侵入の痕跡（Indicators of Compromises、IoCs）

関連する SHA256 値は以下の通りです。

SHA256	検出名
8496E5D746B87976C18E6DE59FE0FEBF97218BFE87028499A5EBB9847281A835	Backdoor.Win32.FARFLI.MRD
CAC7320C0C27C473855ED825988A8C091C9D7FB822F4B9EFF946861EE1EB8F47	Rootkit.Win64.QASSIST.A
0D64F7CB8AFD07DB8803D16BAACCEECEF78C792677EBDFDA9EB3F2583FBC0B8F	Rootkit.Win64.QASSIST.A

RAT が活動時に利用するドメイン／URL は以下の通りです。

URL	通信の目的
151[.]101[.]78[.]133:80 154[.]221[.]22[.]25:80	HTTP POST を介して収集した情報を送信
23[.]215[.]135[.]48:80 23[.]215[.]135[.]42:80	URL にクエリし、インターネットへの接続状態を確認
47[.]246[.]16[.]233:80 47[.]246[.]16[.]233:443 151[.]101[.]78[.]133:80 154[.]221[.]22[.]25:8080	C&C サーバからの応答をリッスンし、バックドアコマンドを取得する
hxxp://www[.]taobao[.]com/help/getip[.]php	URL に接続して C&C サーバの情報を取得する

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 thoughtprovoking research that can shape strategic industry direction. www.trendmicro.com