侵入の痕跡（Indicators of Compromises、IoCs）

ネットワーク

- miniast[.]com:443
- tenchier[.]com:443
- boreye[.]com:80
- boreye[.]com:53
- pilutce[.]com:443

コインマイナーのサンプルハッシュ値

SHA256 値	検出名
dd21a9ce1d87e3a7f9f2a592ec9dd642ca19aee4a60502c8df21d9c25f9acf86	Trojan.Win64.VOOLS.AF
2af73c8603e1d51661b0fffc09be306797558204bcbd4f95dd2dfe8363901606	Trojan.Win64.VOOLS.AB
ed2febf310ae90739002b9ddb07a29d0b2c8e92462ae4a0a6dcc19cc537ddef3	Trojan.Win64.VOOLS.AB
007f81debf1c984c5b4d5b84d6a8c06bcdf84d1a4cccdd9633e45de35015faf3	PE_VIRUX.R-3
125f93883ccccb3c33964c8bcdd17b409b53fbc44de1e3b4afd7dfe79aa358cd	Coinminer.Win64.TOOLXMR.SMA
1ac26e86540610d1293c421ed05c13cd6ed51759be153c45d194ff7552c88855	Coinminer.Win64.TOOLXMR.SMA

4c3575c7b6c530603e4cd76c7dcaed12fc5ebadbf4d4d6b46352eb08458683e8	Coinminer.Win64.TOOLXMR.SMA
4e46cec7f6e7fa13c10e808f0da104a8c810b7ef17c40d0e9a908453be87e7f4	Coinminer.Win64.TOOLXMR.SMA
5472f9ba3bc623450cc208669dacddb1b6a73ffe4dc705b85cf41637070fda28	Coinminer.Win64.TOOLXMR.SMA
572c3943f70a3e362d9bf195ce37cec68074235eb1abba9f0cdbb91f5231a572	Coinminer.Win64.TOOLXMR.SMA
5db45fa654910495592cf1ca00d7ef537708c38c4803d10d89eaa0ddba0e7d8c	Coinminer.Win64.TOOLXMR.SMA
6ee5c5724ecc70f77aadcf00c77829e5313f44c61b2720113ada0c8263ac662c	Coinminer.Win64.TOOLXMR.SMA
7ced0990ac94f36fab21821395f543f3a06be486c9f34cdc137874912573fb27	Coinminer.Win64.TOOLXMR.SMA
7f5bddeb0c9ecde4d64ddac8b046859fb1627811d96c29dfa2b88102740571ce	Coinminer.Win64.TOOLXMR.SMA
94af094fc02cfe85a80f2f90d408f9598f9d77def36155e16a90e2bd8f8fdcce	Coinminer.Win64.TOOLXMR.SMA
975dc8ecda9a9c15d19c4d9d67f961366d2f0ac1074b5eb5d3b36e653092a6a3	Coinminer.Win64.TOOLXMR.SMA
bafe63e8fd76f1c9010137e6cd5137655ea12ab5c25d0b86700627b2ebad2be0	Coinminer.Win64.TOOLXMR.SMA
ce5025a484b3e2481e248dee404e6d321b6d7f58bae77b284ec9e602672e6a10	Coinminer.Win64.TOOLXMR.SMA

ce8cb7c8dc29b9e4feab463fdf53b569b69e6a5c4ab0e50513b264563d74a6ac	Coinminer.Win64.TOOLXMR.SMA
9af55d177e7d7628dc63f7753de4780031073098e1c674e619826cb97c190744	Coinminer.Win64.TOOLXMR.AR
f81dd3e5b0507d78815f5909ab442545cb3f5262397abd89b5947e1e7b3fef12	Coinminer.Win64.TOOLXMR.AQ
35d10df58e340b6a7d69e590852b84a6a02f774306c3eb29e60e6b24740456eb	Coinminer.Win32.MALXMR.SMBM4
13800d1075e56f9bd0d87b2e85555040233e8b2ec679770101d046ffa4e39582	Coinminer.Win32.MALXMR.SMBM4
199e0419622e108ffdd7c9de571931d9aedc4f980a602766c0fdcb17bdddfc2a	Coinminer.Win32.MALXMR.SMBM4
1bc9762470423393521d9aa64d505501d201d3cb50c8e6576d4381590b090d75	Coinminer.Win32.MALXMR.SMBM4
2d6a5eb8a78cddee8ce90321aab80f85784b11a87b00fde75c4c457998a5aebd	Coinminer.Win32.MALXMR.SMBM4
3638ee8c0153b2763eb36246d9ffe4f7ec6d1f7e76876fb6f579c45e6e55e260	Coinminer.Win32.MALXMR.SMBM4
469e7ac4b5bad89e305e1e7ec65773844f3d639e84476da4b1fdf442a7c28504	Coinminer.Win32.MALXMR.SMBM4
59e3cf8f342a2bb5ce22bb03f8671568f68751f807002f9b329ed58e12a8831c	Coinminer.Win32.MALXMR.SMBM4
5cd9ff29454e84923d4178484ecfb3bc48561d4401fa94b98f9d2693d47a740a	Coinminer.Win32.MALXMR.SMBM4

6173542183c304ac2efc0348df799c1e3dea508cceaaac461bd509dc436d4edf	Coinminer.Win32.MALXMR.SMBM4
82c0b0fbb0f44ad2bc46c8b105f167f0feadf936ff811f97aab3a9a6cccc2fb2	Coinminer.Win32.MALXMR.SMBM4
87488d9ad54b88e5488c18d8de6a338eaf4fe7bdeec2df7eeaf90380de1533b6	Coinminer.Win32.MALXMR.SMBM4
8d402a3871bada94d84dd8a7c29361f27b75ac37394f6de059b06afb340fe3d6	Coinminer.Win32.MALXMR.SMBM4
9853e7bd0906cf92d2767fa55ee0a645f23099b37d59654d3c388d897a19fb1e	Coinminer.Win32.MALXMR.SMBM4
af21fb86d48b60ee58084570fba12cf3dbc3992c713421a265cd451c169967d2	Coinminer.Win32.MALXMR.SMBM4
cf60518d2a22631d0539964ff97bc396b44ef5f6979f7a9e59e03c89598db0bf	Coinminer.Win32.MALXMR.SMBM4
ec85ec44771401d4a71cb7f8bc3597d55ec02b84178464ab33161c77c4f51f0b	Coinminer.Win32.MALXMR.SMBM4
ecfcd390712f6ac57b822ef519063f8e9151e90549e245e4e2a70d02ff584634	Coinminer.Win32.MALXMR.SMBM4

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