แจ้งเตือน :
รายงานวิเคราะห์การโจมตี Emotet Trojan

ผลกระทบทางธุรกิจ
- ☒ Financial damage
- ☒ Reputation damage
- ☐ Non-compliance
- ☒ Privacy violation

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : White
(Traffic Light Protocol)

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

รายงานวิเคราะห์การโจมตีองค์กรในประเทศไทยด้วย Phishing Email เพื่อติดตั้ง Emotet Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ

วันแจ้งเตือนที่ 15 มิถุนายน 2565

ตามที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช. สกมช.) ได้รายงานข้อมูลการตรวจพบกิจกรรมการโจมตีของ malware Emotet และ ก.ล.ต. ได้แจ้งเตือนข้อมูลดังกล่าวเมื่อวันที่ 17 พฤษภาคม 2565 นั้น

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) รายงานการวิเคราะห์การโจมตีของ malware ดังกล่าวเพิ่มเติม พบว่ามีรูปแบบและวิธีการโจมตี โดยการส่ง Phishing Email ด้วยการปลอมแปลง Email Address ของผู้ส่งเพื่อให้ดูเหมือนส่งมาจากพนักงานขององค์กรหนึ่งในประเทศไทยที่มีตัวตนจริง และทำงานในสายงานที่ติดต่อกับองค์กรเป้าหมายที่จะโจมตี โดยเบื้องต้นคาดว่าข้อมูลบุคคลที่ใช้ในการล่อลวงจะมาจากSocial Media

การโจมตีในครั้งนี้มีความเป็นไปได้สูงที่ผู้ไม่หวังดีกำหนดเป้าหมายโจมตีต่อองค์กรที่ทำหน้าที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ อย่างไรก็ดี ก.ล.ต. เล็งเห็นถึงความเสี่ยงและภัยคุกคามที่อาจจะเกิดต่อบริษัทจดทะเบียนและผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งรายงานผลการวิเคราะห์ดังกล่าวให้ทราบโดยมีรายละเอียดเอกสารรายงานผลการวิเคราะห์ด้านล่างนี้ เพื่อเป็นประโยชน์ในการตรวจสอบและติดตาม หรือต่อยอดผลการวิเคราะห์ต่อไป

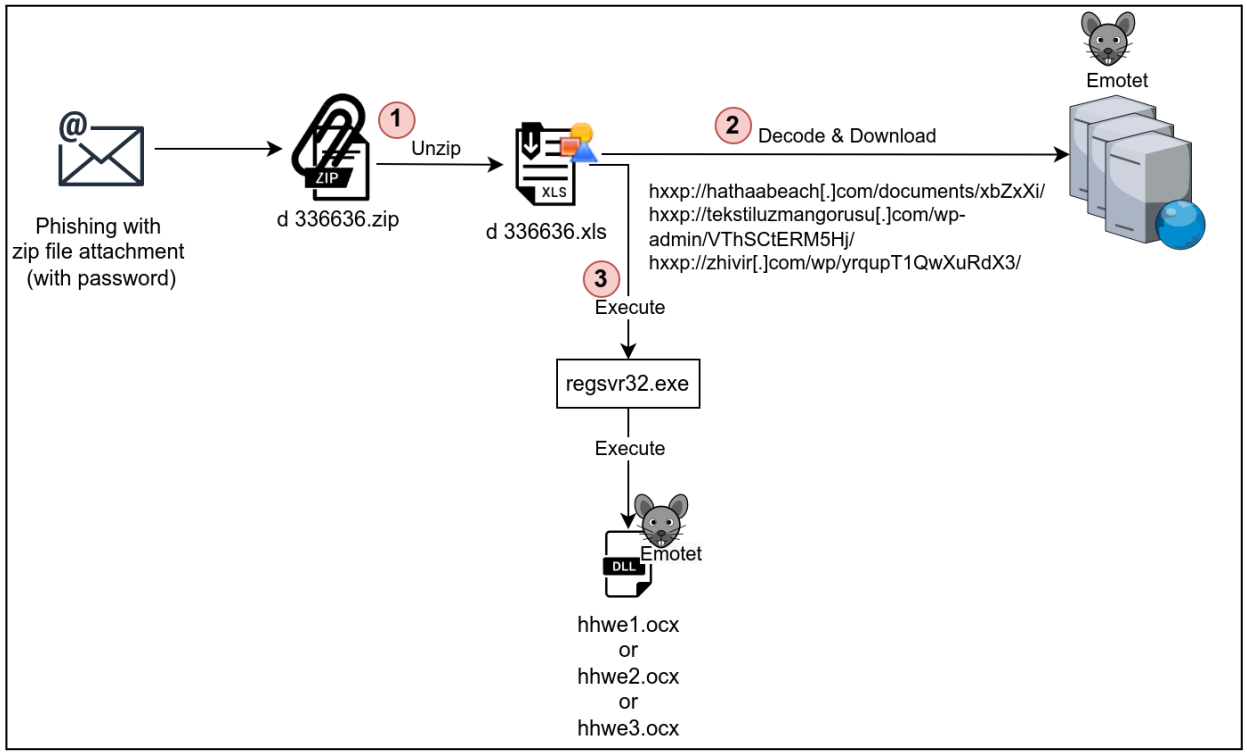
[TLP:WHITE] รายงานการวิเคราะห์แคมเปญการโจมตีองค์กรในประเทศไทยด้วยวิธี Phishing เพื่อติดตั้ง Emotet Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ

14 มิ.ย.65

Executive Summary

ศูนย์ TTC-CERT ได้รับรายงานจากองค์กรหนึ่ง พบว่ามีการส่ง Phishing Email จากผู้ไม่หวังดีให้กับพนักงานในองค์กร เพื่อติดตั้ง Emotet Trojan Epoch5 ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ

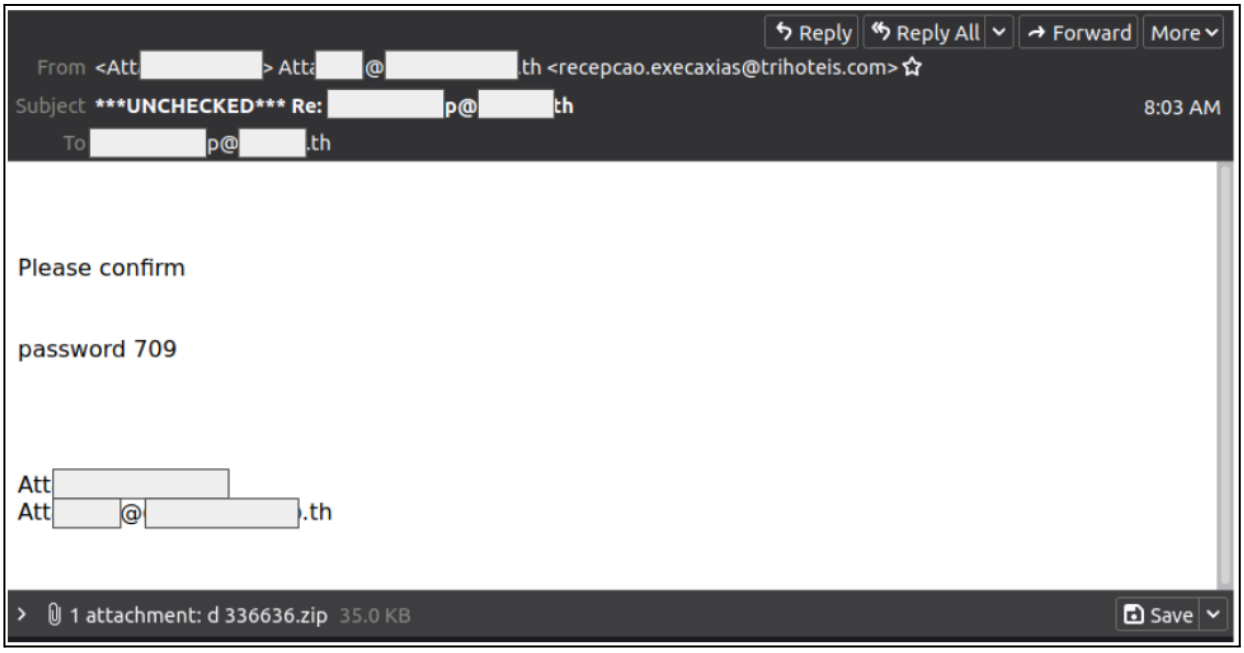
โดยการโจมตีในครั้งนี้ ผู้ไม่หวังดีใช้วิธีการโจมตีในรูปแบบที่เคยใช้ในการโจมตีตามปกติของ Emotet ด้วย การส่ง Phishing Email โดยการปลอมแปลง Email Address ของผู้ส่งเพื่อให้ดูเหมือนกับว่ามาจากผู้ส่งที่เป็นพนักงานขององค์กรหนึ่งในประเทศไทยที่มีตัวตนจริง และทำงานในสายงานที่ต่อติดต่อกับองค์กรเป้าหมายต่อการโจมตีในครั้งนี้ คาดว่าข้อมูลบุคคลที่ใช้ในการล่อลวงน่าจะมาจากการหาข้อมูลใน Social Media ในขณะที่ทำการวิเคราะห์แคมเปญนี้ ผู้เขียนพบว่าผู้ไม่หวังดีดำเนินการตามภาพรวมของแคมเปญนี้โดยสรุป ดังนี้



ศูนย์ TTC-CERT ประเมินแล้วพบว่า การโจมตีในครั้งนี้มีความเป็นไปได้ในระดับสูงที่ผู้ไม่หวังดีกำหนดเป้าหมายโจมตีต่อองค์กรเป้าหมาย โดยเฉพาะองค์กรที่ทำหน้าที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ เพื่อติดตั้ง Emotet Trojan Epoch5 ลงบนเครื่องคอมพิวเตอร์ขององค์กรเป้าหมาย

รายละเอียดทางเทคนิค

Initial Access ผู้ไม่หวังดีใช้วิธีการส่ง Phishing Email และแนบไฟล์ zip ที่มีการเข้ารหัสขนาด 35.0 KB โดยในเนื้อความของ Email จะระบุรหัสผ่านสำหรับแตกไฟล์ zip รายละเอียดตาม **ภาพที่ 1**



ภาพที่ 1 *แสดงเนื้อความใน Email ที่ใช้ในการโจมตี (Initial Access)*

เมื่อทำการตรวจสอบ Email Header พบว่า Email ต้นทางส่งมาจาก IP Address 119.93.220[.]55 (ประเทศฟิลิปปินส์) ส่งโดย recepcao.execaxias@trihoteis[.]com (recepcao execaxias เป็นภาษาโปรตุเกส แปลว่า “แผนกต้อนรับ” คาดว่า Email ของ trihoteis.com ถูก compromised) โดยได้ทำการส่งผ่านพร็อกซี่ ของ proxy.email-ssl.com.br (ประเทศบราซิล)

เมื่อทำการดาวน์โหลดไฟล์แนบจาก Email จะได้ไฟล์ชื่อ **d 336636.zip** ซึ่งการที่จะแตกไฟล์ zip นี้ เหยื่อจะต้องใช้รหัสผ่าน (709) ที่ได้จากเนื้อความใน Email มาใช้ในการแตกไฟล์ ซึ่งผู้โจมตีนิยมเลือกใช้วิธีนี้ใน การลักลอบส่งไฟล์ที่เป็นอันตรายผ่าน Emaill เข้ามาในเครือข่ายขององค์กร เนื่องจากเป็นวิธีการในการหลบเลี่ยง การตรวจจับจากจากอุปกรณ์ป้องกันเครือข่ายขององค์กรได้เป็นอย่างดี

จากนั้น ศูนย์ TTC-CERT จึงทำการแตกไฟล์ **d 336636.zip** จะพบไฟล์ Microsoft Excel ชื่อ **d 336636.xls** ศูนย์ TTC-CERTทำการตรวจสอบขั้นต้นพบว่าไฟล์ดังกล่าว มีการฝัง XLM macro (หรือ Excel 4.0 macros) ที่คาดว่าเป็นอันตราย และมีการกำหนดให้เมื่อเปิดไฟล์ Microsoft Excel ดังกล่าว จะทำการ execute XLM macro ที่เป็นอันตรายโดยอัตโนมัติ รายละเอียดอื่น ๆ ตาม **ภาพที่ 2**

```
+----------+--------------------+--------------------------------------------+
|Type      |Keyword             |Description                                 |
+----------+--------------------+--------------------------------------------+
|AutoExec  |Auto_Open           |Runs when the Excel Workbook is opened      |
|Suspicious|Windows             |May enumerate application windows (if       |
|          |                    |combined with Shell.Application object)     |
|Suspicious|Hex Strings         |Hex-encoded strings were detected, may be   |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                    |
|Hex String|'\x00\x00\x00\x00\x0|00000000000000000000                        |
|          |0\x00\x00\x00\x00\x0|                                            |
|          |0'                  |                                            |
|Suspicious|XLM macro           |XLM macro found. It may contain malicious   |
|          |                    |code                                        |
+----------+--------------------+--------------------------------------------+
```

ภาพที่ 2 *แสดงผลลัพท์บางส่วนที่ได้จากคำสั่ง olevba*

ศูนย์ TTC-CERT จึงได้ทำการ decode XLM macro และทำการวิเคราะห์ พบว่า XLM macro ถูกกำหนดให้ทำงานทันที เมื่อมีการเปิดไฟล์ Excel นี้ และจะสั่งให้เครื่องคอมพิวเตอร์ของเหยื่อไปดาวน์โหลดไฟล์เพิ่มเติมจำนวน 3 URL ดังนี้ (1) hxxp://hathaabeach[.]com/documents/xbZxXi/ (2) hxxp://tekstiluzmangorusu[.]com/wp-admin/VThSCtERM5Hj/ และ (3) hxxp://zhivir[.]com/wp/yrqupT1QwXuRdX3/ จากนั้นจะบันทึกไฟล์ที่ดาวน์โหลดมาด้วยชื่อ hhwe1.ocx, hhwe2.ocx, hhwe3.ocx และท้ายที่สุดจะสั่งให้ execute ไฟล์ที่ดาวน์โหลดมาด้วยคำสั่ง C:\Windows\System32\regsvr32.exe /S ..\hhwe1.ocx หรือ C:\Windows\System32\regsvr32.exe /S ..\hhwe2.ocx หรือ C:\Windows\System32\regsvr32.exe /S ..\hhwe3.ocx

จากนั้น ศูนย์ TTC-CERT จึงได้พยายามเข้าถึง URL ทั้ง 3 เพื่อทำการวิเคราะห์เพิ่มเติม โดยเครื่องคอมพิวเตอร์จะทำการดาวน์โหลดไฟล์ชนิด Dynamic-link library (dll) โดยชื่อไฟล์ที่ดาวน์โหลดในแต่ละครั้งจะเป็นชื่อไฟล์แบบสุ่ม รายละเอียดตามรูป **ภาพที่ 3** **ภาพที่ 4** และ **ภาพที่ 5**

```
(base) pisut@teletron:~$ proxychains wget --content-disposition http://hathaabeach.com/documents/xbZxXi/
ProxyChains-3.1 (http://proxychains.sf.net)
--2022-06-14 15:38:14--  http://hathaabeach.com/documents/xbZxXi/
Resolving hathaabeach.com (hathaabeach.com)... |DNS-request| hathaabeach.com
|R-chain|-<>-127.0.0.1:9050-<><>-4.2.2.2:53-<><>-OK
|DNS-response| hathaabeach.com is 166.62.26.11
166.62.26.11
Connecting to hathaabeach.com (hathaabeach.com)|166.62.26.11|:80... |R-chain|-<>-127.0.0.1:9050-<><>-166.
62.26.11:80-<><>-OK
connected.
HTTP request sent, awaiting response... 200 OK
Length: 374272 (366K) [application/x-msdownload]
Saving to: '958OahsIAXb11iiqW6.dll'

958OahsIAXb11iiqW6.dll     100%[===================================>] 365.50K  31.7KB/s    in 11s

2022-06-14 15:38:30 (34.6 KB/s) - '958OahsIAXb11iiqW6.dll' saved [374272/374272]
```

ภาพที่ 3 *แสดงการดาวน์โหลดไฟล์ชนิด Dynamic-link library (dll) จาก hxxp://hathaabeach[.]com/documents/xbZxXi/*

```
(base) pisut@teletron:~$ proxychains wget --content-disposition http://tekstiluzmangorusu.com/wp-admin/VT
hSCtERM5Hj/
ProxyChains-3.1 (http://proxychains.sf.net)
--2022-06-14 15:38:35--  http://tekstiluzmangorusu.com/wp-admin/VThSCtERM5Hj/
Resolving tekstiluzmangorusu.com (tekstiluzmangorusu.com)... |DNS-request| tekstiluzmangorusu.com
|R-chain|-<>-127.0.0.1:9050-<><>-4.2.2.2:53-<><>-OK
|DNS-response| tekstiluzmangorusu.com is 188.132.217.108
188.132.217.108
Connecting to tekstiluzmangorusu.com (tekstiluzmangorusu.com)|188.132.217.108|:80... |R-chain|-<>-127.0.0
.1:9050-<><>-188.132.217.108:80-<><>-OK
connected.
HTTP request sent, awaiting response... 200 OK
Length: 374272 (366K) [application/x-msdownload]
Saving to: ‘xix08oXf6jx.dll’

xix08oXf6jx.dll            100%[===================================>] 365.50K  33.8KB/s    in 18s

2022-06-14 15:38:58 (20.1 KB/s) - ‘xix08oXf6jx.dll’ saved [374272/374272]
```

ภาพที่ 4 *แสดงการดาวน์โหลดไฟล์ชนิด Dynamic-link library (dll) จาก hxxp://tekstiluzmangorusu[.]com/wp-admin/VThSCtERM5Hj/*

```
(base) pisut@teletron:~$ proxychains wget --content-disposition http://zhivir.com/wp/yrqupT1QwXuRdX3/
ProxyChains-3.1 (http://proxychains.sf.net)
--2022-06-14 15:39:07--  http://zhivir.com/wp/yrqupT1QwXuRdX3/
Resolving zhivir.com (zhivir.com)... |DNS-request| zhivir.com
|R-chain|-<>-127.0.0.1:9050-<><>-4.2.2.2:53-<><>-OK
|DNS-response| zhivir.com is 38.117.65.129
38.117.65.129
Connecting to zhivir.com (zhivir.com)|38.117.65.129|:80... |R-chain|-<>-127.0.0.1:9050-<><>-38.117.65.129
:80-<><>-OK
connected.
HTTP request sent, awaiting response... 200 OK
Length: 374272 (366K) [application/x-msdownload]
Saving to: ‘FGvBqJPZS1ogQMYmH.dll’

FGvBqJPZS1ogQMYmH.dll      100%[===================================>] 365.50K  13.5KB/s    in 19s

2022-06-14 15:39:31 (19.4 KB/s) - ‘FGvBqJPZS1ogQMYmH.dll’ saved [374272/374272]
```

ภาพที่ 5 *แสดงการดาวน์โหลดไฟล์ชนิด Dynamic-link library (dll) จาก hxxp://zhivir[.]com/wp/yrqupT1QwXuRdX3/*

ศูนย์ TTC-CERT ทำการตรวจสอบค่า SHA-1 ของทั้ง 3 ไฟล์ที่ได้ดาว์โหลดมา ตรวจพบว่าทั้ง 3 ไฟล์เป็นไฟล์ตัวเดียวกัน รายละเอียดตาม**ภาพที่ 6**

```
(base) pisut@teletron:~$ sha1sum *.dll
4c92984f9ebbfac6c40c8fd775c3a357139944c9  958OahsIAXb11iiqW6.dll
4c92984f9ebbfac6c40c8fd775c3a357139944c9  FGvBqJPZS1ogQMYmH.dll
4c92984f9ebbfac6c40c8fd775c3a357139944c9  xix08oXf6jx.dll
```

ภาพที่ 6 *แสดงผลการตรวจสอบค่า SHA-1 ของทั้ง 3 ไฟล์ ที่มีค่าเหมือนกัน*

จากนั้น ศูนย์ TTC-CERT จึงนำไฟล์ 958OahsIAXb11iiqW6.dll (ที่ดาวน์โหลมาในครั้งนี้) ไปวิเคราะห์ด้วยวิธี Dynamic Analysis พบว่าไฟล์ 958OahsIAXb11iiqW6.dll เป็น Trojan ชนิด Emotet Epoch5 โดยมีรายละเอียดของ Emotet C2 Configuration ตามที่ระบุไว้ในหัวข้อ “**Indicators of compromise (IOCs)**”

ศูนย์ TTC-CERT จึงแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง และดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศและระบบเครือข่ายขององค์กร อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในกรณีนี้ จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

MITRE ATT&CK

- **Initial Access**
  - T1566.001 Phishing: Spearphishing Attachment
- **Execution**
  - T1137.001 Office Application Startup: Office Template Macros
  - T1204.002 User Execution: Malicious File
  - T1218.010 System Binary Proxy Execution: Regsvr32
- **Privilege Escalation**
  - T1055.001 Process Injection: Dynamic-link Library Injection
- **Defense Evasion**
  - T1027 Obfuscated Files or Information
  - T1140 Deobfuscate/Decode Files or Information
  - T1027.002 Obfuscated Files or Information: Software Packing
  - T1055.001 Process Injection: Dynamic-link Library Injection
- **Command and Control**
  - T1571 Non-Standard Port

Indicators of compromise (IOCs)

- Source Email: recepcao.execaxias@trihoteis[.]com
- d 336636.zip (ไฟล์แนบ)
  - MD5: af8584a1a4bc59db332dde34f8bd052f
  - SHA-1: f150cc27306df4a67ef2c7a3e969bac96145a387

- SHA-256: b2927ac3dc006a68d0ff034beeae3d9bfa866d3c65177ed1557897d30020021b

- d 336636.xls (MalDoc)
  - MD5: 5b8818d4de62fd78fb7332710bcdab43
  - SHA-1: f71b42d8998058843ff66c76b1a7051ee5834350
  - SHA-256: 2b879cc66eca9f45e901e5eca73005a09b0e43fdb2d33dee725c64c0380a40ac
- URL ที่เก็บ Emotet Trojan (dll file)
  - hxxp://hathaabeach[.]com/documents/xbZxXi/
  - hxxp://tekstiluzmangorusu[.]com/wp-admin/VThSCtERM5Hj/
  - hxxp://zhivir[.]com/wp/yrqupT1QwXuRdX3/
- 958OahsIAXb11iiqW6.dll (Emotet Epoch5 Trojan)
  - MD5: f0c527db2c8b2564a3d95aa9218bba92
  - SHA-1: 4c92984f9ebbfac6c40c8fd775c3a357139944c9
  - SHA-256: d663f2deaac027d7a24ccc3c22ea5231de5b2b7154b34eea7edfd7b5eb439a1b
  - SSDEEP: 6144:Qc7dlejqnMo2/qUdszzI9XIMBNB79Wz97+9n+8M25jOR0z:Qc7dlemnMp/Nszs9YU9WzFt1xs
- Emotet Trojan C2
  - 175[.]126[.]176[.]79:8080
  - 188[.]225[.]32[.]231:4143
  - 64[.]227[.]55[.]231:8080
  - 87[.]106[.]97[.]83:7080
  - 167[.]86[.]75[.]145:443
  - 103[.]41[.]204[.]169:8080
  - 88[.]217[.]172[.]165:8080
  - 178[.]62[.]112[.]199:8080
  - 165[.]232[.]185[.]110:8080
  - 54[.]37[.]228[.]122:443
  - 202[.]29[.]239[.]162:443
  - 37[.]44[.]244[.]177:8080

- 139[.]196[.]72[.]155:8080
- 157[.]245[.]111[.]0:8080
- 36[.]67[.]23[.]59:443
- 190[.]145[.]8[.]4:443
- 103[.]254[.]12[.]236:7080
- 202[.]134[.]4[.]210:7080
- 190[.]107[.]19[.]179:443
- 165[.]22[.]254[.]236:8080
- 198[.]199[.]70[.]22:8080
- 118[.]98[.]72[.]86:443
- 78[.]47[.]204[.]80:443
- 85[.]25[.]120[.]45:8080
- 128[.]199[.]242[.]164:8080
- 116[.]124[.]128[.]206:8080
- 195[.]77[.]239[.]39:8080
- 54[.]37[.]106[.]167:8080
- 46[.]101[.]98[.]60:8080
- 103[.]71[.]99[.]57:8080
- 93[.]104[.]209[.]107:8080
- 210[.]57[.]209[.]142:8080
- 103[.]56[.]149[.]105:8080
- 103[.]224[.]241[.]74:8080
- 103[.]126[.]216[.]86:443
- 85[.]214[.]67[.]203:8080
- 103[.]85[.]95[.]4:8080
- 104[.]248[.]225[.]227:8080
- 157[.]230[.]99[.]206:8080
- 196[.]44[.]98[.]190:8080
- 37[.]187[.]114[.]15:8080
- 68[.]183[.]91[.]111:8080
- 62[.]171[.]178[.]147:8080
- 128[.]199[.]217[.]206:443

- 104[.]244[.]79[.]94:443
- 202[.]28[.]34[.]99:8080