侵入の痕跡（Indicators of Compromise, IoC）

SHA-256	ファイル名	トレンドマイクロ製品の検出名
D55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e	Agent.exe	Trojan.Win32.SODINSTALL.YABGC
E2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2	mpsvc.dll (Side-loaded DLL)	Ransom.Win32.SODINOKIBI.YABGC
8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd	mpsvc.dll (Side-loaded DLL, alternate version)	Trojan.Win32.SODINSTALL.YABGC
2093c195b6c1fd6ab9e1110c13096c5fe130b75a84a27748007ae52d9e951643	Agent.crt	Trojan.Win32.SODINSTALL.YABGC

- このランサムウェアの本体は不正な DLL ファイルです。ドロッパーである「agent.exe」によって作成され、正規の実行ファイルを使用した「DLL サイドローディング」の手法によって実行されます。
  （「agent.exe」と不正な DLL ファイルの双方とも「Trojan.Win32.SODINSTALL.YABGC」として検出対応）
- VSA の手順は「Kaseya VSA Agent Hot-fix」と命名されている
- ランサムウェア本体は、少なくとも 2 つのタスク（encryption と process termination）から特定の PowerShell スクリプトを介して実行されていると推測される

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