侵入の痕跡（Indicators of Compromise, IoC）

ボットネット「Muhstik」による攻撃キャンペーン

File Name	SHA 256	Trend Micro Pattern Detection
pty86	0e574fd30e806fe4298b3cbccb8d1089454f42f52892f87554325cb352646049	Backdoor.Linux.TSUNAMI.AMX
m8	3dbcd99edb3422b8fdc458b82aa7ecfe31296d32bb4d54450c9e9cac29fb6141	Trojan.SH.MALXMR.UWELD
kswapd	a254a26a27e36de4d96b6023f2dc8a82c4c4160a1d72b822f34ffdd5e9a0e0c9	Coinminer.Linux.MALXMR.SMDSL64

IPs

- hxxp://188[.]166[.]137[.]241/wp-content/themes/twentyseventeen/dk86
- hxxp://153[.]121[.]58[.]102:80/wp-content/themes/zuki/m8
- hxxp://3[.]10.224[.]87/[.]a/dk86

マルウェア「Kinsing」による攻撃キャンペーン

File Name	SHA 256	Trend Micro Pattern Detection
wb.sh	61879d5b2f083b69e8e6cc6afce00be6619176151b093de14f2778a87ea46565	Trojan.SH.CVE20207961.SM

kinsing	6e25ad03103a1a972b78c642bac09060fa79c460011dc5748cbb433cc459938b	Coinminer.Linux.MALXMR.PUWEMA
kdevtmpfsi	dd603db3e2c0800d5eaa262b6b8553c68deaa486b545d4965df5dc43217cc839	Coinminer.Linux.MALXMR.SMDSL64

IPs

- hxxp://194[.]38[.]20[.]199/wb.sh
- hxxp://194[.]38[.]20[.]199/kinsing

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