侵入の痕跡（Indicators of Compromise, IoC）

種類	値
C&C サーバ	mazeclmhbacucxin[.]onion
C&C サーバ	mazeclmhbacucxin[.]tor2web[.]su
C&C サーバ	mazeclmhbacucxin[.]tor2web[.]to
C&C サーバ	mazeclmhbacucxin[.]tor2web[.]io
C&C サーバ	mazeclmhbacucxin[.]tor2web[.]in
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]onion/int.x86_64
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]onion/cpu
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]onion/bot
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]onion/trc
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]onion/cmd
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]su/int.x86_64
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]su/cpu
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]su/bot
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]su/trc
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]su/cmd
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]to/int.x86_64

マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]to/cpu
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]to/bot
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]to/trc
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]to/cmd
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]io/int.x86_64
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]io/cpu
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]io/bot
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]io/trc
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]io/cmd
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]in/int.x86_64
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]in/cpu
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]in/bot
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]in/trc
マルウェアのダウンロード	hxxp://mazeclmhbacucxin[.]tor2web[.]in/cmd

種類	ファイル名	sha1	検出
マルウェアファイル	int.x86_64	e4bf3e717ba34f3f06e0c35acce0e3138a7f85b3	Coinminer.Linux.SYSTEMDMINER.C
マルウェアファイル	cpu	0872a8a5a9847d3d2296ae390b21f179418312aa	TROJ=FRS.VSNTE820
マルウェアファイル	ucxin.sh	8e0498cf71e54533e6510ea02b852b721bcbdc0f	Coinminer.Linux.MALXMR.UWEKO

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.