一、IPInfo数据

1.1 去中心化messagers的IP地址所属大陆：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Matrix | Berty | Jami | Status |
| NA | 13158 | 5093 | 512 | 17 |
| EU | 21274 | 7848 | 1676 | 207 |
| AS | 1201 | 3409 | 420 | 121 |
| OC | 574 | 139 | 208 | 0 |
| AF | 39 | 335 | 52 | 2 |
| SA | 142 | 149 | 97 | 1 |

1.2 去中心化messagers的IP地址所属国家和城市数量：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Matrix | Berty | Jami | Status |
| # Country | 91 | 96 | 98 | 26 |
| # City | 3306 | 2024 | 1103 | 79 |

去中心化messagers的IP地址所属国家的top-10：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Matrix | Berty | Jami | Status |
| 1 | ('United States', 12068) | ('United States', 4778) | ('United States', 341) | ('Germany', 156) |
| 2 | ('Germany', 10404) | ('Russia', 2879) | ('Russia', 256) | ('Indonesia', 64) |
| 3 | ('France', 2488) | ('Germany', 1999) | ('France', 255) | ('Hong Kong', 30) |
| 4 | ('Netherlands', 1724) | ('United Kingdom', 855) | ('Germany', 249) | ('United States', 17) |
| 5 | ('United Kingdom', 1149) | ('China', 797) | ('Australia', 186) | ('Netherlands', 17) |
| 6 | ('Finland', 1091) | ('South Korea', 641) | ('Canada', 133) | ('Russia', 10) |
| 7 | ('Canada', 1057) | ('Japan', 484) | ('China', 131) | ('United Kingdom', 9) |
| 8 | ('Russia', 602) | ('Singapore', 421) | ('Italy', 121) | ('India', 6) |
| 9 | ('Switzerland', 568) | ('France', 414) | ('United Kingdom', 116) | ('Singapore', 6) |
| 10 | ('Australia', 498) | ('Hong Kong', 359) | ('India', 104) | ('China', 5) |

1.3 去中心化messagers的IP地址所属IPv4 Prefix (/8, /16, /24)：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Matrix | Berty | Jami | Status |
| # /8 | 202 | 207 | 188 | 75 |
| # /16 | 7688 | 4878 | 1842 | 158 |
| # /24 | 25769 | 13424 | 2473 | 251 |

前三位去中心化messagers的IP地址所属IPv4 Prefix (/8, /16, /24)：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Matrix | Berty | Jami | Status |
| # /8 | ('104/8', 3146), ('172/8', 2100), ('185/8', 1039) | ('45/8', 750), ('95/8', 575), ('178/8', 394) | ('132/8', 124), ('176/8', 87), ('37/8', 84) | ('91/8', 31), ('193/8', 24), ('182/8', 23) |
| # /16 | ('172.67', 1729), ('104.21', 1629), ('104.27', 305) | ('149.28', 185), ('45.32', 181), ('45.76', 160) | ('132.234', 124), ('213.87', 27), ('176.59', 25) | ('91.108', 27), ('193.233', 18), ('94.141', 16) |
| # /24 | ('192.64.119', 112), (162.255.119, 105), ('185.26.156', 82) | ('193.223.242', 55), ('193.8.130', 52), ('116.163.20', 27) | ('132.234.228', 62), ('132.234.229', 62), ('45.187.51', 16) | ('91.108.227', 9), ('164.138.14', 8), ('91.108.247', 7) |

Todo: 分析这些/24 IP的归属组织

1.4 去中心化messagers的IP地址所对应的hostname数量：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Matrix | Berty | Jami | Status |
| # hostname | 24275 | 11838 | 1946 | 6 |
| Most common | nobody.yourvserver.net  (100) | dedicated.vsys.host | rs.as51430.net | contaboserver.net |

1.5 去中心化messagers的IP地址所对应的AS数量：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Matrix | Berty | Jami | Status |
| # AS | 2477 | 1207 | 764 | 70 |
| Most common | ('AS13335 Cloudflare, Inc.', 4523), ('AS24940 Hetzner Online GmbH', 4278), ('AS14061 DigitalOcean, LLC', 2152) | ('AS20473 The Constant Company, LLC', 2260), ('AS12389 PJSC Rostelecom', 1681), ('AS51167 Contabo GmbH', 1346) | ('AS7575 Australian Academic and Research Network (AARNet)', 124), ('AS3320 Deutsche Telekom AG', 85), ('AS212238 Datacamp Limited', 79) | ('AS215590 DpkgSoft International Limited', 133), ('AS132203 Tencent Building, Kejizhongyi Avenue', 35), ('AS23693 PT. Telekomunikasi Selular', 23) |

1.5 去中心化messagers的IP地址所对应的ISP数量：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Matrix | Berty | Jami | Status |
| # ISP | 3244 | 1603 | 922 | 85 |
| Most common | ('Cloudflare, Inc.', 4367), ('Hetzner Online GmbH', 4179), ('DigitalOcean, LLC', 2054), ('OVH SAS', 1444), ('netcup GmbH', 1235), ('Oracle Corporation', 752), ('Akamai Technologies, Inc.', 746), ('Contabo GmbH', 645), ('Deutsche Telekom AG', 636), ('Amazon.com, Inc.', 604) | ('The Constant Company', 1405), ('Contabo GmbH', 1163), ('Amazon.com, Inc.', 654), ('Hetzner Online GmbH', 532), ('HostPapa', 517), ('The Constant Company, LLC', 450), ('Nubes, LLC', 429), ('Chinanet', 395), ('Rostelecom networks', 382), ('DigitalOcean, LLC', 340) | ('Australian Academic and Research Network', 118), ('Datacamp Limited', 79), ('Deutsche Telekom AG', 70), ('Reliance Jio Infocomm Limited', 39), ('Free Mobile SAS', 33), ('Chinanet', 30), ('AT&T Services, Inc.', 29), ('INFOSTRADA', 29), ('Mobile TeleSystems', 27), ('Vodafone', 26) | ('DpkgSoft International Limited', 128), ('PT Telekomunikasi Selular Indonesia', 23), ('PT. TELKOM INDONESIA', 18), ('Play2go International Limited', 16), ('Shenzhen Tencent Computer Systems Company Limited', 12), ('DigitalOcean, LLC', 10), ('Aceville Pte.ltd', 10), ('Alibaba (US) Technology Co., Ltd.', 7), ('Tencent Cloud Computing (Beijing) Co', 6), ('ComsenzNet', 5) |

1.6 去中心化messagers的IPv6的挖掘：

1.7 单个IP地址对应多个去中心化messagers：

至少在任意两组中共同存在的IP: 34。注：不算多，也就是说，绝不大部分的节点IP并不交互，即，不存在一个IP作为多个节点的server IP。

二、Shodan数据

2.1

三、VirusTotal数据

3.1 去中心化messagers的Malicious IP地址数量：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Matrix | Berty | Jami | Status |
| # Malicious | 2255 | 822 | 345 | 28 |

3.2 去中心化messagers的IP地址中Malicious标签最多的IP地址：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # Malicious | Matrix | Berty | Jami | Status |
| 1 | ('209.141.59.9', 18) | ('192.3.3.160', 14) | ('213.152.161.10', 10) | ('207.244.199.140', 11) |
| 2 | ('198.54.117.197', 13) | ('154.53.58.35', 12) | ('103.12.42.245', 8) | ('45.133.251.34', 4) |
| 3 | ('91.207.102.163', 13) | ('213.152.186.168', 12) | ('149.40.62.54', 7) | ('146.70.194.107', 3) |
| 4 | ('141.8.226.58', 12) | ('107.172.90.243', 11) | ('146.70.137.90', 6) | ('87.120.186.78', 3) |
| 5 | ('198.54.117.199', 12) | ('87.121.79.75', 11) | ('5.182.110.143', 6) | ('103.175.157.64', 2) |
| 6 | ('107.167.244.67', 11) | ('213.152.187.200', 10) | ('95.173.222.46', 6) | ('147.45.66.5', 2) |
| 7 | ('142.93.68.220', 11) | ('123.112.153.8', 9) | ('138.199.15.170', 5) | ('193.148.16.60', 2), |
| 8 | ('144.91.110.55', 11) | ('123.112.165.80', 9) | ('156.146.56.133', 5) | ('43.134.229.98', 2) |
| 9 | ('173.212.224.110', 11) | ('123.112.172.41', 9) | ('185.90.60.215', 5) | ('45.83.220.212', 2) |
| 10 | ('193.218.118.148', 11) | ('164.92.91.179', 9) | ('212.83.165.160', 5) | ('87.120.84.219', 2) |

Todo：对这些恶意IP地址进行重点分析，人工分析

类型：botnet\_cc、

Malware：Mirai、Venom RAT

3.3 去中心化messagers的IP地址的communicating\_files：

3.3.1 communicating\_files所属于的popular\_threat\_classification以及label：

3.3.1 communicating\_files所属于的文件类型type\_description：

3.4 去中心化messagers的IP地址的referrer\_files：