

侵入の痕跡 (Indicators of Compromises、IoCs)

モジュール名	SHA256 値	検出名
importDll32.dll	be201f8a0ba71b7ca14027d62ff0e1c4fd2b00caf135ab2b048fa9c3529f98c8	TSPY_TRICKBOT.NL
injectDll32.dll	a02593229c8e75c4bfc6983132e2250f3925786224d469cf881dbc37663c355e	TrojanSpy.Win32. TRICKBOT.TIGOCCA
mailsearcher32.dll	7f55daf593aab125cfc124a1aeeb50c78841cc2e91c8f6e6118eeae45c94549e	TrojanSpy.Win32. TRICKBOT.TIGOCCA
networkDll32.dll	c560cca7e368ba23a5e48897e2f89ed1eb2e5918a3db0b94a244734b11a009c6	TrojanSpy.Win32. TRICKBOT.TIGOCCA
psfin32.dll	f82d0b87a38792e4572b15fab574c7bf95491bf7c073124530f05cc704c1ee96	TrojanSpy.Win32. TRICKBOT.TIGOCCA
pwgrab32.dll	fe89e399b749ee9fb04ea5801a99a250560ad1a4112bbf6ef429e8e7874921f2	TrojanSpy.Win32. TRICKBOT.TIGOCCA
shareDll32.dll	7daa04b93aff93bb2ffe588a557089fad731cac7af11b07a281a2ae847536d5	TrojanSpy.Win32. TRICKBOT.TIGOCCA
systeminfo32.dll	312dec124076289d8941797ccd2652a9a0e193bba8982f9f1f9bdd31e7388c66	TrojanSpy.Win32. TRICKBOT.TIGOCCA
wormDll32.dll	55f74affe702420ab9e63469d2b6b47374f863fe06ef2ffef7045fb5cbb1079	TrojanSpy.Win32. TRICKBOT.TIGOCCA
8_81_32.vbs	11b4c8b88142e9338a3cee2464e2ac1f4caccbdf94ab0c4cf40c03b6960b35dd2	Trojan.VBS.TRICKBOT. SMDLDR
84_692_6.vbs	23b3cbf50531ff8cb4f81cc5d89e73f2b93f24bec575334bc133722fd9abb8fb	Trojan.VBS.TRICKBOT. SMDLDR
Day5Inypriv	ce46ce023e01d2afa2569962e3c0daa61f825eaa1fb5121e982f36f54bb6ab53	TrojanSpy.Win32. TRICKBOT.THDEAI

不正なサイト：

- [hxxp://mastelecomusa\[.\]com/2019/05/02/order-review/](http://hxxp://mastelecomusa[.]com/2019/05/02/order-review/)

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



©2019 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.