侵入の痕跡（Indicators of Compromises、IoCs）

本ブログ記事で解析した不正プログラム検体、および関連検体のハッシュ値とファイル名は以下の通りです：

SHA256 ハッシュ値	ファイル名	トレンドマイクロ検出名
6a67af76bdc7ad14d5bf5940786bc7381258l108810075d0ee07683d6a6939c0	miori.arm	Backdoor.Linux.MIRAI.VWIQI
07200eed2edb30665807e641b2290767a40b5bc76f7a035249dee596a982730c	miori.arm5	Backdoor.Linux.MIRAI.VWIQI
c0afc9278c68f75643513987a1d2366f651c4187e1cb1019249f7b0a2d8a1675	miori.arm6	Backdoor.Linux.MIRAI.VWIQI
e086aad1088cd5204f18420e4f953c77c773195226410ca91723345bc539a044	miori.arm7	Backdoor.Linux.MIRAI.VWIQI
0e841443e378a6abd9b9bd51177286f36f421bd5949c28c661e40c187b1b597b	miori.m68k	Backdoor.Linux.MIRAI.VWIQI
86bd270b3e9bc43f8f6bc2e5b0cf5c627ccb2d9e972cfc21fd1faf187d356b43	miori.mips	Backdoor.Linux.MIRAI.VWIQI
dc330cb226e7cc5f14750c91b790c118aaf12116fb77085b34a829b58cdb666c	miori.mpsl	Backdoor.Linux.MIRAI.VWIQI
376536260aa2bf5d8a8155e1a778b547a86575aaadfe5546907eaf34f56d913e	miori.ppc	Backdoor.Linux.MIRAI.VWIQI
739c96713ef797a4fbf204b6b62e31ff9a204f66878aeb330631801f4ee87a24	miori.sh4	Backdoor.Linux.MIRAI.VWIQI
0a2843d1ba842de52795185d11deae5962e869cca0e4b927c3150d49fd576bec	miori.spc	Backdoor.Linux.MIRAI.VWIQI
9f551b1dd0aa5f50d0715f482448d650a2a4dd2e6fb3b2272e2a69d0791d5633	miori.x86	Backdoor.Linux.MIRAI.VWIQI
0a11ec9408298267e8a016a2f4cbf775db961f16e009ddc66279a41d919916fd	sh	Trojan.SH.MIRAI.BNW

今回の検体に関連する不正サイトは以下の通りです：

URL	概要
185.244.39[.]74:10019	C&C サーバ
185.244.39[.]74:25346	情報送出先

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