侵入の痕跡（Indicators of Compromise, IoC）

タイプ	値
C&C サーバ	37[.]49[.]226[.]182:45
C&C サーバ	37[.]49[.]226[.]142:60004
C&C サーバ	192[.]236[.]161[.]206:3456
マルウェアのダウンロード	hxxp://37[.]49[.]226[.]142/bins/
マルウェアのダウンロード	hxxp://37[.]49[.]226[.]142/bins/asdfghjkl.arm
マルウェアのダウンロード	hxxp://37[.]49[.]226[.]142/bins/asdfghjkl.arm5
マルウェアのダウンロード	hxxp://37[.]49[.]226[.]142/bins/asdfghjkl.arm6
マルウェアのダウンロード	hxxp://37[.]49[.]226[.]142/bins/asdfghjkl.arm7
マルウェアのダウンロード	hxxp://37[.]49[.]226[.]142/bins/asdfghjkl.m68k
マルウェアのダウンロード	hxxp://37[.]49[.]226[.]142/bins/asdfghjkl.mips
マルウェアのダウンロード	hxxp://37[.]49[.]226[.]142/bins/asdfghjkl.mpsl
マルウェアのダウンロード	hxxp://37[.]49[.]226[.]142/bins/asdfghjkl.ppc
マルウェアのダウンロード	hxxp://37[.]49[.]226[.]142/bins/asdfghjkl.sh4
マルウェアのダウンロード	hxxp://37[.]49[.]226[.]142/bins/asdfghjkl.spc
マルウェアのダウンロード	hxxp://37[.]49[.]226[.]142/bins/asdfghjkl.x86

タイプ	ファイル名	sha1	検出
マルウェアファイル	asdfghjkl.arm	1d8c184ab3e51460fd5fba39315582da7bb7c76c	Backdoor.Linux.MIRAI.VWISY
	asdfghjkl.arm5	fc81c1ff3cbb07fe9f82fe64168979acd51905cb	Backdoor.Linux.MIRAI.VWISY
	asdfghjkl.arm6	40e6aeb73219139bdcbc06476ae7aadeaa17060c	Backdoor.Linux.MIRAI.VWISY
	asdfghjkl.arm7	ccb9c356f3704c2ae35e63968296a96bacaf1628	Backdoor.Linux.MIRAI.VWISY
	asdfghjkl.m68k	90cbefd3ed9a263641ddb9c3acd98ee220593a9d	Backdoor.Linux.MIRAI.VWISY
	asdfghjkl.mips	91b6ea4dc18fcfa649cada39f8bcaf6ef25c0052	Backdoor.Linux.MIRAI.VWISY
	asdfghjkl.mpsl	67afd5262e4bc1e9eff0feb2100b3ff954b09163	Backdoor.Linux.MIRAI.VWISY
	asdfghjkl.ppc	32eb58ef75630cf4f21801a47c6a2073ec5d885d	Backdoor.Linux.MIRAI.VWISY
	asdfghjkl.sh4	*1fbfe326d1c31e66514abe4b42be21d8824d299f*	*Backdoor.Linux.MIRAI.VWISY*
	asdfghjkl.spc	3045c92842a23f0e88c1c9cd20cc82c33a25e67d	Backdoor.Linux.MIRAI.VWISY
	asdfghjkl.x86	8f4f2ab75fd1f6e9df25cc80350c2232847ad823	Backdoor.Linux.MIRAI.VWISY

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