侵入の痕跡（Indicators of Compromise, IoC）

SHA256 値	トレンドマイクロでの検出名
effeeeadfdc3caf523635fcb86581a807f719fa5e322872854499f5270bc0eba	Backdoor.MacOS.THIEFQUEST.A
365a5c72f52de964b8dc134d2fc45f9c73ba045cebd9fd397b1e26fdb11bfec6	Backdoor.MacOS.THIEFQUEST.A
eeac57f7ca9df9199f0346ed9097e9f5482c06214cddc162d1500d15d045b4ed	Ransom.MacOS.THIEFQUEST.A
5a024ffabefa6082031dccdb1e74a7fec9f60f257cd0b1ab0f698ba2a5baca6b	Virus.MacOS.THIEFQUEST.A-O
c5a77de3f55cacc3dc412e2325637ca7a2c36b1f4d75324be8833465fd1383d3	Virus.MacOS.THIEFQUEST.B-O
d18daea336889f5d7c8bd16a4d6358ddb315766fa21751db7d41f0839081aee2	Virus.MacOS.THIEFQUEST.B-O
e69e9dc0d343165aa0f5df942d1b48ddd0337c8a79dcdf40f3c3b490d6e96a78	Virus.MacOS.THIEFQUEST.B-O
f7efda39c80d68db168316732732d04a00fe6fb10f37d1013df1a8a4cde1f68a	Virus.MacOS.THIEFQUEST.B-O
851dfdbffd250523c5c7ff07b29778a04ebd44400b12f23d18a6ee5a3fcfbedc	Virus.MacOS.THIEFQUEST.B-O
06974e23a3bf303f75c754156f36f57b960f0df79a38407dfdef9a1c55bf8bff	Virus.MacOS.THIEFQUEST.B-O
41036e1b78a122e57f2125526d673ffe3358d7323fc577703662740b3e651dcc	Virus.MacOS.THIEFQUEST.B-O
7292004b57562223fed4ee122a956a8db38349c95d4dd8853b1ebc60ef7508b1	Virus.MacOS.THIEFQUEST.B-O
92ad2b0220f6903fb5fa48ce411af44a60c06031fee3aa682bd28f3f3fde1eda	Virus.MacOS.THIEFQUEST.B-O
bcdb0ca7c51e9de4cf6c5c346fd28a4ed28e692319177c8a94c86dc676ee8e48	Virus.MacOS.THIEFQUEST.B-O

Network artifacts	WRS action
hxxp://andrewka6[.]pythonanywhere[.]com/ret[.]txt	Blocked and categorized as C&C server
167[.]71[.]237[.]219	
hxxp://lemareste[.]pythonanywhere[.]com/cfgr[.]txt	

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