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 |

总共的节点IP数：Matrix（36393）、Berty（29818）、Jami（12332）、Status（1190）。

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 |
| 1 | ('AS13335 Cloudflare, Inc.', 4523), 69 | ('AS20473 The Constant Company, LLC', 2260) | ('AS7575 Australian Academic and Research Network (AARNet)', 124), | ('AS215590 DpkgSoft International Limited', 133), |
| 2 | ('AS24940 Hetzner Online GmbH', 4278), 668 | ('AS12389 PJSC Rostelecom', 1681), | ('AS3320 Deutsche Telekom AG', 85), | ('AS132203 Tencent Building, Kejizhongyi Avenue', 35), |
| 3 | ('AS14061 DigitalOcean, LLC', 2152), 5641 | ('AS51167 Contabo GmbH', 1346) | ('AS212238 Datacamp Limited', 79) | ('AS23693 PT. Telekomunikasi Selular', 23) |

AS Rank：https://asrank.caida.org/

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 不同平台的节点开放的端口分布

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ports | Matrix | Berty | Jami | Status |
| 1 | (80, 17315) | (22, 6733) | (443, 103) | (22, 182) |
| 2 | (443, 16682) | (80, 2060) | (80, 82) | (3000, 176) |
| 3 | (22, 9402) | (4001, 1940) | (8443, 41) | (8080, 41) |
| 4 | (8080, 4414) | (443, 1276) | (22, 38) | (8545, 32) |
| 5 | (8443, 4233) | (5443, 870) | (7547, 22) | (53, 30) |
| 6 | (2087, 3886) | (5080, 868) | (8080, 20) | (30303, 29) |
| 7 | (8880, 3823) | (8080, 699) | (7443, 19) | (80, 28) |
| 8 | (2083, 3807) | (5001, 347) | (8089, 19) | (1234, 25) |
| 9 | (2082, 3787) | (7547, 210) | (4000, 19) | (3001, 20) |
| 10 | (2086, 3763) | (9000, 170) | (1701, 17) | (443, 15) |

Matrix网络的节点开放了4023种不同的端口，Berty网络的节点开放了1419种不同的端口，Jami网络的节点开放了1539种不同的端口，Status网络的节点开放了79种不同的端口。

2.2 不同平台的节点IP属于哪类tag（cdn、cloud等）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tags | Matrix | Berty | Jami | Status |
| 1 | ('self-signed', 4383) | ('cloud', 2727) | ('self-signed', 39) | ('cloud', 18) |
| 2 | ('cloud', 4133) | ('eol-product', 759) | ('vpn', 38) | ('eol-product', 13) |
| 3 | ('starttls', 4019) | ('self-signed', 455) | ('eol-product', 17) | ('cryptocurrency', 8) |
| 4 | ('cdn', 3788) | ('database', 165) | ('starttls', 12) | ('vpn', 5) |
| 5 | ('eol-product', 3484) | ('starttls', 156) | ('cloud', 8) | ('compromised', 4) |
| 6 | ('database', 874) | ('cryptocurrency', 77) | ('iot', 4) | ('database', 4) |
| 7 | ('videogame', 255) | ('vpn', 63) | ('database', 4) | ('self-signed', 2) |
| 8 | ('vpn', 235) | ('proxy', 63) | ('videogame', 2) | ('eol-os', 1) |
| 9 | ('devops', 149) | ('iot', 37), | ('eol-os', 1) | - |
| 10 | ('open-dir', 76) | ('devops', 36) |  | - |

在Matrix系统的节点IP资产中，发现了('cryptocurrency', 17), ('honeypot', 11)，在Berty则是发现了('honeypot', 26)

2.3 不同平台的节点IP属于哪些domain和hostname（可以弄成wordmap图）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Domains | Matrix | Berty | Jami | Status |
| 1 | ('your-server.de', 1997) | ('vultrusercontent.com', 2128) | ('datapacket.com', 15) | ('status.im', 11) |
| 2 | ('vultrusercontent.com', 448) | ('contaboserver.net', 1767) | ('btcentralplus.com', 14) | ('contaboserver.net', 4) |
| 3 | ('linodeusercontent.com', 412) | ('your-server.de', 471) | ('t-ipconnect.de', 13) | ('pbiaas.com', 2) |
| 4 | ('contaboserver.net', 398) | ('colocrossing.com', 423) | ('proxad.net', 11) | ('spacecore.network', 1) |
| 5 | ('yunohost.org', 336) | ('amazonaws.com', 265) | ('versanet.de', 6) | ('starnet.md', 1) |
| 6 | ('amazonaws.com', 284) | ('163data.com.cn', 108) | ('jami.net', 6) | - |
| 7 | ('ovh.net', 223) | ('linodeusercontent.com', 95) | ('frontiernet.net', 5) | - |
| 8 | ('t-ipconnect.de', 218) | ('googleusercontent.com', 90) | ('telecomitalia.it', 5) | - |
| 9 | ('googleusercontent.com', 138) | ('netvigator.com', 84) | ('penbasics.com', 4) | - |
| 10 | ('linode.com', 128) | ('multacom.com', 67) | ('zen.co.uk', 4) | - |

在Matrix系统的节点IP资产中，发现了17862个domains，在Berty则是发现了1705个，在Jami中发现了209个，在Status发现了19个。

Hostnames:

Matrix: ('www.yunohost.org', 336), ('ns.yunohost.org', 336), ('yunohost.org', 336), ('xmpp-upload.yunohost.org', 234), ('uberspace.de', 111), ('cloudwaysapps.com', 57), ('kasserver.com', 45), ('wpmudev.host', 31), ('myfritz.box', 29), ('www.myfritz.box', 29)

Berty: ('router.asus.com', 19), ('www.asusrepeater.com', 7), ('www.asusrouter.com', 7), ('www.asusswitch.com', 7), ('ap.asus.com', 7), ('expertwifi.net', 7), ('asusrouter.com', 7), ('asusap.net', 7), ('asusswitch.com', 7), ('asusswitch.net', 7)

Jami: ('fritz.box', 3), ('myfritz.box', 3), ('www.myfritz.box', 3), ('www.fritz.box', 3), ('www.yunohost.org', 3), ('ns.yunohost.org', 3), ('yunohost.org', 3), ('rs.as51430.net', 3), ('xmpp-upload.yunohost.org', 2), ('rad1o.cn', 1)

Status: ('boot-01.do-ams3.status.staging.status.im', 1), ('boot-01.do-ams3.shards.staging.status.im', 1), ('store-02.do-ams3.shards.test.status.im', 1), ('store-02.do-ams3.status.prod.status.im', 1), ('store-01.do-ams3.status.prod.status.im', 1), ('store-01.do-ams3.shards.test.status.im', 1), ('boot-01.do-ams3.status.prod.status.im', 1), ('boot-01.do-ams3.shards.test.status.im', 1), ('252725.vm.spacecore.network', 1), ('vmi2074400.contaboserver.net', 1)

Todo：是否存在恶意的hostnames/domains？

2.4 不同平台的节点IP关联了哪些products

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Products | Matrix | Berty | Jami | Status |
| 1 | ('nginx', 19066) | ('OpenSSH', 6844) | ('nginx', 62) | ('OpenSSH', 185) |
| 2 | ('OpenSSH', 10653) | ('nginx', 2108) | ('OpenSSH', 50) | ('Grafana (Open Source)', 176) |
| 3 | ('CloudFlare', 10628) | ('Apache httpd', 332) | ('Apache httpd', 35) | ('nginx', 26) |
| 4 | ('Apache httpd', 4175) | ('Prometheus Node Exporter', 149) | ('PPTP', 16) | ('Redis key-value store', 15) |
| 5 | ('Postfix smtpd', 2671) | ('Postfix smtpd', 115) | ('MikroTik bandwidth-test server', 11) | ('MikroTik', 8) |
| 6 | ('Socks4A', 822) | ('Remote Desktop Protocol', 89) | ('MikroTik Winbox', 8) | ('Apache httpd', 8) |
| 7 | ('Exim smtpd', 681) | ('OpenResty', 74) | ('Postfix smtpd', 7) | ('Remote Desktop Protocol', 7) |
| 8 | ('OpenResty', 567) | ('Plex Media Server', 62) | ('MikroTik', 6) | ('MikroTik bandwidth-test server', 6) |
| 9 | ('Mumble Server', 407) | ('MySQL', 61) | ('OpenResty', 4) | ('anvil', 6) |
| 10 | ('MariaDB', 316) | ('Redis key-value store', 58) | ('Plex Media Server', 4) | ('PPTP', 5) |

Todo: 是否存在恶意的或者特殊的产品？

2.5 不同平台的节点IP具有远程ssh，采用的哪些安全防御策略，如cipher\_method、mac\_algorithms、server\_host\_key\_algorithms、encryption\_algorithms，等

ssh\_mac\_algorithms in Matrix: ('hmac-sha2-256-etm@openssh.com', 10586), ('hmac-sha2-512-etm@openssh.com', 10411), ('umac-128-etm@openssh.com', 10275), ('hmac-sha2-256', 10213), ('hmac-sha2-512', 10001), ('umac-128@openssh.com', 9582), ('hmac-sha1', 9527), ('hmac-sha1-etm@openssh.com', 9169), ('umac-64@openssh.com', 8734), ('umac-64-etm@openssh.com', 8653)

ssh\_mac\_algorithms in Berty: ('hmac-sha2-256', 6842), ('hmac-sha2-256-etm@openssh.com', 6836), ('hmac-sha2-512-etm@openssh.com', 6831), ('umac-128-etm@openssh.com', 6822), ('hmac-sha2-512', 6819), ('hmac-sha1', 6814), ('umac-128@openssh.com', 6798), ('hmac-sha1-etm@openssh.com', 6773), ('umac-64@openssh.com', 6741), ('umac-64-etm@openssh.com', 6735)

ssh\_mac\_algorithms in Jami: ('hmac-sha2-256', 50), ('hmac-sha2-512', 49), ('hmac-sha2-256-etm@openssh.com', 48), ('hmac-sha2-512-etm@openssh.com', 48), ('umac-128-etm@openssh.com', 47), ('umac-128@openssh.com', 46), ('hmac-sha1', 46), ('hmac-sha1-etm@openssh.com', 43), ('umac-64@openssh.com', 43), ('umac-64-etm@openssh.com', 42)

ssh\_mac\_algorithms in Status: ('umac-64-etm@openssh.com', 184), ('umac-128-etm@openssh.com', 184), ('hmac-sha2-256-etm@openssh.com', 184), ('hmac-sha2-512-etm@openssh.com', 184), ('hmac-sha1-etm@openssh.com', 184), ('umac-64@openssh.com', 184), ('umac-128@openssh.com', 184), ('hmac-sha2-256', 184), ('hmac-sha2-512', 184), ('hmac-sha1', 184)

ssh\_encryption\_algorithms in Matrix: ('aes256-ctr', 10943), ('aes128-ctr', 10909), ('aes128-gcm@openssh.com', 10698), ('aes256-gcm@openssh.com', 10689), ('chacha20-poly1305@openssh.com', 10503), ('aes192-ctr', 10224), ('aes128-cbc', 623), ('aes256-cbc', 616), ('3des-cbc', 364), ('aes192-cbc', 361)

ssh\_encryption\_algorithms in Berty: ('aes256-ctr', 6876), ('aes128-ctr', 6871), ('chacha20-poly1305@openssh.com', 6843), ('aes256-gcm@openssh.com', 6837), ('aes128-gcm@openssh.com', 6836), ('aes192-ctr', 6808), ('aes128-cbc', 67), ('aes256-cbc', 66), ('3des-cbc', 52), ('aes192-cbc', 46)

ssh\_encryption\_algorithms in Jami: ('aes256-ctr', 51), ('aes128-ctr', 50), ('chacha20-poly1305@openssh.com', 49), ('aes256-gcm@openssh.com', 49), ('aes192-ctr', 48), ('aes128-gcm@openssh.com', 48), ('aes256-cbc', 3), ('aes128-cbc', 3), ('3des-cbc', 2), ('aes192-cbc', 2)

ssh\_encryption\_algorithms in Status: ('chacha20-poly1305@openssh.com', 184), ('aes128-ctr', 184), ('aes192-ctr', 184), ('aes256-ctr', 184), ('aes128-gcm@openssh.com', 184), ('aes256-gcm@openssh.com', 184)

2.6 不同平台的节点IP的SSL，采用的哪些安全防御策略，如sig\_alg，等

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Products | Matrix | Berty | Jami | Status |
| 1 | ('sha256WithRSAEncryption', 23540) | ('sha256WithRSAEncryption', 1579) | ('sha256WithRSAEncryption', 100) | ('sha256WithRSAEncryption', 33) |
| 2 | ('ecdsa-with-SHA384', 6828) | ('ecdsa-with-SHA384', 466) | ('ecdsa-with-SHA384', 34) | ('ecdsa-with-SHA384', 15) |
| 3 | ('ecdsa-with-SHA256', 3966) | ('ecdsa-with-SHA256', 88) | ('sha512WithRSAEncryption', 13) | ('sha1WithRSAEncryption', 1) |
| 4 | ('sha1WithRSAEncryption', 318) | ('sha1WithRSAEncryption', 23) | ('sha1WithRSAEncryption', 9) |  |
| 5 | ('sha384WithRSAEncryption', 226) | ('sha384WithRSAEncryption', 16) | ('ecdsa-with-SHA256', 6) |  |
| 6 | ('sha512WithRSAEncryption', 43) | ('sha512WithRSAEncryption', 15) | - |  |
| 7 | ('md5WithRSAEncryption', 15) | ('md5WithRSAEncryption', 4) | - |  |
| 8 | ('ecdsa-with-SHA512', 9) | ('ED25519', 2) | - |  |
| 9 | ('ED448', 4) | - | - |  |
| 10 | ('ED25519', 4) | - | - |  |

Todo：哪些是不安全的加密算法？

2.7 不同平台的节点IP的Cloud Provider

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Matrix | Berty | Jami | Status |
| 1 | ('Google', 11629) | ('Vultr', 3342) | ('DigitalOcean', 11) | ('DigitalOcean', 65) |
| 2 | ('DigitalOcean', 8356) | ('Amazon', 1119) | ('Vultr', 4) | ('Alibaba Cloud', 31) |
| 3 | ('Linode', 6513) | ('DigitalOcean', 927) | ('Tencent Cloud', 2) | ('Vultr', 18) |
| 4 | ('Vultr', 5685) | ('Google', 251) | ('Amazon', 2) | ('Linode', 3) |
| 5 | ('Oracle Cloud Infrastructure', 1775) | ('Linode', 247) |  | ('Amazon', 2) |
| 6 | ('Amazon', 765) | ('Oracle Cloud Infrastructure', 118) |  |  |
| 7 | ('Azure', 187) | ('Azure', 90) |  |  |
| 8 | ('Alibaba Cloud', 68) | ('Alibaba Cloud', 40) |  |  |
| 9 | ('Tencent Cloud', 32) | ('Tencent Cloud', 21) |  |  |
|  | ('Rackspace', 20) |  |  |  |

2.8 不同平台的节点IP资产都存在哪些漏洞（vulns），存在这些漏洞的节点都是采用的哪些防御策略？

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Matrix | Berty | Jami | Status |
| 1 | ('CVE-2023-44487', 1862) | ('CVE-2023-44487', 584) | ('CVE-2013-4365', 70) | ('CVE-2013-4365', 16) |
| 2 | ('CVE-2025-26465', 1819) | ('CVE-2021-3618', 531) | ('CVE-2012-3526', 70) | ('CVE-2012-3526', 16) |
|  | ('CVE-2021-3618', 1785) | ('CVE-2021-23017', 516) | ('CVE-2009-0796', 70) | ('CVE-2024-38476', 16) |
| 4 | ('CVE-2021-23017', 1694) | ('CVE-2013-4365', 204) | ('CVE-2012-4001', 70) | ('CVE-2024-38477', 16) |
| 5 | ('CVE-2013-4365', 1472) | ('CVE-2012-3526', 204) | ('CVE-2011-1176', 70) | ('CVE-2009-0796', 16) |
| 6 | ('CVE-2012-3526', 1472) | ('CVE-2009-0796', 204) | ('CVE-2011-2688', 70) | ('CVE-2012-4001', 16) |
| 7 | ('CVE-2009-0796', 1472) | ('CVE-2012-4001', 204) | ('CVE-2013-2765', 70) | ('CVE-2012-4360', 16) |
| 8 | ('CVE-2012-4001', 1472) | ('CVE-2012-4360', 204) | ('CVE-2007-4723', 70) | ('CVE-2011-1176', 16) |
| 9 | ('CVE-2012-4360', 1472) | ('CVE-2011-1176', 204) | ('CVE-2013-0941', 70) | ('CVE-2024-40898', 16) |
| 10 | ('CVE-2011-1176', 1472) | ('CVE-2011-2688', 204) | ('CVE-2012-4360', 70) | ('CVE-2011-2688', 16) |

Todo：分析这些漏洞的行为

Todo：分析存在这些漏洞的节点IP的特征，如，ssl加密算法、位置、归属、

2.8.1 CWE ID

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Matrix | Berty | Jami | Status |
| 1 | ('CWE-79', 84) | ('CWE-400', 21) | ('CWE-79', 11) | ('CWE-400', 8) |
| 2 | ('CWE-400', 40) | ('CWE-200', 15) | ('CWE-400', 9) | ('CWE-444', 6) |
|  | ('CWE-125', 38) | ('CWE-79', 15) | ('CWE-476', 8) | ('CWE-476', 5) |
| 4 | ('CWE-200', 36) | ('CWE-125', 15) | ('CWE-200', 8) | ('CWE-200', 5) |
| 5 | ('CWE-20', 24) | ('CWE-20', 13) | ('CWE-444', 6) | ('CWE-125', 4) |
| 6 | ('CWE-416', 20) | ('CWE-476', 11) | ('CWE-787', 5) | ('CWE-190', 4) |
| 7 | ('CWE-190', 18) | ('CWE-190', 11) | ('CWE-20', 5) | ('CWE-787', 3) |
| 8 | ('CWE-770', 17) | ('CWE-444', 9) | ('CWE-190', 5) | ('CWE-601', 3) |
| 9 | ('CWE-863', 16) | ('CWE-787', 8) | ('CWE-125', 4) | ('CWE-79', 3) |
| 10 | ('CWE-284', 15) | ('CWE-284', 5) | ('CWE-126', 3) | ('CWE-287', 2) |

Todo: CWE ID的含义、产生的危害，具体的案例，CWE与IP、CVE之间关联起来

2.8.1 affected vendors

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Matrix | Berty | Jami | Status |
| 1 | ('Oracle Corporation', 769), | ('Oracle Corporation', 425), | ('Oracle Corporation', 388), | ('Red Hat', 53), |
| 2 | ('Red Hat', 116), | ('Red Hat', 85), | ('Red Hat', 85), | ('Apache Software Foundation', 41), |
|  | ('Apache Software Foundation', 69), | ('Apache Software Foundation', 67), | ('Apache Software Foundation', 64), | ('OpenSSL', 19), |
| 4 | ('JetBrains', 66), | ('OpenSSL', 54), | ('OpenSSL', 43), | ('grafana', 14), |
| 5 | ('discourse', 63), | ('PHP Group', 46), | ('PHP Group', 18), | ('squid-cache', 7), |
| 6 | ('OpenSSL', 57), | ('The Eclipse Foundation', 27), | ('grafana', 17), | ('Apache', 5), |
| 7 | ('Mozilla', 57), | ('grafana', 19), | ('Synology', 14), | ('zmartzone', 4), |
| 8 | ('PHP Group', 54), | ('Grafana', 11), | ('Oracle', 13), | ('[UNKNOWN]', 3), |
| 9 | ('Canonical', 26), | ('Microsoft', 10), | ('squid-cache', 10), | ('MongoDB Inc', 1), |
| 10 | ('Microsoft', 24) | ('squid-cache', 10) | ('Grafana', 8) | ('Grafana', 1) |

affected products：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Matrix | Berty | Jami | Status |
| 1 | ('MySQL Server', 713), | ('MySQL Server', 365), | ('MySQL Server', 341), | ('Apache HTTP Server', 54), |
| 2 | ('Apache HTTP Server', 81), | ('Apache HTTP Server', 79), | ('Apache HTTP Server', 78), | ('OpenSSL', 19), |
| 3 | ('TeamCity', 66), | ('OpenSSL', 58), | ('MySQL Cluster', 54), | ('grafana', 14), |
| 4 | ('discourse', 63), | ('MySQL Cluster', 54), | ('OpenSSL', 47), ('PHP', 19), | ('squid', 7), |
| 5 | ('OpenSSL', 61), | ('PHP', 48), | ('grafana', 17), | ('Red Hat Enterprise Linux 8', 6), |
| 6 | ('PHP', 56), | ('grafana', 19), | ('Red Hat Enterprise Linux 9', 13), | ('Red Hat Enterprise Linux 9', 6), |
| 7 | ('MySQL Cluster', 55), | ('Eclipse Jetty', 18), | ('Red Hat Enterprise Linux 8', 11), | ('mod\_auth\_openidc', 4), |
| 8 | ('MongoDB Server', 25), | ('Red Hat Enterprise Linux 9', 13), | ('Synology Router Manager | ('Red Hat Enterprise Linux 6', 4), |
| 9 | ('grafana', 22), | ('MongoDB Server', 12), | (SRM)', 10), | ('nginx', 3), |
| 10 | ('Thunderbird', 20) | ('Red Hat Enterprise Linux 8', 11) | ('squid', 10) | ('Red Hat Enterprise Linux 8.2 Advanced Update Support', 3) |

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：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # Malicious | Matrix | Berty | Jami | Status |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # Malicious | Matrix | Berty | Jami | Status |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # Malicious | Matrix | Berty | Jami | Status |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # Malicious | Matrix | Berty | Jami | Status |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |

3.4.1 referrer\_files所属于的文件类型type\_description：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # Malicious | Matrix | Berty | Jami | Status |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |

3.4.2 referrer\_files所属于popular\_threat\_classification以及label：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # Malicious | Matrix | Berty | Jami | Status |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |