

侵入の痕跡 (Indicators of Compromise, IoC)

SHA256	検出名
e394e53e53cd9047d6cff184ac333ef7698a34b777ae3aac82c2c669ef661dfe	AndroidOS_SpyAgent.HRxB
e8d4713e43241ab09d40c2ae8814302f77de76650ccf3e7db83b3ac8ad41f9fa	AndroidOS_ProjectSpy.HRX
29b0d86ae68d83f9578c3f36041df943195bc55a7f3f1d45a9c23f145d75af9d	AndroidOS_ProjectSpy.HRX
3a15e7b8f4e35e006329811a6a2bf291d449884a120332f24c7e3ca58d0fbbd	IOS_ProjectSpy.A

関連する URL

- cashnow[.]ee Backend server
- ftp[.]XXXX[.]com Backend server
- spy[.]cashnow[.]ee Backend server
- xyz[.]cashnow[.]ee Backend server

MITRE ATT&CK Framework

- Android

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



©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.