侵入の痕跡（Indicators of Compromise, IoC）

File	SHA-256	Detection name
ldr.ps1	093b72e9b4efcc30c1644a763697a235c9c3e496c421eceaac97d4babeba7108	Trojan.PS1.MALXMR.MPF
sys.exe	566b0187d8ff500d923859c98da2c96b8b581e93ac0c94dacba76328b34412b3	PUA.Win64.CRYPTOMINER.CFL
kthreaddk	67e38438759f34eaf50d8b38b6c8f18155bcc08a2e79066d9a367ea65e89aa3d	Coinminer.Linux.MALXMR.SMDSL64
ldr.sh	93d380ba2bedd37c2313924784b26fec27c9e96e4c500b5cb78259b3c824ee4e	Coinminer.SH.MALXMR.SM

IP address	Detail
194[.]145[.]227[.]21	Malware accomplice

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