■侵入の痕跡（Indicators of Compromise、IoC）

本記事で紹介した「Avaddon」ランサムウェアに関連する侵入の痕跡（IoC）の一覧は、こちらをご参照ください。

Avaddon Ransomware

SHA-256	Trend Micro pattern detection	Trend Micro machine learning detection
f3f4d4e4c6704788bc8954ca6f6ddc61b006aba89d5d384794f19424a3d24132	Ransom.Win32.AVADDON.YJAF-A	Troj.Win32.TRX.XXPE50FFF036
6616abb725c24307f4f062996edc5150079bc477acd4236a4f450e5835a20c62	Ransom.Win32.AVADDON.YJAF-A	Troj.Win32.TRX.XXPE50FFF036
4f198228806c897797647eecce0f92d4082476b82781183062a55c417c0bb197	Ransom.Win32.AVADDON.YJAF-A	Troj.Win32.TRX.XXPE50FFF036
05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2	Ransom.Win32.AVADDON.YJAF-A	Troj.Win32.TRX.XXPE50FFF036

b8d6fd333973adb640649cab8c9e7575a17b5a8bc382e3335400d43a606a6253	Trojan.JS.AVADDON.YJAF-A	Not Applicable
a481d2b64c546f68d55e1fd23e57ada80b6b4e2c3dd7b0466380dba465f3d318	Trojan.JS.AVADDON.YJAF-A	Not Applicable
5a47a89a870d7db244c76da43887e33c9ee4b26f9972878b1a6616be0302439f	Trojan.JS.AVADDON.YJAF-A	Not Applicable
12bc439445f10a04b574d49ed8ccc405e2dfaa493747585439643e8a2129e5e5	Trojan.JS.AVADDON.YJAF-A	Not Applicable
cc4d665c468bcb850baf9baab764bb58e8b0ddcb8a8274b6335db5af86af72fb	Trojan.JS.AVADDON.YJAF-A	Not Applicable
ea93ce421be8a2eba34752b8e8da4d241d671ef808a0f8e55a04ceca8ad5113f	Trojan.JS.AVADDON.YJAF-A	Not Applicable

URLs

- hxxp://217.8.117.63/jpr.exe
- hxxp://217.8.117.63/sava.exe
- hxxp://myphotoload.com/photo.php

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