

侵入の痕跡 (Indicators of Compromises, IoCs)

SHA256 値	機械学習による 検出名	パターン検出名
13a4751b83e53abdf0fb6d5876d6cc9dfbd33e34303 8dae6951de755d93c8284	Troj.Win32.TRX.XXP E50FFF031	Coinminer.Win64.MALXM R.TIAOODBZ
558914713cf3174c8b489aef12a1a7871ad886bc9483 fd7b0790383702bfd75d		
7cec25bdb7c3cb2778168e9b02e0fdd608a6c94cb69f eba7b4ee647aef0588b1		
8ffa7f991637e28fa5b4ae7f5522fe5fee622307bed87 d1d478c48fa0696dc5a		Coinminer.Win64.MALXM R.TIAOODC
a0e0e5d0ff95e3193ed0999234588e3327ea8d75931 6a0d1175c5084daf5b083		
aa16c957a85ecedaac9f629082913dfdaefe95b8b819 1d7cb3e8c02da2963452		

今回の検体に関連する不正な URL および IP アドレスは以下の通りです。

- 118[.]24[.]63[.]208
- 103[.]105[.]59[.]68

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.