■ 侵入の痕跡（Indicators of Compromise、IoC）

ファイル名	SHA256	検出名
setup-installv1.3.exe	787939d2fc30c7b6ff6ddb7f4e7f981c2a2bad0788b2f4d858c3bb10186d42f6	Trojan.Win32.MULTDROPEX.A
setup_installer.exe	bdf727b2ac0b42a955c4744bf7768cbb9fa67167321e4fb5639ee5529ccbcfa4	Trojan.Win32.MULTDROPEX.A
setup_install.exe	97f18d430b68ac9379ecd267492e58734b3c57ffd66615e27ff621ea2bce8e6b	Trojan.Win32.MULTDROPEX.A
5f9a813bc385231.exe	9dcacda3913e30cafd92c909648b5bffde14b8e39e6adbfb15628006c0d4d3c2	Trojan.Win32.SOCELARS.CDK
sqlite.dll	5c41a6b98890b743dd67caa3a186bf248b31eba525bec19896eb7e23666ed872	TrojanSpy.Win32.SOCELARS.CDK
b5203513d7.exe	a5f373f8bcfae3d9f4895c477206de63f66f08e66b413114cf2666bed798eb71	Coinminer.MSIL.MALXMR.TIAOODBH
5f9a813bc38523010.exe	8bd8f7a32de3d979cae2f487ad2cc5a495afa1bfb1c740e337c47d1e2196e1f2	Trojan.Win32.DEALOADER.A
aae15d524bc2.exe	1cdddf182f161ab789edfcc68a0706d0b8412a9ba67a3f918fe60fab270eabff	TrojanSpy.Win32.BROWALL.A
bf2e8642ac5.exe	e3c9119e809a1240caaaf4b6d5420352f037cc2585cb321cb746f05ed0ec0e43	TrojanSpy.Win32.SOCELARS.D
745d0d3ff9cc2c3.exe	b151ffd0f57b21600a05bb28c5d1f047f423bba9750985ab6c3ffba7a33fa0ff	TrojanSpy.Win32.VIDAR.D
438dc1669.exe	e254914f5f7feb6bf10041e2c705d469bc2b292d709dc944381db5911beb1d9f	Trojan.Win64.REDLINESTEALER.N

1cr.exe	949eec48613bd1ce5dd05631602e1e1571fa9d6b0034ab1bffe313e923aff29c	TrojanSpy.MSIL.REDLINESTEALER.N
a6168f1f756.exe	c5483b2acbb352dc5c9a811d9616c4519f0e07c13905552be5ec869613ada775	Coinminer.MSIL.MALXMR.TIAOODBL
f65dc44f3b4.exe	dc5bbf1ea15c5235185184007d3e6183c7aaeb51e6684fbd106489af3255a378	Mal_HPGen-50
a070c3838.exe	9e1a149370efe9814bf2cbd87acfcfa410d1769efd86a9722da4373d6716d22e	TROJ_GEN.R053C0PHC21

不正な **URL:**

- **hxxp://fsstoragecloudservice[.]com/data/data[.]7z**
- **hxxp://3[.]128[.]66[.]194/**
- **45[.]14[.]49[.]68**
- **plugnetx[.]com**
- **znegs[.]xyz**
- **iryarahara[.]xyz**
- **swiftlaunchx[.]com**
- **bluewavecdn[.]com**
- **sproutfrost[.]com**
- **hxxp://37[.]0[.]11[.]8/**
- **hxxp://52[.]51[.]116[.]220/**
- **195[.]181[.]169[.]68**
- **88[.]99[.]66[.]31**

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 thoughtprovoking research that can shape strategic industry direction. www.trendmicro.com