侵入の痕跡（Indicators of Compromise, IoC）

MITRE ATT&CK

戦術	技術	ID	概要
Execution	Native API	T1106	Windows API を使用してバイナリを実行
Defense Evasion	Deobfuscate/Decode Files or Information	T1140	ファイルまたは情報の難読化解除を実行
	Masquerading	T1036	実行可能ファイルの名前または場所を操作して、防御を回避
	Virtualization/Sandbox Evasion	T1497	仮想化/サンドボックスの存在を確認して、検出または解析を回避
Discovery	File and Directory Discovery	T1083	ホストまたはネットワーク共有の特定の場所で、ファイルシステム内の特定の情報を検索
	Process Discovery	T1057	システムで実行中のプロセスに関する情報を取得
	Query Registry	T1012	Windows レジストリと対話して、システム、構成、およびインストールされているソフトウェアに関する情報を収集
	System Network Configuration Discovery	T1016	ローカルコンピュータ上のアダプタに関連付けられているアドレスを取得

Collection	Data from Local System	T1005	機密データをローカルシステムソースから収集可能
Exfiltration	Exfiltration Over Alternative Protocol	T1048	データの抽出をメインの C2C プロトコルまたはチャネルとは異なるプロトコルで実行

侵入の痕跡

SHA-256	トレンドマイクロでの検出名
a29da4c0ffe15f0cf1b6c9867af54280da1bad2f28515eb4a49e6260b6388f3c	Trojan.Win32.GLUPTEBA.WLDR

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