

## 侵入の痕跡 (Indicators of Compromises, IoCs)

日本事例 :

関連するメールと不正サイト情報

送信元アドレス (From :)	"AmazaClub" <info@amaza.club>
送信元アドレス (From :)	"AmazaClub" <support@amaza.club>
件名 (Subject :)	緊急入荷！数量限定！ マスク 使い捨て サージカルマスク レギュラー 50 枚 <省略>
不正サイト URL	hxxps://shop[.]amaza[.]club
送信元アドレス (From :)	"AU" <MARLBORO_IQOS@<文字列>.AMAZING-INIT.NET>
件名 (Subject :)	【au 会員様限定】コロナ対策補助金配布(No.g<数字列>)
不正サイト URL	hxxp://prone-elont[.]com/<文字列>
不正サイト URL	hxxp://rain-walker[.]com/log_index.php
不正サイト URL	hxxp://busy-instruct[.]net/<文字列>

海外事例：

関連するマルウェアファイルの情報

ファイル名	SHA 256	トレンドマイクロのパートナー検出名	トレンドマイクロの機械学習検出による予測検出名
CORONA VIRUS AFFECTED CREW AND VESSEL.xlsm	ab533d6ca0c2be8860a0f7bfc7820ffd 595edc63e540ff4c5991808da6a257d	Trojan.X97M.CVE201711882.T HCOOBO	N/A
CORONA VIRUS AFFECTED CREW AND VESSEL.xlsm	17161e0ab3907f637c2202a384de67fca 49171c79b1b24db7c78a4680637e3d5	Trojan.X97M.CVE201711882.T HCOOBO	Downloader.VBA.TRX.XXVBAF01FF006
CORONA VIRUS AFFECTED CREW AND VESSEL.xlsm	315e297ac510f3f2a60176f9c12cf9 2681bbad758135767ba805cdea830b9ee	Trojan.X97M.CVE201711882.T HCOOBO	Downloader.VBA.TRX.XXVBAF01FF006
CoronaVirusSafetyMeasures_.pdf.exe	c9c0180eba2a712f1aba1303b90cbf12c11 17451ce13b68715931abc437b10cd	TrojanSpy.Win32.FAREIT.UHBA ZCLIZ	Troj.Win32.TRX.XXPE50FFF034
CoronaVirusSafetyMeasures_.xls.exe	29367502e16bf1e2b788705014d0142 d8bcb7fcc6a47d56fb82d7e333454e923	TrojanSpy.Win32.FAREIT.SMTH C.hp	N/A
LIST OF CORONA VIRUS VICTIM.exe	3f40d4a0d0fe1eea58fa1c71308431b5c2c e6e381cacc7291e501f4eed57bfd2	Trojan.MSIL.AGENTTESLA.THC OCBO	N/A
POEA HEALTH ADVISORY re-2020 Novel Corona Virus.pdf.exe	3e6166a6961bc7c23d316ea9bca87d82 87a4044865c3e73064054e805ef5ca1a	Backdoor.Win32.REMCOS.USM ANEAGFG	Troj.Win32.TRX.XXPE50FFF034
POEA Advisories re-2020 Novel Corona Virus.2.pdf.exe	b78a3d21325d3db7470bf1a6d254e23d34 9531fca4d7f458b33ca93c91e61cd	Backdoor.Win32.REMCOS.USM ANEAGFE	Troj.Win32.TRX.XXPE50FFF034

関連する不正サイトの情報

Url	分類
accorona[.]com	詐欺サイト
alphacoronavirusvaccine[.]com	詐欺サイト
anticoronaproducts[.]com	詐欺サイト
beatingcorona[.]com	詐欺サイト
beatingcoronavirus[.]com	詐欺サイト
bestcorona[.]com	詐欺サイト
betacoronavirusvaccine[.]com	詐欺サイト
buycoronavirusfacemasks[.]com	詐欺サイト
byebyecoronavirus[.]com	詐欺サイト
cdc-coronavirus[.]com	詐欺サイト
combatcorona[.]com	詐欺サイト
contra-coronavirus[.]com	詐欺サイト

corona-armored[.]com	詐欺サイト
corona-crisis[.]com	詐欺サイト
corona-emergency[.]com	詐欺サイト
corona-explained[.]com	詐欺サイト
corona-iran[.]com	詐欺サイト
corona-ratgeber[.]com	詐欺サイト
coronadatabase[.]com	詐欺サイト
coronadeathpool[.]com	詐欺サイト
coronadetect[.]com	詐欺サイト
coronadetection[.]com	詐欺サイト
coronadocapitalgroup[.]com	詐欺サイト
coronadocreatives[.]com	詐欺サイト

## 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](http://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.