# 2022年5月勒索病毒态势分析

勒索病毒传播至今，360反勒索服务已累计接收到上万勒索病毒感染求助。随着新型勒索病毒的快速蔓延，企业数据泄露风险不断上升，勒索金额在数百万到近亿美元的勒索案件不断出现。勒索病毒给企业和个人带来的影响范围越来越广，危害性也越来越大。360安全大脑针对勒索病毒进行了全方位的监测与防御，为大量需要帮助的用户提供360反勒索服务。

2022年5月，全球新增的活跃勒索病毒家族有：7Locker、EAF、QuickBubck、PSRansom、Cheers、RansomHouse、Mindware等家族，其中Cheers、RansomHouse、Mindware均为具有双重勒索功能的家族。

本月最值得关注的有三个热点：

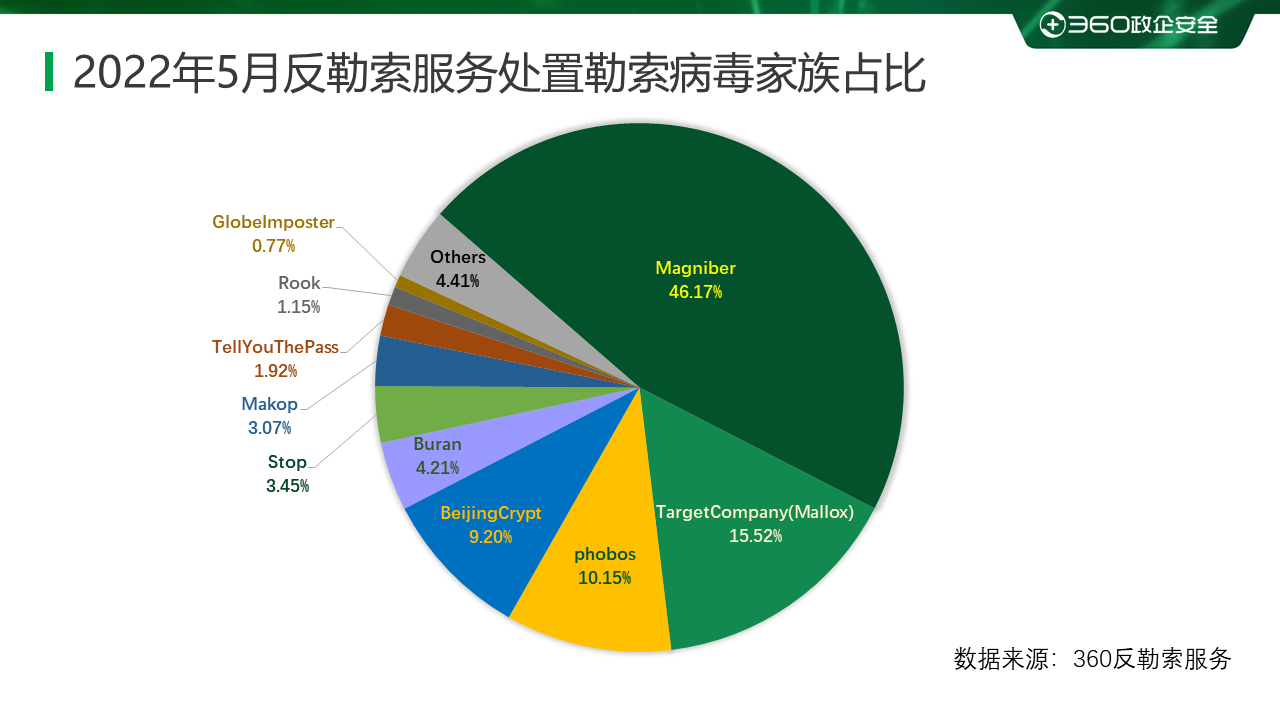
1. 5月初开始，Magniber将Windows 11加入到其攻击目标中，本月被该家族感染的受害者数量达到历史数据最高峰。
2. TargetCompany(Mallox)勒索病毒新增Web应用入侵渠道，迎来一波快速传播。
3. 本月新增通过OA系统漏洞进行传播的7Locker勒索病毒。
4. 哥斯达黎加因多个政府部门遭Conti攻击宣布国家进入紧急状态。

基于对360反勒索数据的分析研判，360政企安全集团高级威胁研究分析中心(CCTGA勒索软件防范应对工作组成员）发布本报告。

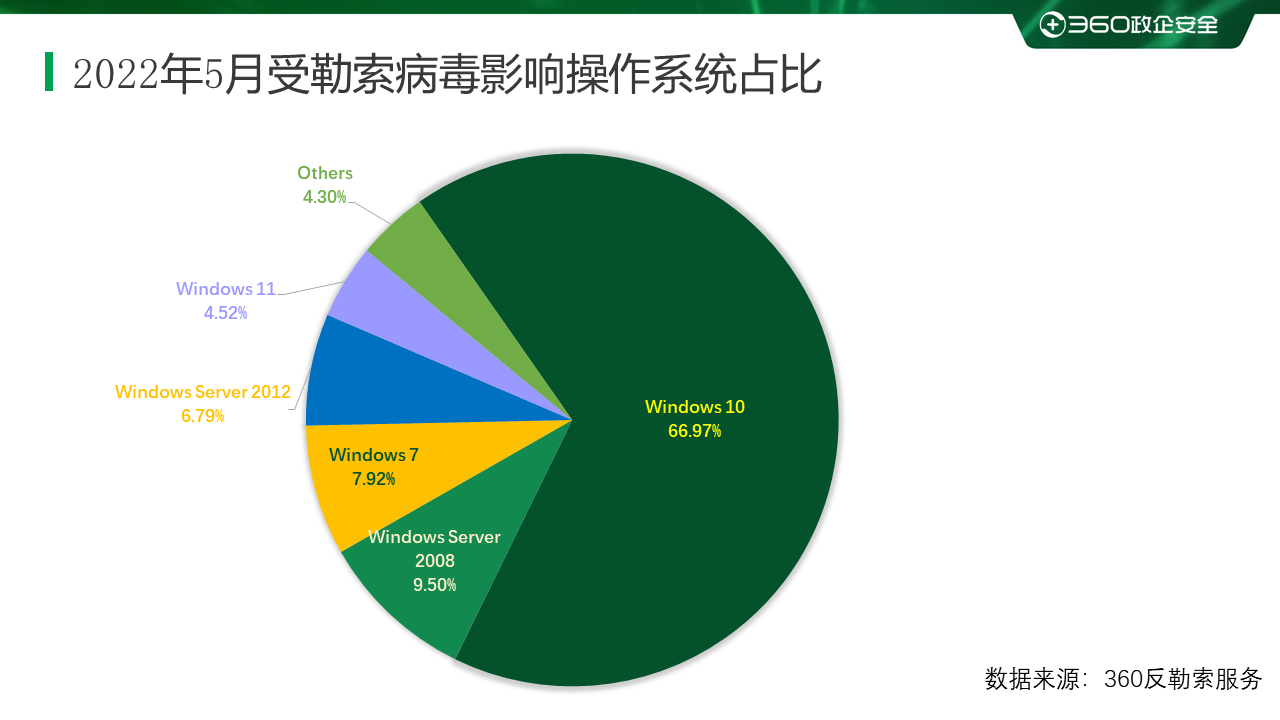
## 感染数据分析

根据本月勒索病毒受害者排查反馈统计，Magniber家族占比46.17%居首位，其次是占比15.52%的TargetCompany(Mallox)，phobos家族以10.15%位居第三。

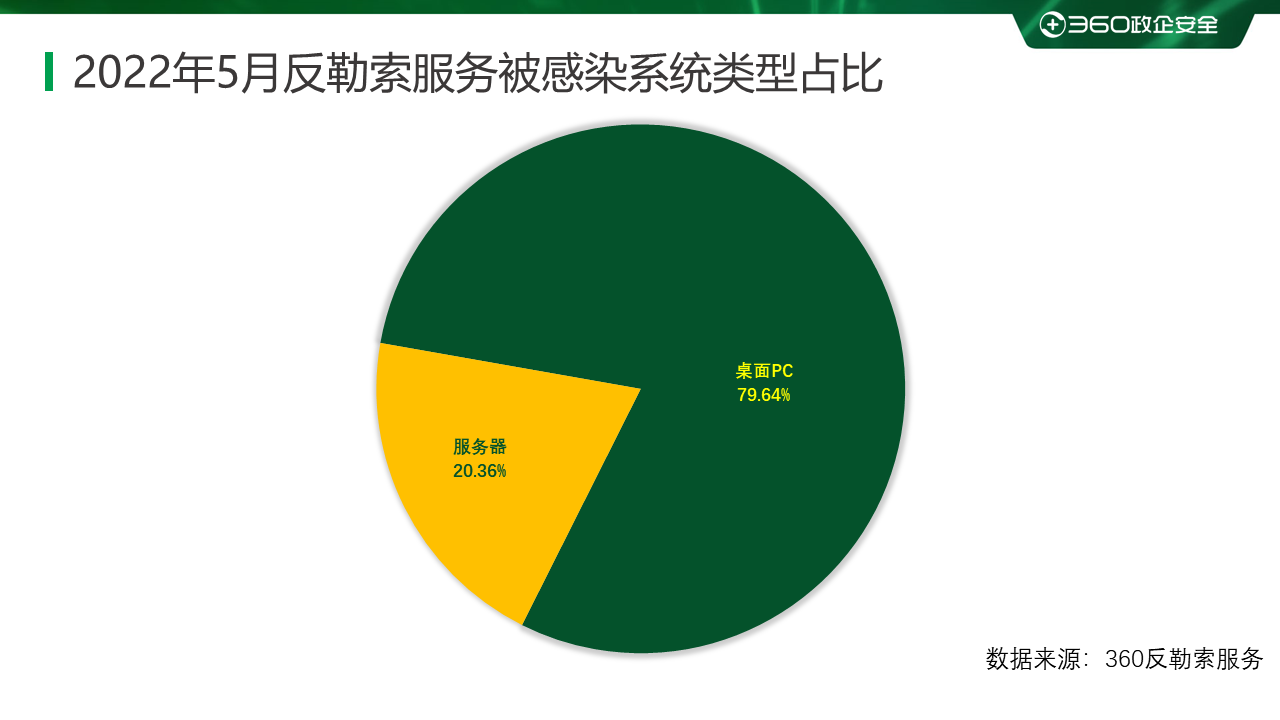
本月因大量用户浏览网站时有意或无意下载伪装成Win10/win11的补丁/升级包的Magniber勒索病毒而中招，首次出现单个家族感染量占比近50%的“霸榜”现象。



对本月受害者所使用的操作系统进行统计，位居前三的是：Windows 10、Windows Server 2008以及Windows 7。



2022年5月被感染的系统中桌面系统和服务器系统占比显示，因Magniber勒索病毒攻击这针对Windows 10和Windows 11，导致桌面PC占比上涨。



## 勒索病毒疫情分析

### Magniber勒索病毒再升级，剑指win11

今年4月底，Magniber勒索病毒伪装成Wndows10升级补丁包进行大肆传播，360安全大脑对其进行了预警。

而5月初，360安全大脑再次监测到该家族新增对Windows 11系统的攻击，其主要传播的包名也有所更新，比如：

win10-11\_system\_upgrade\_software.msi

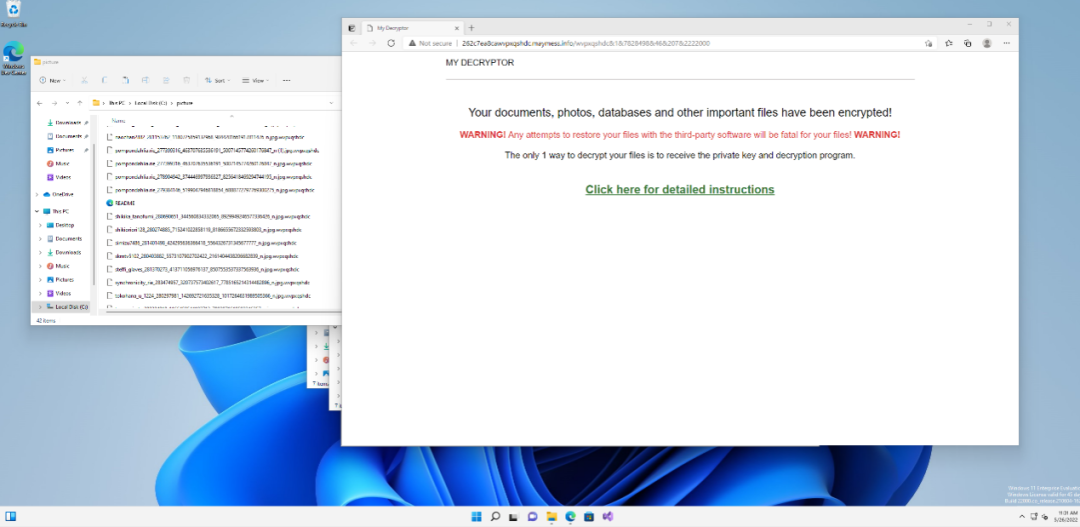
covid.warning.readme.xxxxxxxx.msi

其传播方式仍然是各类论坛、破解软件网站、虚假色情站等。用户在访问这些站点时，会被诱导至第三方网盘下载伪装成补丁或更新的勒索病毒。此外也有部分网站存在自动下载情况。

以下是该病毒近期传播针对Windows 11的攻击态势图：



遭到该勒索病毒加密后，文件后缀会被修改为随机后缀，且每个受害者会有一个独立的支付页面——若不能在规定时间内支付赎金，该链接将失效。若受害者能在5天内支付赎金，则只需支付0.09个比特币(截止该报告撰写时，约合人民币17908元)，而超过5天赎金将会翻倍。

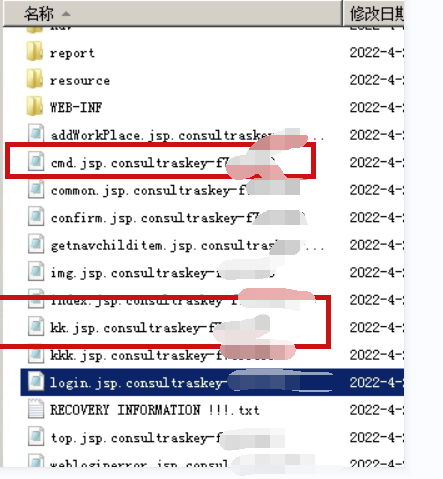


### 新增Web应用入侵渠道，Mallox勒索病毒迎来一波快速传播

本月360安全大脑监测发现多起Mallox勒索病毒攻击事件。该病毒主要针对企业的Web应用发起攻击，包括Spring Boot、Weblogic、通达OA等。在其拿下目标设备权限后还会尝试在内网中横向移动，获取更多设备的权限，危害性极大。360提醒用户加强防护，并建议使用360终端安全产品提供的安全补丁，防御查杀该病毒。

360安全大脑监测历史显示，Mallox（又被称作Target Company）于2021年10月进入中国，早期主要通过SQLGlobeImposter渠道进行传播（通过获取到数据库口令后，远程下发勒索病毒。该渠道曾长期被GlobeImposter勒索病毒使用）。而今年GlobeImposter勒索病毒的传播量逐渐下降，Mallox就逐渐占据了这一渠道。

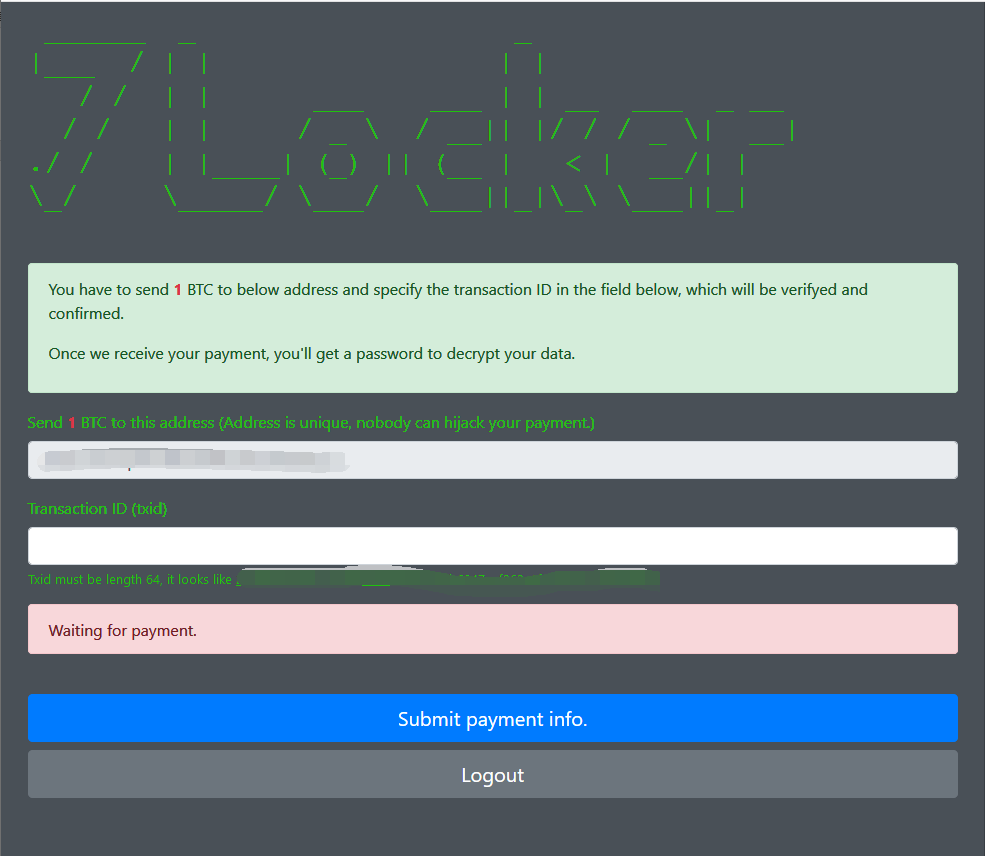
除了传播渠道之外，360通过分析近期攻击案例发现攻击者会向Web应用中植入大量的WebShell，而这些文件的文件名中会包含“kk”的特征字符。一旦成功入侵目标设备，攻击者会尝试释放PowerCat、lCX、AnyDesk等黑客工具控制目标机器、创建账户，并尝试远程登录目标机器。此外，攻击者还会使用fscan工具扫描设备所在内网，并尝试攻击内网中的其它机器。在获取到最多设备权限后开始部署勒索病毒。



### 新增通过OA系统漏洞进行传播的7Locker勒索病毒

近日360安全大脑监控到一款新型勒索病毒7Locker，该病毒使用java语言编写，并通过OA系统漏洞进行传播。其本质上是利用7z压缩工具将文件添加密码后进行压缩，被加密压缩后的文件被新增扩展名.7z。每个受害者通过唯一的Client Key查看具体赎金要求以及指定的赎金支付地址。

另外，根据目前已掌握的信息推测：该家族的传播事件有很大概率是中国台湾黑客针对中国内陆发起的勒索攻击。

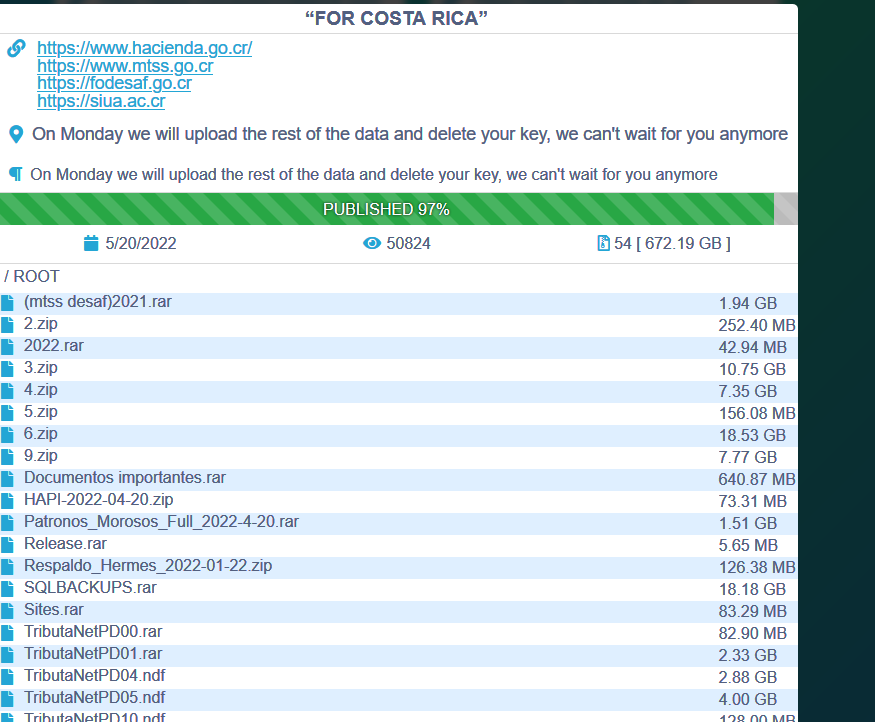


## 哥斯达黎加因多个政府部门遭Conti攻击宣布国家进入紧急状态

5月8日星期日，新当选的哥斯达黎加总统查韦斯宣布国家进入紧急状态，理由是多个政府机构正遭到Conti勒索病毒攻击。

Conti勒索病毒最初声称上个月对哥斯达黎加政府进行了攻击。该国的公共卫生机构哥斯达黎加社会保障基金（CCSS）早些时候曾表示，“正在对Conti勒索病毒进行外围安全审查，以验证和防止其可能再次发动攻击。”

目前，Conti已发布了大约672 GB的数据，其中似乎包含属于哥斯达黎加政府机构的数据。



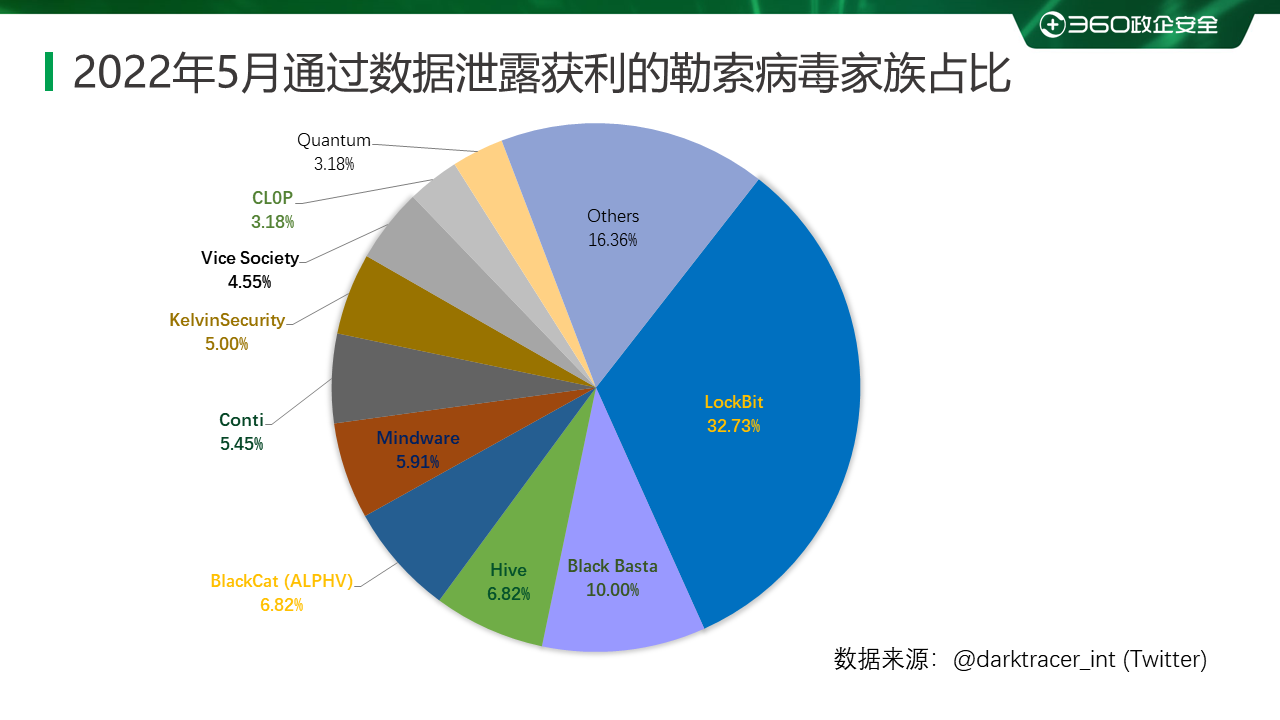
## 黑客信息披露

以下是本月收集到的黑客邮箱信息：

|  |  |  |
| --- | --- | --- |
| martin1993douglas@pressmail.ch | mallox@stealthypost.net | paid-files@email.tg |
| avastdata@privatemail.com | @pipikaki | filerecoveryassistant@privatemail.com |
| peekaboom@tuta.io | avastdata@airmail.cc | avastdata@privatemail.com |
| blackcatcc@airmail.cc | blackcat@privatemail.com | manager@time2mail.ch |
| dear\_decript2022@mail2tor.com | dear\_decript2022@jabbim.com | avastdata@privatemail.com |
| mallox@stealthypost.net | uped97@mail.ee | ginnydterrell@onionmail.org |
| martin1993douglas@pressmail.ch | back2023@proxy.tg | uped97@mail.ee |
| uped98@mail.ee | Spiderlock@email.tg | fast\_decript2022@mail2tor.com |
| avastdata@airmail.cc | help001@privatemail.com | FreedomTeam@mail.ee |
| bryan1984jackson@tutanota.com | cris\_nickson@xmpp.jp | manager@time2mail.ch |
| Spiderlock@email.tg | ginnydterrell@onionmail.org | yoshihama@tutanota.com |
| fine3412@mailfence.com | fine3413@mailfence.com | hughclapperton1877@gmx.com |
| help24@nerdmail.co | millenniumcrypt@msgsafe.io | ironse2022@tutanota.com |
| NormanBaker1929@gmx.com | ThomasJames1597@gmx.com | dec\_keys@tutanota.com |
| mallox@stea1thypost.net | maliflynanth@aol.com | devicezzz@tutanota.com |
| helprecoverthis@mailfence.com | qamrani@airmail.cc | dec\_keys@tutanota.com |
| johnhelper@gmx.de | supportx@onionmail.com | file\_decryption@privatemail.com |
| elmorenolan30@nerdmail.co | Rdpmanager@airmail.cc | decryptyourfiles@firemail.cc |
| ariakei@protonmail.com | 2022blue@mailfence.com | ironse2022@tutanota.com |
| lordgarson@aol.com | marcosmelborn@aol.com | Gotoworld@tutanota.com |
| blosson821@protonmail.com | return.files@yandex.com | return.files@keemail.me |
| horsemagyar@onionmail.org | d3add@protonmail.com | propersolot@gmail.com |
| propersolot@gmail.com | d3add@tutanota.com |  |

表格1. 黑客邮箱

当前，通过双重勒索或多重勒索模式获利的勒索病毒家族越来越多，勒索病毒所带来的数据泄露的风险也越来越大。以下是本月通过数据泄露获利的勒索病毒家族占比，该数据仅为未能第一时间缴纳赎金或拒缴纳赎金部分（已经支付赎金的企业或个人，可能不会出现在这个清单中）。



以下是本月被双重勒索病毒家族攻击的企业或个人。若未发现被数据存在泄露风险的企业或个人也请第一时间自查，做好数据已被泄露准备，采取补救措施。

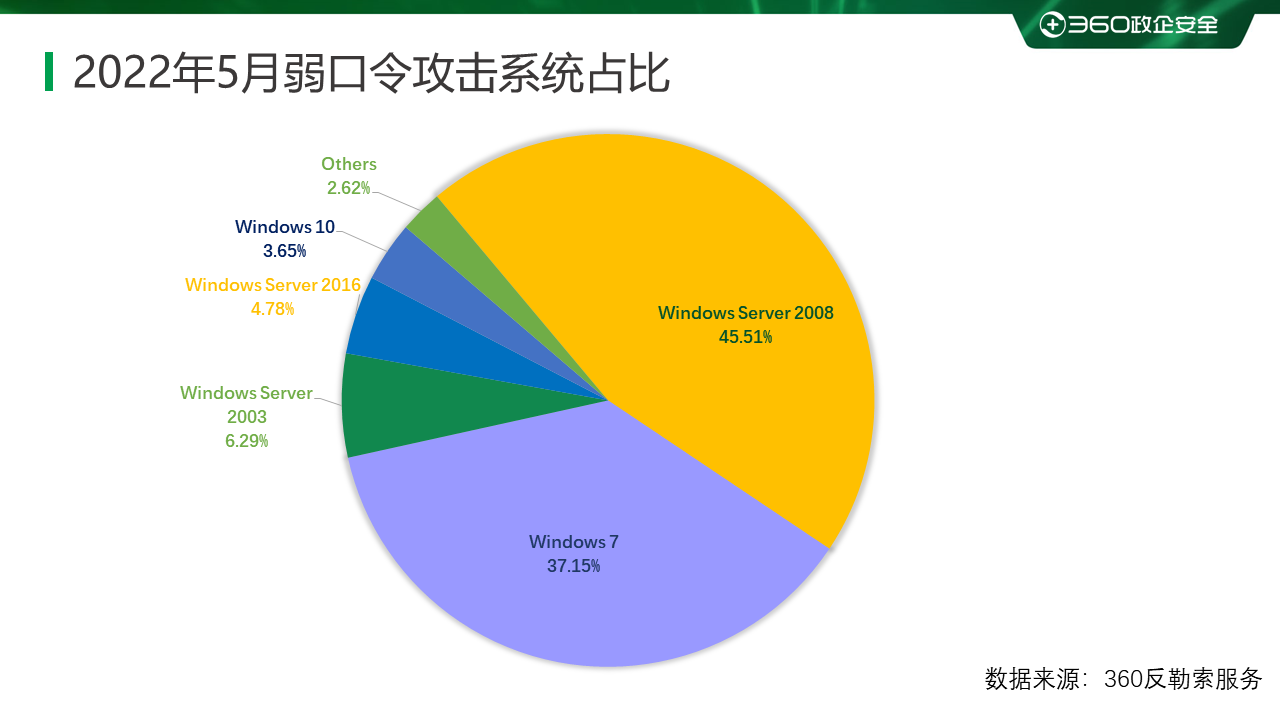
本月总共有220个组织/企业遭遇勒索攻击，其中包含中国10个组织/企业（含中国台湾省5个组织/企业）在本月遭遇了双重勒索/多重勒索。

|  |  |  |
| --- | --- | --- |
| EYP | Elkuch Group | bradfordmarine.com |
| smd | Grupo Pavisa | agapemeanslove.org |
| AGCO | M+A Partners | sherpamarketing.ca |
| LCRD | 2easy.com.br | aref.government.bg |
| FAMO | agenilsen.no | ELTA Hellenic Post |
| SOUCY | fnoutlet.com | Jameco Electronics |
| XEIAD | erediriva.it | An Belgium Hospital |
| SYSOL | edm-stone.com | The Contact Company |
| NUAIRE | foxconnbc.com | FERRAN-SERVICES.COM |
| XYTECH | pointsbet.com | virtus-advocaten.be |
| ivu.de | TRANSCONTRACT | morrisonexpress.com |
| Magtek | gdctax.com.au | BRITISH LINK KUWAIT |
| Tri-Ko | purapharm.com | Dellner Couplers AB |
| Pianca | grupocabal.cl | ATAPCOPROPERTIES.COM |
| ProJet | hinakaorg.com | An Financial Company |
| Upskwt | fodesaf.go.cr | groupe-trouillet.com |
| Cabase | nizing.com.tw | kuwaitflourmills.com |
| nottco | intertabak.com | Ludwig Freytag Group |
| diager | koenigstahl.pl | boltburdonkemp.co.uk |
| Mebulbs | suntecktts.com | Atron Solutions, LLC |
| EIITNET | Allports Group | An Technology Company |
| HEMERIA | Carmel College | Allcat Claims Service |
| callinc | mosaiceins.com | Brunk Industries Inc. |
| allwell | www.mtss.go.cr | Unicity International |
| Westwood | mercyhurst.edu | silverbayseafoods.com |
| pauly.de | Haynes Manuals | erdwaerme-gruenwald.de |
| RateGain | PTC Industries | modetransportation.com |
| VMT-GmbH | ENSSECURITY.COM | Jefferson Credit Union |
| RateGain | Whitehall. (OH) | Sarasin & partners LLP |
| AMETHYST | CMC Electronics | LATOURNERIE-WOLFROM.COM |
| Eurocept | firbarcarolo.it | The Catholic Foundation |
| InnPower | wsretailers.com | Asia Pacific University |
| rogz.com | FTSUMNERK12.COM | Municipality of Posadas |
| bfclcoin | seatarrabida.pt | Richardson & Pullen, PC |
| willsent | berschneider.de | Omicron Consulting S.r.L |
| smtuc.pt | Black Bros. Co. | realestateconsulting.com |
| welplaat | Tex-Isle Supply | orthopaedie-appenzell.ch |
| gymund.dk | sgservicesud.it | ChemStation International |
| Tecnopack | NEWCOURSECC.COM | Trans Technology Pte Ltd. |
| khs-wp.de | riken-nosan.com | saludparatodos.ssm.gob.mx |
| xydias.gr | AmCham Shanghai | architectenbureaugofflo.be |
| CAVENDERS | cassagne.com.ar | Blairex Laboratories, Inc. |
| toshfarms | talaadthaii.com | Collegiate sports medicine |
| thebureau | zine-eskola.eus | Central Restaurant Products |
| micropakk | ats-insubria.it | Grohmann Aluworks GmbH & Co |
| Caracol TV | rexontec.com.tw | Instance IT Solutions India |
| BLAIR inc. | Rollecate Group | ils.theinnovatecompanies.com |
| SPORTPLAZA | apsmsystems.com | Atlanta Perinatal Associates |
| CARTEGRAPH | shimamura.gr.jp | Wilks Tire & Battery Service |
| detego.com | Sole Technology | G&P Projects And Systems S.A. |
| Fronteousa | tcpharmachem.com | Guardian Fueling Technologies |
| usu.org.au | Mansfield Energy | Flexible Circuit Technologies |
| optoma.com | vitalprev.com.br | GREEN MOUNTAIN ELECTRIC SUPPLY |
| mef.gob.pe | skinnertrans.net | Campbell & Partners Consulting |
| siua.ac.cr | clublinks.com.au | UNIWELL Rohrsysteme GmbH & Co. |
| vivalia.be | alliancesand.com | Jasper County Sheriff's Office |
| topaces.us | boltburdon.co.uk | Horwitz Law, Horwitz & Associates |
| Zito Media | arcelormittal.hu | An International Maritime Company |
| mediuscorp | Tosoh Bioscience | Hirsch Watch Straps & Accessories |
| zdgllc.com | nipmo.dst.gov.za | The People's Federal Credit Union |
| SPERONI SpA | PRGX Global Inc. | Contraloría General de la República |
| Travira Air | cwaengineers.com | Active Communications International |
| gpmlife.com | The Scholz Group | Faw-Volkswagen Automobile Co., Ltd. |
| fed-gmbh.de | Imagen Television | AHS Aviation Handling Services GmbH |
| teka.com.mx | Channel Navigator | Boom Logistics (boomlogistics.com.au) |
| Salud Total | Caldes de Montbui | Florida Department of Veterans' Affairs |
| sportco.com | J.F. Taylor, Inc. | Contractors Pipe and Supply Corporation |
| safarni.com | FIBERTEL PERÚ SAC | Love, Barnes & McKew Insurance Adjusters |
| delcourt.fr | Tosoh Corporation | Saskatchewan Liquor and Gaming Authority |
| acorentacar | simpsonplastering | CPQD - BANCO CENTRAL OF BRASIL BLOCKHAIN |
| PRICEDEX.COM | hospitalsanjose.es | Piggly Wiggly Alabama Distributing Company |
| pet-link.com | Yachiyo Of America | Higher School of the Public Ministry of the Union |
| cysco.com.tw | Transsion Holdings | Klasner Solomon & Partners Chartered Professional Accountants |
| www.intertabak.com |  |  |

表格2. 受害组织/企业

## 系统安全防护数据分析

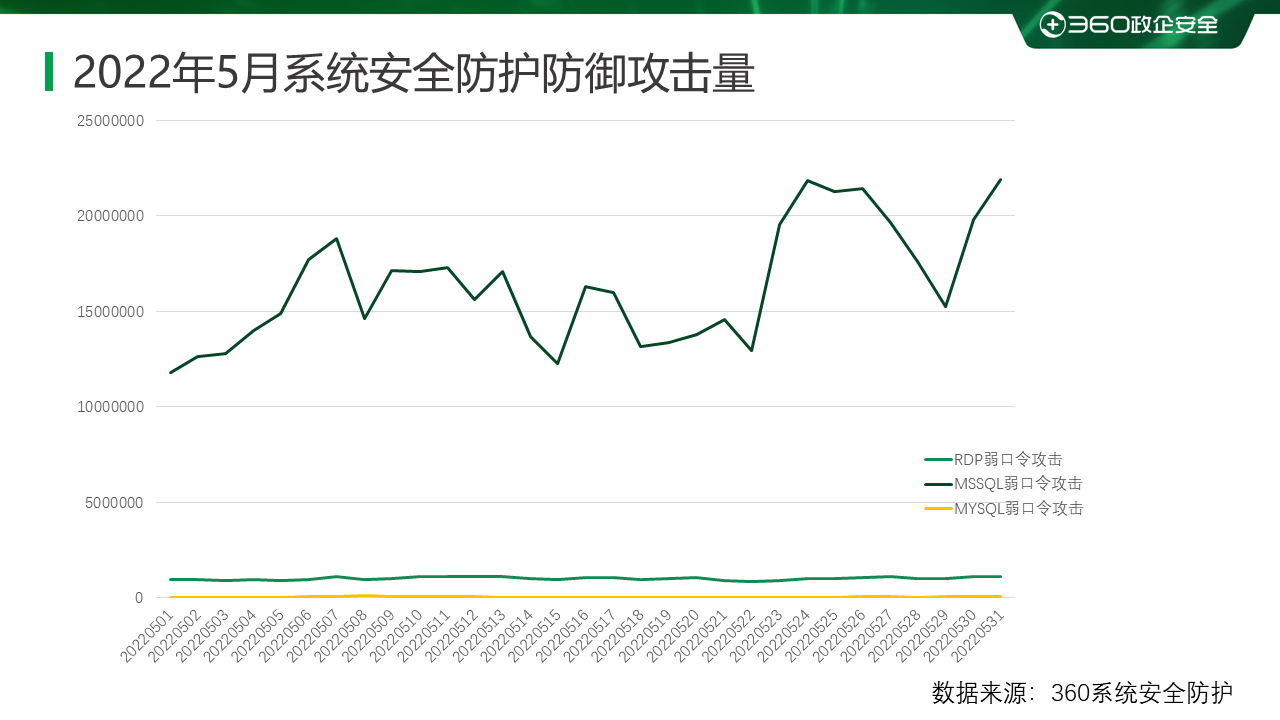
在本月被攻击的系统版本中，排行前三的依次为Windows Server 2008 、Windows 7以及Windows Server 2003。



对2022年5月被攻击系统所属地域统计发现，与之前几个月采集到的数据进行对比，地区排名和占比变化均不大。数字经济发达地区仍是攻击的主要对象。



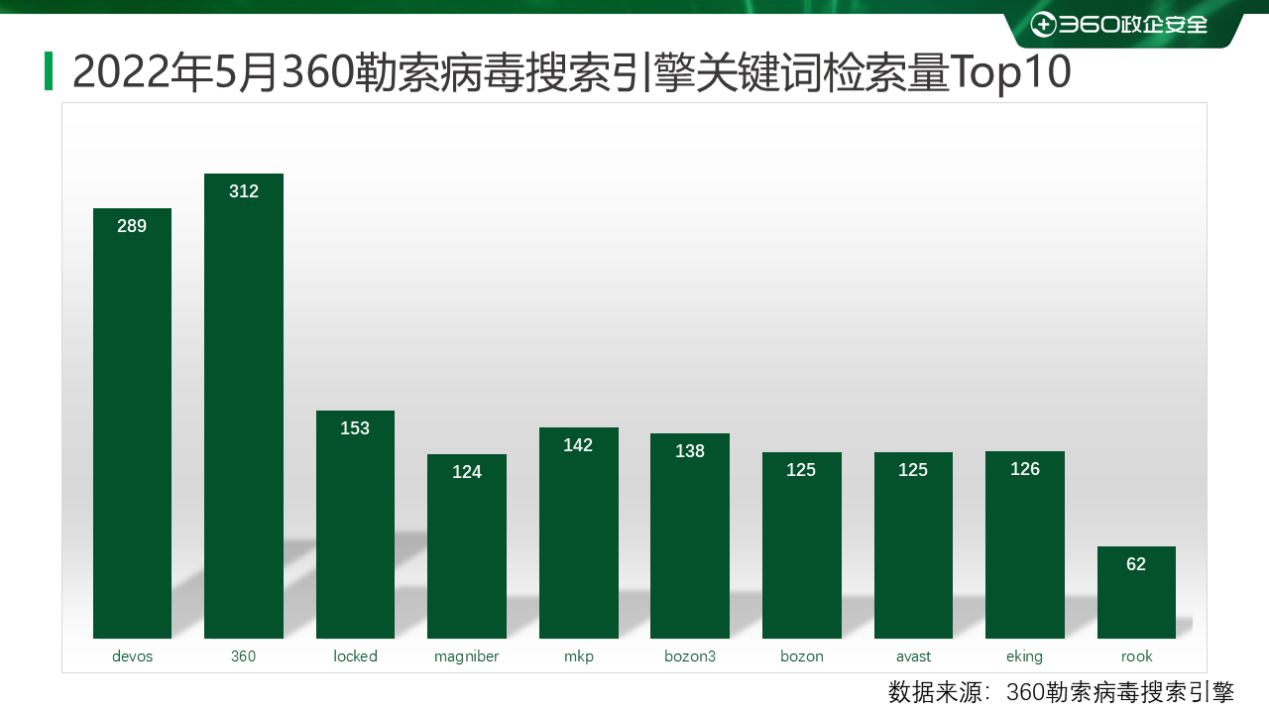
通过观察2022年5月弱口令攻击态势，发现RDP弱口令攻击和MYSQL弱口令攻击整体无较大波动。MSSQL弱口令攻击虽有波动，但依然处于常规范围内且整体呈上升态势。



## 勒索病毒关键词

以下是本月上榜活跃勒索病毒关键词统计，数据来自360勒索病毒搜索引擎。

* devos：该后缀有三种情况，均因被加密文件后缀会被修改为devos而成为关键词。但本月活跃的是phobos勒索病毒家族，该家族的主要传播方式为：通过暴力破解远程桌面口令成功后手动投毒。
* 360：属于BeijngCrypt勒索病毒家族，由于被加密文件后缀会被修改为360而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒，本月新增通过数据库弱口令攻击进行传播。
* locked:locked曾被多个家族使用，但在本月使用该后缀的家族是TellYouThePass勒索病毒家族。由于被加密文件后缀会被修改为locked而成为关键词。该家族本月主要的传播方式为：通过Log4j2漏洞进行传播。
* Magniber：
* mkp：属于Makop勒索病毒家族，由于被加密文件后缀会被修改为mkp而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。
* bozon3:属于TargetCompany(Mallox)勒索病毒家族，由于被加密文件后缀会被修改为bozon3。该家族传播渠道有多个，包括匿隐僵尸网络、横向渗透以及数据库弱口令爆破。本月新增通过入侵Web应用进行传播。
* bozon:同bozon3。
* avast: 同bozon3。
* eking:属于phobos勒索病毒家族，由于被加密文件后缀会被修改为eking而成为关键词。家族的主要传播方式为：通过暴力破解远程桌面口令成功后手动投毒。
* rook:属于Rook勒索病毒家族，由于被加密文件后缀会被修改为rook而成为关键词。该家族的主要传播方式为：通过匿隐僵尸网络进行传播。本月(2022年2月)受害者大部分是因为到下载网站下载注册机感染的匿隐僵尸网络。



## 解密大师

从解密大师本月解密数据看，解密量最大的是GandCrab，其次是Coffee。使用解密大师解密文件的用户数量最高的是被Crysis家族加密的设备，其次是被CryptoJoker家族加密的设备。

