

## ■ 侵入の痕跡 (Indicators of Compromise、IoC)

ファイル名	SHA-256	検出名
<i>SecureCRT.dmg</i>	1e462f8716275dbae6acb3ff4f7a95624c1afb23c5069fa42a14ed49c2588921	TrojanSpy.MacOS.ZU RU.A
<i>com.microsoft.rdc.macos</i>	5ca2fb207762e886dd3336cf1cb92c28f096a5fbb1798ea6721b7c94c1395259	TrojanSpy.MacOS.ZU RU.A
<i>iTerm.app.zip</i>	5f59ead37fa836c6329a7ba3edd4afc9a2c5fec61de4e0cdb8e8a41031ae4db0	TrojanSpy.MacOS.ZU RU.A
<i>Navicat15_cn.dmg</i>	6df91af12c87874780cc9d49e700161e1ead71ae045954adbe7633ec9e5e45ff	TrojanSpy.MacOS.ZU RU.A
<i>Navicat15_cn.dmg</i>	91541cfc0474d6c06376460759517ae94f36fca74d5ab84cf5c23d98bd33939e	TrojanSpy.MacOS.ZU RU.A
<i>SecureCRT.dmg</i>	ae0510032cd4699ef17de7ed1587918ffcd7ff7c9a77fc45f9d68effe2934132	TrojanSpy.MacOS.ZU RU.A
<i>iTerm.dmg</i>	e5126f74d430ff075d6f7edcae0c95b81a5e389bf47e4c742618a042f378a3fa	TrojanSpy.MacOS.ZU RU.A
<i>Microsoft Remote Desktop.dmg</i>	4e8287b61b0269e0d704c6d064cb584c1378e9b950539fea366ee304f695743f	TrojanSpy.MacOS.ZU RU.A
<i>libcrypto.2.dylib</i>	4aece9a7d73c1588ce9441af1df6856d8e788143cd9e53a2e9cf729e23877343	TrojanSpy.MacOS.ZU RU.A
<i>libcrypto.2.dylib</i>	4e8287b61b0269e0d704c6d064cb584c1378e9b950539fea366ee304f695743f	TrojanSpy.MacOS.ZU RU.A

<i>libcrypto.2.dylib</i>	8db4f17abc49da9dae124f5bf583d0645510765a6f7256d264c82c2b25becf8b	TrojanSpy.MacOS.ZU RU.A
<i>libcrypto.2.dylib</i>	62cae3c971ed01c61454e4c3d9a8439cddb409a8e1c5641e5c7c4ac7667cb5e5	TrojanSpy.MacOS.ZU RU.A
<i>libcrypto.2.dylib</i>	aba7c61d2c16cdae17785a38b070df57aa3009f00686881642be31a589fabe0a	TrojanSpy.MacOS.ZU RU.A
<i>libcrypto.2.dylib</i>	af2cb957387b7c4b0c5c9fa24a711988c9e8802e758622b321c9bdc5720120d2	TrojanSpy.MacOS.ZU RU.A
<i>libcrypto.2.dylib</i>	e8184e1169373e2d529f23b9842f258dddc1d24c77ced0d12b08959967dfadef	TrojanSpy.MacOS.ZU RU.A
<i>libcrypto.2.dylib</i>	2c269ff4216dc6a14fd81ffe541994531b23a1d8e0fbd75b9316a9fa0e0d5fef	TrojanSpy.MacOS.ZU RU.A
<i>g.py</i>	ffb0a802fdf054d4988d68762d9922820bdc3728f0378fcd6c4ed28c06da5cf0	TrojanSpy.Python.ZU RU.A

## 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](http://www.trendmicro.com)

