侵入の痕跡（Indicators of Compromise, IoC）

ランサムウェア「**DARKSIDE**」

SHA-256	検出名
9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c12045839075f7627297	Ransom.Win32.DARKSIDE.YXAH-THA

URL

- hxxp://darksidedxcftmqa[.]onion/

ランサムウェア「**CRYSIS**」

SHA-256	ファイル名	検出名
1cec5e4563e2c1570353e54a4ecc12ab4d896ab7227fd8651adcd56b884c0c1c	GdAgentSrv.de.dll	HackTool.Win64.CVE20160099.A
28042dd4a92a0033b8f1d419b9e989c5b8e32d1d2d881f5c8251d58ce35b9063	process-hacker-2-39.exe	PUA.Win32.ProcHack.A
3680b9e492f49abc108313c62ceb0f009d5ed232c874cae8828c99ebf201e075	takeaway.exe	Ransom.Win32.CRYSIS.TIBGGS
47dc3672971c242154a36622145de7060f17f56af75d21e2130e4f57089f5e48	takeaway.exe	Ransom.Win32.CRYSIS.TIBGGS
75d9d85b152e030eb73d17c691203b49bf593ea6a4bddeae48ca255b22c2d36d	takeaway_ps1	Trojan.PS1.CRYSIS.AA

77cbab006cf6a801dbd1c752659bddf28562fb8681d20305dd1dc0b1e105c67a	takeaway.exe	Ransom.Win32.CRYSIS.TIBGGS
78983ad10fe05fadccb201dd3e8c7f952e93332433a42e3d331531c5497d1330	winhost.exe	Ransom.Win32.CRYSIS.TIBGGQ
b0b8fd4f6ab383014ea225c2b7776735af059f526cd7c4fdbdcb2e99d074ade7	takeaway.exe	Ransom.Win32.CRYSIS.TIBGGS
b2d2f4ecbc680d590743044744b3ff33c38e4aeb0ada990b0ae7be8291368155	takeaway.exe	Ransom.Win32.CRYSIS.TIBGGS
b5a69f7c4a3681a753f3512e3b36ac06c6ddbb1129a3e87f8c722ff4f9834f0a	purgeMemory.ps1	Trojan.PS1.KILLSVC.Ahacktool
edef024abe48d6ed7b4757d63a8fd448a8ecf1ad15afd39cc97c97b27ed4498e	takeaway.exe	Ransom.Win32.CRYSIS.TIBGGS
ef5f2ce1a4d68d656400906ae906b0c7e7f61017f14840a7ac145d59ee69a4bd	takeaway.exe	Ransom.Win32.CRYSIS.TIBGGS
f47e3555461472f23ab4766e4d5b6f6fd260e335a6abc31b860e569a720a5446	NS2.ex	HackTool.Win32.NetTool.A

情報窃取型マルウェア「**NEGASTEAL**」

SHA-256	検出名
58e74875b3659fa34aa1ecefba1a43cc049b7bb1c83de5a26ec8045c60f1099e	Trojan.W97M.CVE201711882.YQUOOUM
6991150c06b278712b052377ef768ca80923ff9c3396e7de18fa0fbce7211c96	TrojanSpy.MSIL.NEGASTEAL.DYSGXT

コインマイナー

SHA-256	検出名	機械学習型検索による検出

12434186b803afd5e75b77bf8439d968ef0bb18ed8a871a279b95fe0a6c4e132	Coinminer.Win32.MALXMR.THHADBO	Troj.Win32.TRX.XXPE50FFF036
2da7be1ed9f13424c7b747caea0030b5b19007597640e9700add15bc8d236a1e	Trojan.Win32.MALXMR.THHADBO	N/A
329788672911aaed64ba2add41a09f93b878bf8a3291c1309988acadb3643141	Trojan.VBS.MALXMR.THHADBO	N/A
663e4b7c209e864faaf598d791a9a6958c70f75bf974853d59bd15bc2a931163	Trojan.Win32.MALXMR.BX	N/A
9dade12201cc88cbd90f2fbaf4d50e512d4a377debad6714f19e10195e3a91be	Trojan.Win32.MALXMR.BX	N/A
a24f84fa1302c9f4b68791532d2d7dbb0269e2ac2f245652164934289a1ba37e	Trojan.Win32.MALXMR.BX	N/A
a78c0bd4cf9f4e21dea1fa67e92a6498c5df83c3ae57bb1f02d40da44e55cd69	Coinminer.Win32.MALXMR.THHADBO	Troj.Win32.TRX.XXPE50FFF036
ae54783709a60e685846b3812d4e65b54672c8c40d2e8499fa92255ef89b7375	Trojan.Win32.MALXMR.BX	N/A
cd4b97c42b5ce9540f141498e2fdd4d566ea0b835d0c295994bf644744b5d4dd	Trojan.Win32.MALXMR.BX	N/A

URLs

- hxxps://pastebin[.]com/raw/jimA8sdx
- hxxp://135[.]181[.]34[.]1/min3/loader23435345465446[.]jpg
- hxxps://pastebin[.]com/raw/Yvyd9wXa
- monerohash[.]com:3333

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

©2019 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.