Indicators of Compromise

詳細	SHA256 値	検出名
Kerberods （コインマイナーのバイナリ）	a9228b6a3fe0b8375d6b881626fd4b59fbbf54dbd60a94b085ee0455b3d18fe9	Trojan.Linux.KERBERDS.A
Khugepageds （仮想通貨発掘マルウェア）	25064a5ab78cdd36e7049d00b9319222906dd634908c1858e2262bf333631213	Coinminer.Linux.MALXMR.UWEJI
random.so （ルートキット）	3392589c9ebbf7600035574e338d69625cd5ce83ee655582fe8bbadb663532b3	Rootkit.Linux.KERBERDS.A

関連する URL/ドメインは以下の通りです。

- gwjyhs[.]com
- gwjyhs[.]com
- hxxps://pastebin[.]com/MjGrx7EA
- hxxps://pastebin[.]com/CvJM3qz5
- hxxps://pastebin[.]com/raw/60T3uCcb|sh
- hxxps://pastebin[.]com/raw/rPB8eDpu
- systemten[.]org:51640（マイニングプール）

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