

侵入の痕跡 (Indicators of Compromises, IoCs)

侵入の痕跡	検出名	ファイル名
fastimage[.]site	ShadowGate/WordsJS malicious domain	
ad4989[.]world	ShadowGate/WordsJS malicious domain	
adsfast[.]site	GreenFlash Sundown EK domain	
adsfast[.]info	GreenFlash Sundown EK domain	
cdn-cloud[.]club	GreenFlash Sundown EK domain	
aeb073b5ee2e083aba987c7fcaab7265aa be6e5e2cade821db6d46e406e21e95	Coinminer.Win32.MALXMR.S MBM4	hp_3.exe
58002d0b8acd1a539503d8ea02ff398e7a d079e0b856087f0ca30d767588be4e	Coinminer.Win64.TOOLXMR.S MA	hp_6.exe

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

