侵入の痕跡（Indicators of Compromise, IoC）

関連 URL

- hxxp://45[.]9[.]148[.]123/COVID19/nk/NarrenKappe.sh
- hxxp://45[.]9[.]148[.]123/COVID19/sh/clean.sh
- hxxp://45[.]9[.]148[.]123/COVID19/sh/lan.ssh.kinsing.sh
- hxxp://45[.]9[.]148[.]123/COVID19/sh/setup.basics.sh
- hxxp://45[.]9[.]148[.]123/COVID19/sh/setup.mytoys.sh
- hxxp://45[.]9[.]148[.]123/COVID19/sh/setup.xmrig.curl.sh
- hxxp://teamtnt[.]red/dns
- hxxp://teamtnt[.]red/sysinfo
- hxxp://teamtnt[.]red/up/setup_upload.php
- irc[.]kaiserfranz[.]cc

ファイル名	SHA-256	検出名
clean.sh	6b8d828511b479e3278264eff68059f03b3b8011f9a6daaeff2af06b13ba6090	Trojan.SH.HADGLIDER.C
dns	6c73e45b06544fc43ce0e9164be52810884f317a710978c31462eb5b8ebc30cc	Trojan.SH.HADGLIDER.D
init.sh	459190ba0173640594d9b1fa41d5ba610ecea59fd275d3ff378d4cedb044e26d	Trojan.SH.HADGLIDER.A
mxutzh.sh	8926672fe6ab2f9229a72e344fcb64a880a40db20f9a71ba0d92def9c14497b6	Coinminer.SH.HADGLIDER.A
NarrenKappe.sh	7d791ac65b01008d2be9622095e6020d7a7930b6ce1713de5d713fc3cccfa862	Trojan.SH.HADGLIDER.TSD
setup.mytoys.sh	b60be03a7305946a5b1e2d22aa4f8e3fc93a55e1d7637bebb58bf2de19a6cf4a	Trojan.SH.HADGLIDER.F
setup.xmrig.curl.sh	bebaac2a2b1d72aa189c98d00f4988b24c72f72ae9348c49f62d16b433b05332	Trojan.SH.HADGLIDER.J
sysinfo	3c907087ec77fc1678011f753ddf4531a484009f3c64563d96eff0edea0dcd29	TrojanSpy.SH.HADGLIDER.A

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