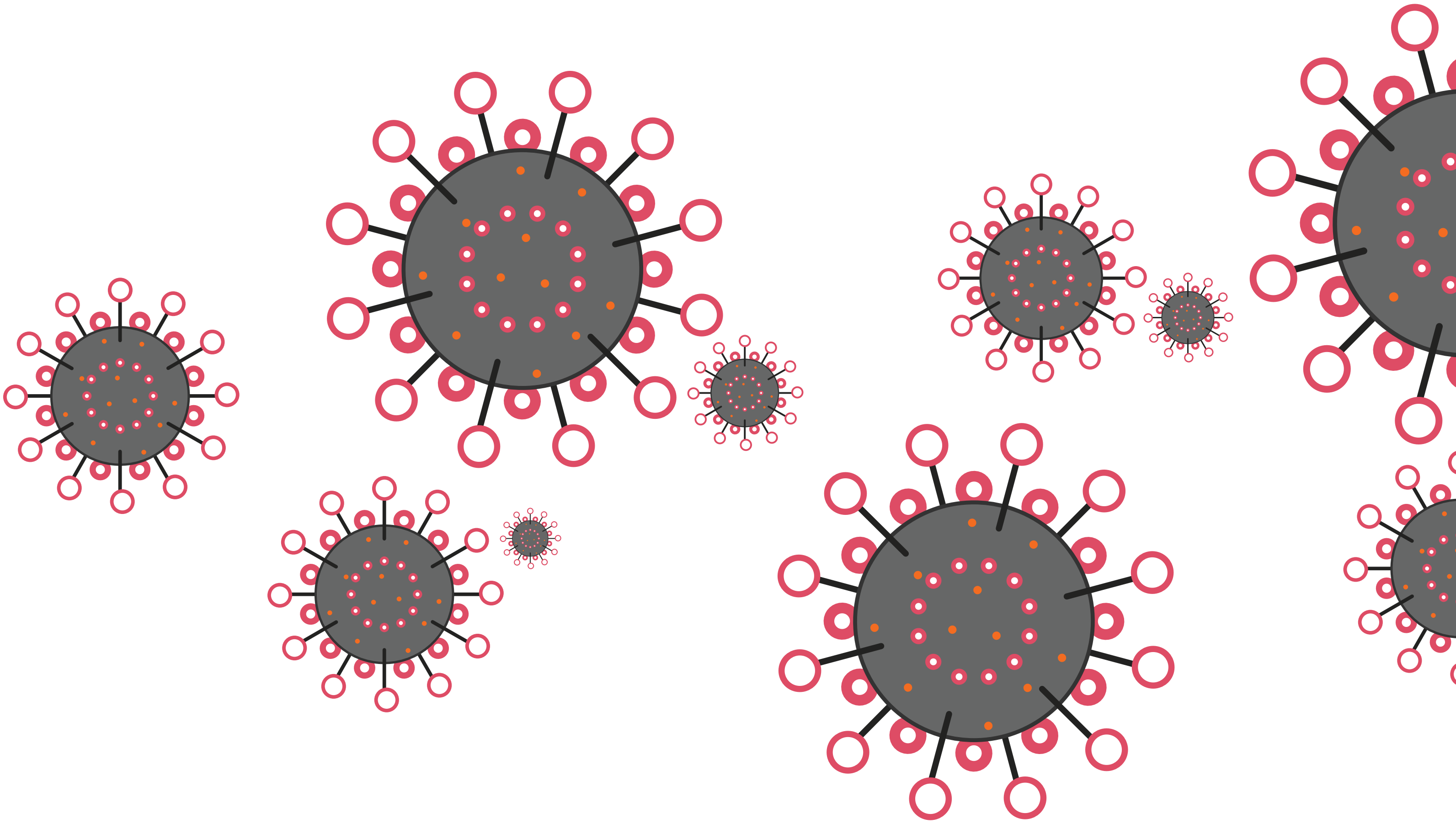
FLASH REPORT

Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide

By Insikt Group®



FR-2020-0312

Recorded Future investigated how threat actors are using the global disruptions caused by COVID-19 to further their cyber threat activities. This research is targeted toward those who hope to understand the technical cybersecurity threats that have emerged from the spread of COVID-19.

Executive Summary

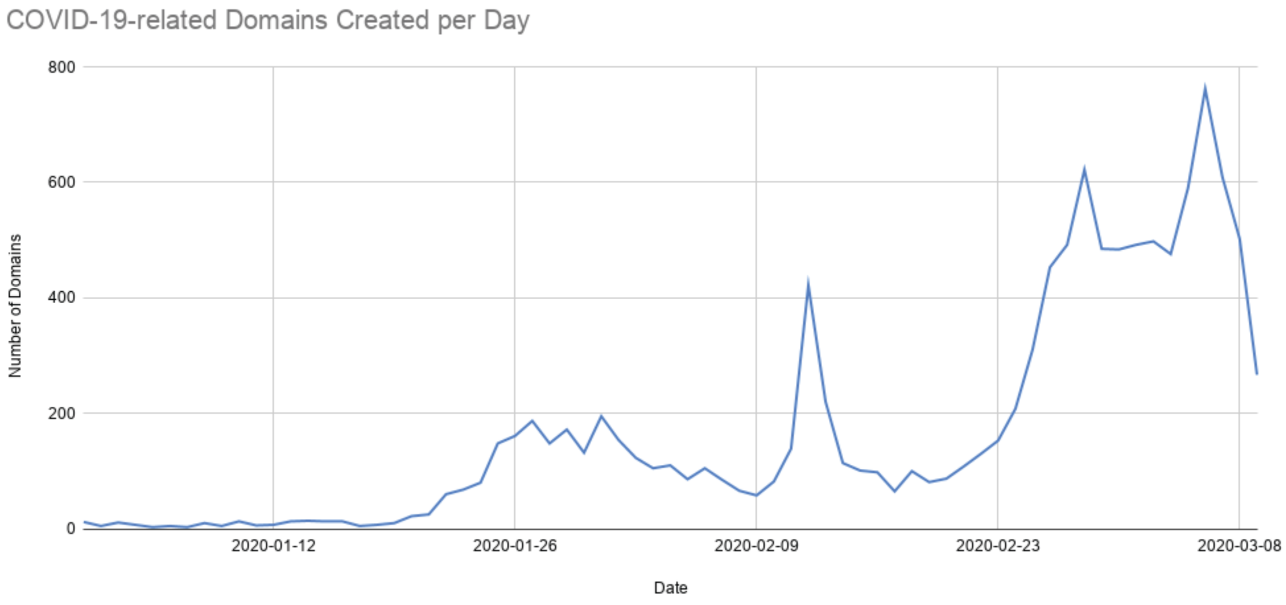
The emergence of coronavirus disease 2019 (COVID-19), the novel coronavirus that originated in late December 2019, has brought with it chaos in many different economic sectors — finance, manufacturing, and healthcare, to name a few. However, it has also originated a new cybersecurity threat, igniting a bevy of COVID-19-themed phishing lures and newly registered COVID-19-related domains. The technical threat surrounding COVID-19 primarily appears to be around phishing, with actors promising that attachments contain information about COVID-19.

Recorded Future observed an extensive list of actors and malware employing these techniques, including Trickbot, Lokibot, and Agent Tesla, targeting a broad set of victims, including those in the United States, Italy, Ukraine, and Iran in particular. Threat actors have also endeavored to gain the trust of victims using branding associated with the U.S. Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO), as well as country-specific health agencies such as the Public Health Center of the Ministry of Health of Ukraine and China's Ministry of Health, and companies such as FedEx.

Key Findings

- As of March 11, 2020, we believe that COVID-19 has been primarily used by cybercriminals as a theme for phishing lures. However, we have observed at least three cases where reference to COVID-19 has been leveraged by possible nation-state actors. We assess that as the number of COVID-19 cases, as well as publicity around the virus, rises globally, both cybercriminals and nation-state actors will increasingly exploit the crisis as a cyberattack vector.
- Cybercriminals will often use the branding of "trusted" organizations in these phishing attacks, especially the World Health Organization and U.S. Centers for Disease Control and Prevention, in order to build credibility and get users to open attachments or click on the link.

- The number of references to COVID-19 in relation to cyberattacks has increased over the last two months, including country-specific phishing lures as the virus becomes more prevalent in that country. Recorded Future assesses that, for the duration of the outbreak, COVID-19 will continue to be used as a lure, and that new versions of these lures targeting new countries will emerge.
- The number of newly registered domains related to coronavirus has increased since the outbreak has become more widespread, with threat actors creating infrastructure to support malicious campaigns referring to COVID-19. The initial spike in domain registrations coincided with a large spike in reported COVID-19 cases in mid-February — a possible indicator that attackers may have begun to realize the utility of COVID-19 as a cyberattack vector.



Graph showing the registrations of COVID-19-related domains per day in 2020. Recorded Future analysts created a query to find domain registrations of URLs containing "corona," "covid19," or "covid2019." See Appendix A for a list of these domains.

Background

According to the World Health Organization, the current coronavirus, known as Coronavirus Disease 2019 (COVID-19), was first reported from Wuhan, China on December 31, 2019. COVID-19 is a viral, respiratory disease that has spread throughout the world, causing fear and panic as the outbreak progresses.

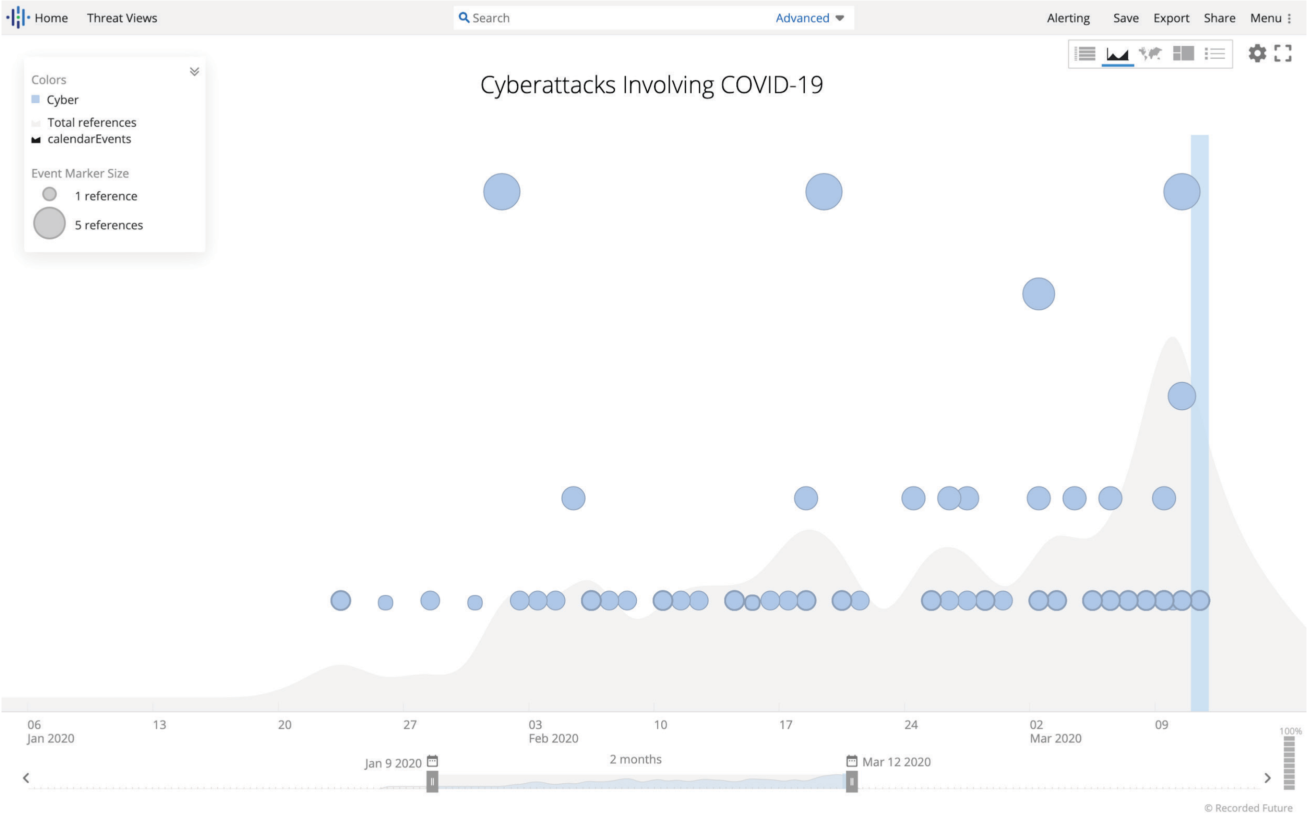
To date, over 100,000 people have been infected across the world, and over 4,000 have died. Cybercriminals and threat actors have begun to take advantage of the notoriety of the virus and the uncertainty and fear associated with it, deploying phishing campaigns that use COVID-19 as a lure to get victims to download malware or give away personal information.

Analysis

To understand the use of COVID-19 by cybercriminals and threat actors, Recorded Future correlated the number of domains created associated with "coronavirus" in 2020 with the number of references to cyberattacks or exploits involving "coronavirus" or "COVID-19."

Cyberattacks Using COVID-19

Over the last two months, Recorded Future has observed an increase in the number of instances involving COVID-19 used as an attack vector in any cyber incident, as shown in the timeline below:



Number of references to coronavirus or COVID-19 used in association with a cyber exploit or cyberattack over the past two months.

Beginning in late January 2020, the volume of data increases, with larger spikes occurring as the number of COVID-19 infections increased through the month of February. While Recorded Future has observed COVID-19 being used as part of different types of cyber incidents, it has been primarily used as a phishing lure. Using a Recorded Future query, Recorded Future identified incidents of the malicious use of COVID-19 over the last month. Where possible, we provide IOCs for these campaigns in Appendix A. The following incidents were identified:

- The AZORuIt malware was observed being delivered by phishing documents that used COVID-19 as a lure in early February 2020. Researchers at Proofpoint observed a COVID-19-themed phishing campaign targeting the manufacturing, industrial, finance, transportation, pharmaceutical, and cosmetic industries. These attacks involved emails that contained Microsoft Office document attachments designed to lure victims and exploit a Microsoft Office vulnerability, tracked as CVE-2017-11882, which allows attackers to run arbitrary code in the context of the current user. The malicious documents contained what is purported to be an advisory on the impact of the virus on the shipping industry. Once the malicious document is opened, it installs the information-stealing malware "AZORult." The AZORult strain observed in the campaign did not download ransomware, as it has done in previous attacks. According to researchers at Proofpoint, the malicious emails are originating from groups in Russia and Eastern Europe.
- In late January 2020, researchers at IBM X-Force observed cybercriminals using coronavirus as a phishing lure to distribute Emotet in a campaign primarily targeting Japan. The phishing emails claimed that the attached Microsoft Word documents contained health information and updates, but in reality contained a malicious VBA macro that installs a PowerShell script, which then downloads the Emotet trojan.

- Kaspersky published an article about phishing emails that emulated the CDC, in particular from emails containing the domains cdc-gov[.]org and cdcgov[.]org. In one instance, the URL contained within a phishing email led to a fake Microsoft Outlook login page, designed to convince victims to input their credentials. In another instance, victims were asked to donate Bitcoin to the CDC to aid in the pursuit of a vaccine.
- The security firm Cofense identified a similar, though more sophisticated, phishing campaign using the subject line "COVID-19 — Now Airborne, Increased Community Transmission" that appears to originate from the address CDC-Covid19[@]cdc[.]gov. When victims click on the embedded link, they are redirected to a Microsoft Outlook login page, and upon entering their legitimate credentials, are further redirected to a legitimate website of the CDC. While these phishing emails appear to come from a legitimate address on the CDC domain, this is due to the threat actor purposefully disguising the true origin of the email. The deception was made possible by inserting an SMTP HELO command that tells the receiving email server to treat the email as if it originated from "cdc[.]gov," despite the fact that the sender has a different domain and IP.
- Cofense also identified a phishing campaign using the subject line "Attention: List Of Companies Affected With Coronavirus March 02, 2020." that contained a malicious attachment that dropped Agent Tesla Keylogger. This attachment used the icon of a Microsoft Excel file to masquerade as a legitimate Office document and was reported to be titled "SAFETY PRECAUTIONS," with an .exe file extension.
- Phishing emails primarily targeting Italian email addresses contained malicious Microsoft Office documents with embedded VBA macros that were used to drop Trickbot. The Trickbot banking trojan can be used to steal victims' confidential information, as well as to drop additional malware. The email subject line used in this campaign was "Coronavirus: informazioni importanti su precauzioni," and to bolster the credibility of the attached lure, the supposed author was "Dr. Penelope Marchetti," an employee of the WHO in Italy.

- The security research team @issuemakerslab observed a malicious Microsoft Word document dropping the North Korean BabyShark malware that claimed to contain information on South Korea’s response to the COVID-19 virus.
- The security research team @reddrip7 identified a malicious Word document attachment called “Коронавірусна інфекція COVID-19.doc” that contained a C# backdoor. Researchers suspect this malware is related to the Hades APT. Due to the presence of the string “TrickyMouse” in the malware, the campaign has been dubbed “TrickyMouse” by the researchers. The document uses the branding and trademark of WHO and the Public Health Center of the Ministry of Health of Ukraine as a decoy and was used to target Ukraine.
- @reddrip7 also identified a COVID-19-themed phishing campaign that used a decoy document containing Nanocore RAT targeting the South Korean chemicals manufacturing company Dongwoo Fine-Chem Corporation.
- Another campaign used the FedEx trademark in a phishing attack, claiming to provide victims with information on global FedEx operations while the COVID-19 outbreak continues. It contained an attachment titled “Customer Advisory.PDF.exe” that, when opened, infected the victim with the Lokibot malware.
- Lokibot was additionally distributed in a phishing campaign that used COVID-19 as a lure, claiming to be sent by the Ministry of Health in the People’s Republic of China. The emails claimed to contain information about emergency regulations surrounding the virus with the subject line “Emergency Regulation Ordiance” (sic), and had a Windows RAR file attachment with the extension .arj. Once opened, the malicious attachment infects the victim with Lokibot, immediately contacting a malicious IP address and exfiltrating user credentials.
- The Grandoreiro banking trojan was observed being distributed via malicious sites that use the ongoing coronavirus epidemic as a lure. Twitter user @JAMESWT_MHT shared an instance of the trojan used as part of this campaign. The websites show information about the coronavirus with an embedded video player, and once the user clicks the

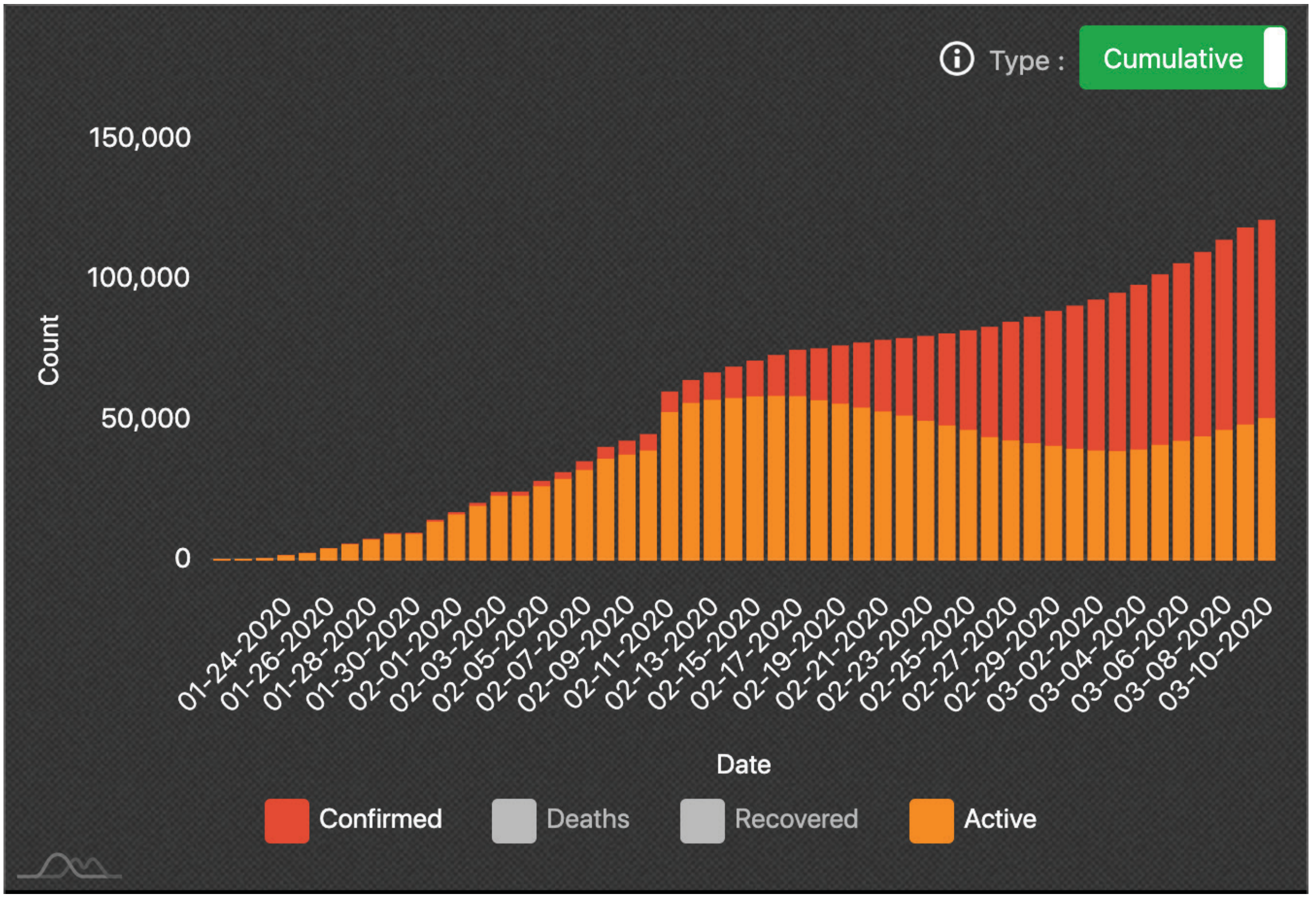
player, the Grandoreiro executable is downloaded. According to Twitter user @ESETresearch, the malware is currently targeting users in Brazil, Mexico, and Spain.

- COVID-19 was also used as a lure in what researchers suspect is a MUSTANG PANDA campaign. MUSTANG PANDA is a suspected Chinese government-linked threat actor group. The lure used in this campaign was a .rar file purportedly containing statements from Vietnamese Prime Minister Nguyen Xuan Phuc regarding COVID-19. The .rar file contains a .lnk file that when opened by the victim, executes mshta.exe via cmd.exe to run the malicious script contained in the .lnk file. While the malicious script executes, a Word document titled "Chi Thi cua thu tuong nguyen xuan phuc.doc" is displayed to the victim. Ultimately, a DLL side-loading technique is used to download and execute a malicious executable and communicate with a command-and-control server.

Coronavirus has also been weaponized as a way to spread spyware by the Iranian government. Iran's Health Ministry sent a message to victims advising them to download a specific application to monitor for potential symptoms of COVID-19. This application was, in reality, spyware. The malicious Android application, called ac19.apk, is capable of gathering victim location services and monitoring a user's physical activity (such as walking or sitting) — ostensibly to determine where the user is going and when. The application is distributed on a website created by the Iranian government, https://ac19[.]ir/.

Domain Registrations

Beginning in on January 12, the number of domain registrations started to increase, with an additional large spike on February 12, as shown in the first image, which aligns with the increase in the number of references seen in the previous image. This spike coincides with the largest single-day spike in the number of COVID-19 cases, as seen in the chart below:



Graph showing number of COVID-19 cases per day over time.

Recorded Future analysts cannot confidently establish the domain registrations in mid-February as the effect of the increase in cases during that time period. However, we assess that this correlative relationship possibly indicates that cybercriminals and other threat actors increasingly observe the relevance of the outbreak as a targeting mechanism.

Outlook

Recorded Future observed cybercriminals and other threat actors employing references to COVID-19 primarily in phishing attacks designed to obtain victims' personal information or to drop additional malware. Because these attacks prey on the fears of victims and often use a sense of urgency to get the victim to click, organizations should take the following precautions:

- Be especially wary of any email or other communications purporting to come from the CDC or WHO, even if it appears to come from a legitimate address on the official domains (cdc[.]gov and who[.]int). Many of the phishing emails used the branding and trademarks of these two organizations as part of the lure, and this trend will likely continue as the outbreak grows in the United States. Threat actors have also incorporated URLs with legitimate websites as the link text, while the underlying link is malicious. The U.S. Federal Trade Commission has suggested that interested parties visit the known WHO and CDC websites directly for up-to-date information and to be cautious about any email purporting to be from those entities. Unless your organization is in the healthcare field, it is unlikely that these agencies will be sending you emails about COVID-19. Also note that the CDC, WHO, and other organizations do not take cryptocurrency payments, so any request of this type should be considered malicious.
- While many legitimate organizations will send emails regarding precautions that they are taking to minimize the threat of COVID-19, the use of legitimate corporate branding has been used to send malware to victims. The malicious emails often use language creating a sense of urgency (though often with bad grammar or spelling), or attachments or links that are said to contain additional information rather than being informational themselves. Users should avoid opening attachments, but it is advisable to treat all emails regarding the COVID-19 outbreak with caution.

- As with all phishing attacks, it is recommended that users disable macros in Microsoft Office for any users that do not absolutely require it. Many of the malicious attachments observed by Recorded Future analysts in association with COVID-19 used VBA macros as an initial part of the infection of victims. VBA macros remain popular infection mechanisms for malicious documents that are used as phishing lures, and analysts assess with high confidence that this trend will continue.

Appendix A — Indicators of Compromise

Agent Tesla

hxxps://healing-yui223.com/cd[.]php
hxxps://www.schooluniformtrading[.]com[.]au/cdcgov/files/
hxxps://onthefx[.]com/cd[.]php
hxxps://urbanandruraldesign[.]com[.]au/cdcgov/files
hxxps://gocycle[.]com[.]au/cdcgov/files/
150[.]95[.]52[.]104
118[.]127[.]3[.]247
153[.]120[.]181[.]196
112[.]140[.]180[.]26
13[.]239[.]26[.]132
SAFETY PRECAUTIONS.rar
SAFETY PRECAUTIONS.exe
05adf4a08f16776ee0b1c271713a7880
Ef07feae7c00a550f97ed4824862c459
Postmaster[@]mallinckrodt[.]xyz
brentpaul403[@]yandex[.]ru

Emotet

8C809B4AC6D95CE85A0F04CD04B7A7EA
586FB4A6FFDFEB423F1F1782AAA9BB9F
8800EBD065B52468FA778B4527437F5A
379959D80D0BFC45AAB6437474D1F727
hxxp://109.236.109.159:8080/vnx8v
hxxp://85.96.49.152/6oU9ipBIjTSU1
hxxp://186.10.98.177/faHtH2y
hxxp://erasmus-plius.tomasjs.com/wp-admin/KfesPCcG/
hxxp://easytogets.com/xfxvqq/UXbKAbm/
hxxp://drhuzaifa.com/wp-includes/2i48k7-evv28gw-205510/
hxxp://dewarejeki.info/wp-includes/up58jauc-pum2w-630352/
hxxp://dewakartu.info/wp-includes/BRVMFYvIR/

CDC-Related

cdc-gov.org
Cdcgov.org
CDC-Covid19[@]cdc[.]gov

Trickbot

hxxps://185[.]234.73.125/wMB03o/Wx9u79.php
23[.]19.227.235
45[.]128.134.14
hxxps://45.128.134.14/C821al/vc2Tmy.php?
insiderppe[.]cloudapp.net
F21678535239.doc
F21678535350.doc
3461B78384C000E3396589280A34D871C1DE3AE266
334412202D4A6A85D02439
88eb57a3b520881b1f3fd0073491da6c50b7284dd8e
66099c172d80ba33a5032f

Lokibot

Customer Advisory.PDF.exe
906EFF4AC2F5244A59CC5E318469F2894F8CED406F
1E0E48E964F90D1FF9FD88
kbfvzoboss.bid/alien/fre.php
198.23.200[.]241
hxxp://198.23.200[.]241/~power13/.xoiaspxo/fre.php

TrickyMouse

1db31ada5f1ac2411ef337902443439 46b741cd603745257a4612c5d2e6a4052
9aea43b22f214228caf4fc714f426c0a140b7dd70b010bf3778cd1c0ec440851
1545401f661f9326f5c604e1a025e811079ba4eace9d3830a05c5e4aa666803e
62dd16724874e0b05257118fb06427a6aeb839602bce52e6a139dc379f538bed
09400e30105b10cd484a2159e8496accd779045ac6775b351b80949a54e772df
5b12f8d817b5f98eb51ef675d5f31d3d1e34bf06befba424f08a5b28ce98d45a
3b701eac4e3a73aec109120c97102c17edf88a20d1883dd5eef6db60d52b8d92
2dfb086bc73c259cac18a9cb1f9dbbc8
6c73d338ec64e0e44bd54ea61b6988b2
Коронавірусна інфекція COVID-19.rar
Коронавірусна інфекція COVID-19.doc
cloud-security.ggpht[.]ml
cloud-security.ggpht[.]ml
123.161.61[.]55
145.239.23[.]7

192.35.177[.]64

Registered Domains

These URLs were the domain registrations that occurred between January 1 2020 and March 11. We cannot confirm whether they were registered with malicious intent, only that they bear a similarity to existing COVID-19 related domains and make use of COVID-19-related terms.

coronavirusoutbreakmap[.]com
www.coronavirusoutbreakmap[.]com
corona-virus[.]healthcare
coronavirusprotectionmasks[.]org
www[.]coronavirusprotectionmasks[.]org
coronavirus[.]1point3acres[.]com
coronavirus[.]dev
wuhancoronavirus[.]blogspot[.]com
coronavirusdata[.]org
www[.]coronavirusdata[.]org
coronamap[.]live
coronamap[.]site
coronatoken[.]org
bestcoronavirusprotect[.]tk
coronavirusnigeria[.]ng4n[.]com
corona[.]yagi[.]news
info-coronavirus[.]be
www[.]info-coronavirus[.]be
coronavirusnews[.]world
coronavirus[.]app
endcoronavirus[.]org
coronavirus-reports[.]com
coronavirus-map[.]com
www[.]endcoronavirus[.]org
coronavirusreport[.]buzz
www[.]coronavirusreport[.]buzz
coronavirusupdates[.]eu
coronavirus-monitor[.]ru
coronavirus123[.]com
coronavirusstatus[.]space
coronaviruszone[.]com

coronavirusofficialnews[.]com
flashnewscoronavirus[.]blogspot[.]com
coronatracker[.]com
survivecoronavirus[.]org
corona[.]help
coronaboard-env[.]csgy3mxprm[.]eu-west-1[.]elasticbeanstalk[.]com
coronavirusinformationforus[.]blogspot[.]com
www[.]coronatracker[.]com
blogcoronacl[.]canalcero[.]digital
virus-corona[.]org
coronavirusupdates[.]online
coronavirus[.]zone
coronavirusthermometer[.]com
coronavirusawerness[.]blogspot[.]com
coronavirustoday[.]com
coronavirus[.]cc
corona-virus[.]tokyo
www[.]coronavirustoday[.]com
coronavirus-testing[.]com
stopcorona[.]org
coronavirusecuador[.]com
viruscorona[.]co[.]uk
coronastop28[.]com
coronavirusepidemia[.]blogspot[.]com
coronanow[.]kr
corona[.]kpwashingtonresearch[.]org
coronaviruses[.]com[.]au
mycoronavirus[.]world
coronavirus-in[.]space
coronawatch[.]eu
coronavirus[.]cms[.]am
www[.]coronawatch[.]eu
trackcorona[.]net
coronavirustechhandbook[.]com
coronavirus[.]tghn[.]org
coronawatch[.]now[.]sh
trackcorona[.]live
coronavirusupdate[.]tk
corona[.]kompa[.]ai
whereisthecoronavirus[.]com

thecoronaviruslive[.]info
coronastats[.]net
coronalive[.]just-shared[.]top
coronavirus19news[.]com
coronavirus[.]page
coronavirusdefense[.]com
www[.]thecoronaviruslive[.]info
coronavirusaware[.]xyz
coronavirus[.]koudaitour[.]com
coronavirusabc[.]com
www[.]trackcorona[.]live
corona-nearby[.]com
coronabye[.]com
trackcoronavirus[.]com
preventcoronaviruses[.]blogspot[.]com
www[.]coronavirusabc[.]com
vaccine-coronavirus[.]com
coronavirus-realtime[.]com
whatcoronavirus[.]com
wuhan-virus-coronavirus-advice[.]blogspot[.]com
corona[.]sums[.]ac[.]ir

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.