dd48c3ba9551dbd342bdb314a87d5c6f730d3c80041da6	TrojanSpy.X97M.PANDASTEAL.THDABBA
05d38ac5460418b0aa813fc8c582ee5be42be192de10d188332901157c54287c	TrojanSpy.Win32.PANDASTEAL.THDABBA
1efa74e72060865ff07bda90c4f5d0c470dd20198de7144960c88cef248c4457	TrojanSpy.Win32.PANDASTEAL.THDABBA

URLs

- hxxp://23.92.213.108/po/aXSz3[.]exe
- hxxp://23.92.213.108/po/tai1[.]exe
- hxxp://prtboss.com/collect[.]php
- hxxp://biscosuae[.]com
- hxxp://prtanet[.]com
- hxxps://paste.ee/r/pLpR9
- hxxps://paste.ee/r/Qsowz
- hxxps://paste.ee/r/6toiY

- hxxp://cocojambo.collector-steal.ga/collect.php
- hxxp://f0522235.xsph.ru/collect.php
- hxxp://guarantte.xyz/collect.php
- hxxp://f0527189.xsph.ru/collect.php
- hxxp://f0527703.xsph.ru/collect.php
- hxxp://j1145058.myjino.ru/collect.php
- hxxp://1wftyu121cwr24v3hswa1234g.tk/collect.php
- hxxp://f0527262.xsph.ru/collect.php

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 thoughtprovoking research that can shape strategic industry direction. www.trendmicro.com