侵入の痕跡（Indicators of Compromise, IoC）

ファイル名	SHA-256	検出名
Java downloader	5210AFA4567B98FB3F8AEE513206B5FD466D3AFE01DD576A2BEE4A623F2CDAE2	Trojan.Java.QNODESERVICE.A
wizard.js (2020-04-30)	9FBAFF43A596921EFD7BB3B015A541A00633320C3DE66BE795BADA098D37F8FE	Trojan.JS.QNODESERVICE.A
qnodejs-win32-ia32.js (2020-04-30)	EB00CD731EE622EAF53BFD19A789E494872BACA156455C38CA3035B2E33CC152	Backdoor.JS.QNODESERVICE.A
qnodejs-win32-x64.js (2020-04-30)	F3C5F8EF9886DC300BCE3E6DB0B973B3408AE82EB5789C4BA72FEC27D61CA693	Backdoor.JS.QNODESERVICE.A
wizard.js (2020-05-05)	5CCED1119F4FDC175967594EC4671EF74E645D46F5F7ED1200513C7EA7DC31CF	Trojan.JS.QNODESERVICE.B
qnodejs-win32-ia32.js (2020-05-05)	76B8E43AB3E38B8635588FBD9C9A527022691962DD158A480671DDF98C7110F8	Backdoor.JS.QNODESERVICE.B

qnodejs-win32-x64.js (2020-05-05)	16376D225C3B16E6E0D50259241939DE6AD19A82668F650AACDAF173576C5003	Backdoor.JS.QNODESERVICE.B

C&C サーバ

central[.]qhub[.]qua[.]one

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