侵入の痕跡（Indicators of Compromise, IoC）

Kaiji

ファイル名	SHA 256	トレンドマイクロでの検出名
123.sh	9301d983e9d8fad3cc205ad67746cd111024daeb4f597a77934c7cfc1328c3d8	Trojan.SH.KAIJI.A
linux_arm	d315b83e772dfddbd2783f016c38f021225745eb43c06bbdfd92364f68fa4c56	DDoS.Linux.KAIJI.A

関連する URL：

- hxxp://62[.]171[.]160[.]189/linux_arm
- hxxp://62[.]171[.]160[.]189/11/123.sh

同一の U R L から確認された XORDDoS と他のマルウェアの亜種

SHA 256	トレンドマイクロでの検出名
dba757c20fbc1d81566ef2877a9bfca9b3ddb84b9f04c0ca5ae668b7f40ea8c3	Backdoor.Linux.XORDDOS.AE
6c8f95b82592ac08a03bfe32e4a4dbe637d1f542eb3ab3054042cec8ec301a3c	Backdoor.Linux.DOFLOO.AB
286f774eb5b4f2f7c62d5e68f02a37b674cca7b8c861e189f1f596789322f9fe	Backdoor.Win32.SDDOS.A

関連する URL：

- hxxp://122[.]51[.]133[.]49:10086/VIP

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