侵入の痕跡（Indicators of Compromise, IoC）

ファイル名	SHA-256	検出名
d.py	29316f604f3c0994e8733ea43da8e0e81a559160f5c502fecbb15a71491faf64	Trojan.Python.MALXMR.D
i686	35e45d556443c8bf4498d8968ab2a79e751fc2d359bf9f6b4dfd86d417f17cfb	Coinminer.Linux.MALXMR.UWELD
x32b	9b8280f5ce25f1db676db6e79c60c07e61996b2b68efa6d53e017f34cbf9a872	Backdoor.Linux.KAITEN.AMV
x64b	855557e415b485cedb9dc2c6f96d524143108aff2f84497528a8fcddf2dc86a2	Backdoor.Linux.KAITEN.AMV
x86_64	fdc7920b09290b8dedc84c82883b7a1105c2fbad75e42aea4dc165de8e1796e3	Coinminer.Linux.MALXMR.UWELD
xmi	51654c52e574fd4ebda83c107bedeb0965d34581d4fc095bbb063ecefef08221	Trojan.Linux.MALXMR.USNELH820

URL

- 205[.]185[.]113[.]151

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