# 2022年1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控与防御，为需要帮助的用户提供360反勒索服务。

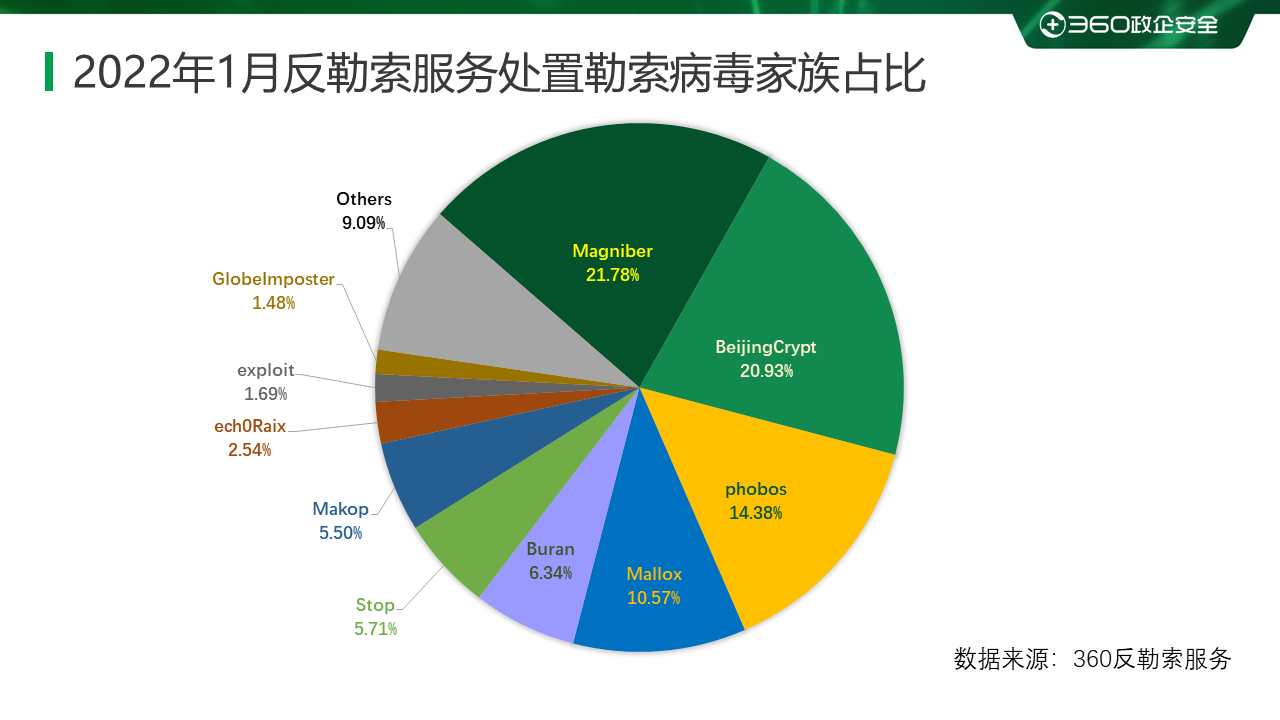
2022年1月，全球新增的活跃勒索病毒家族有: Coffee、Night Sky、DeadBolt、Koxic、Trap、EvilNominatus等家族，其中NightSky是本月新增的双重勒索病毒，利用Log4j漏洞对VMwaer Horizon服务器发起攻击；DeadBolt是一款针对QNAP网络存储设备进行攻击的勒索病毒，该团伙向QNAP索要50BTC以提供万能密钥。

## 感染数据分析

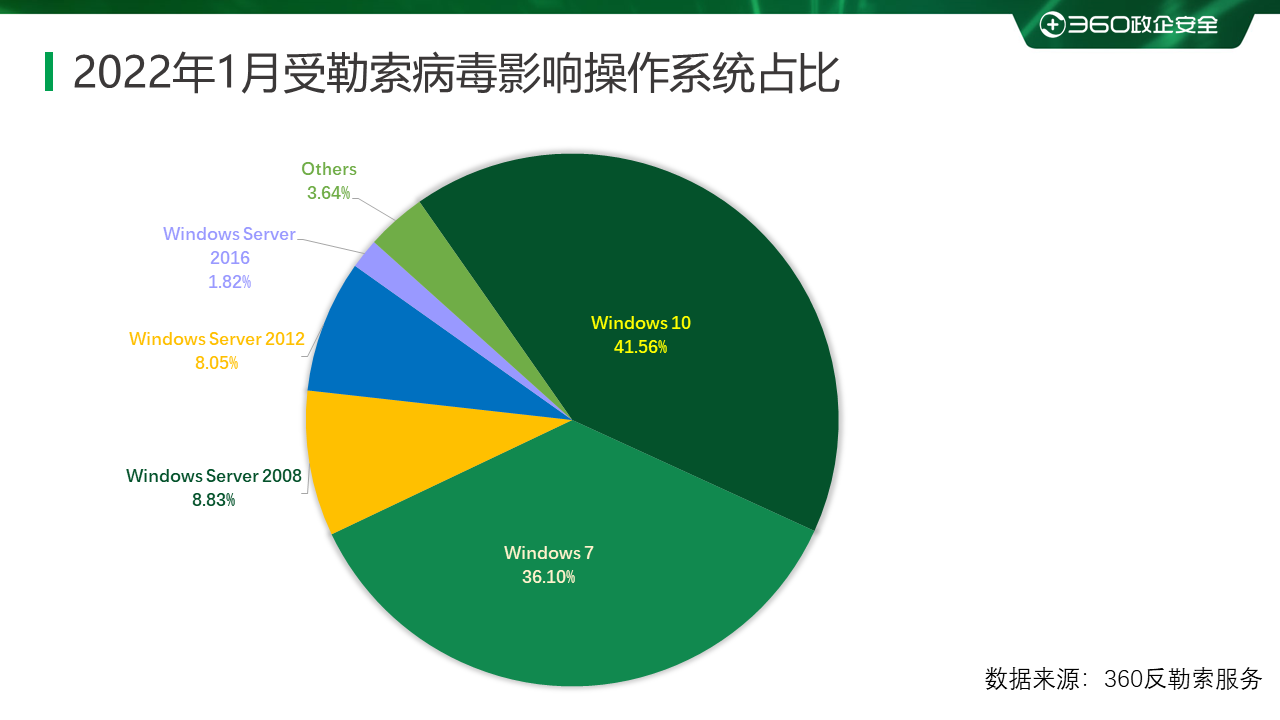
针对本月勒索病毒受害者所中勒索病毒家族进行统计，Magniber家族占比21.78%居首位，其次是占比20.93%的BeijingCrypt，phobos家族以14.38%位居第三。

根据360安全大脑监控到的数据显示：

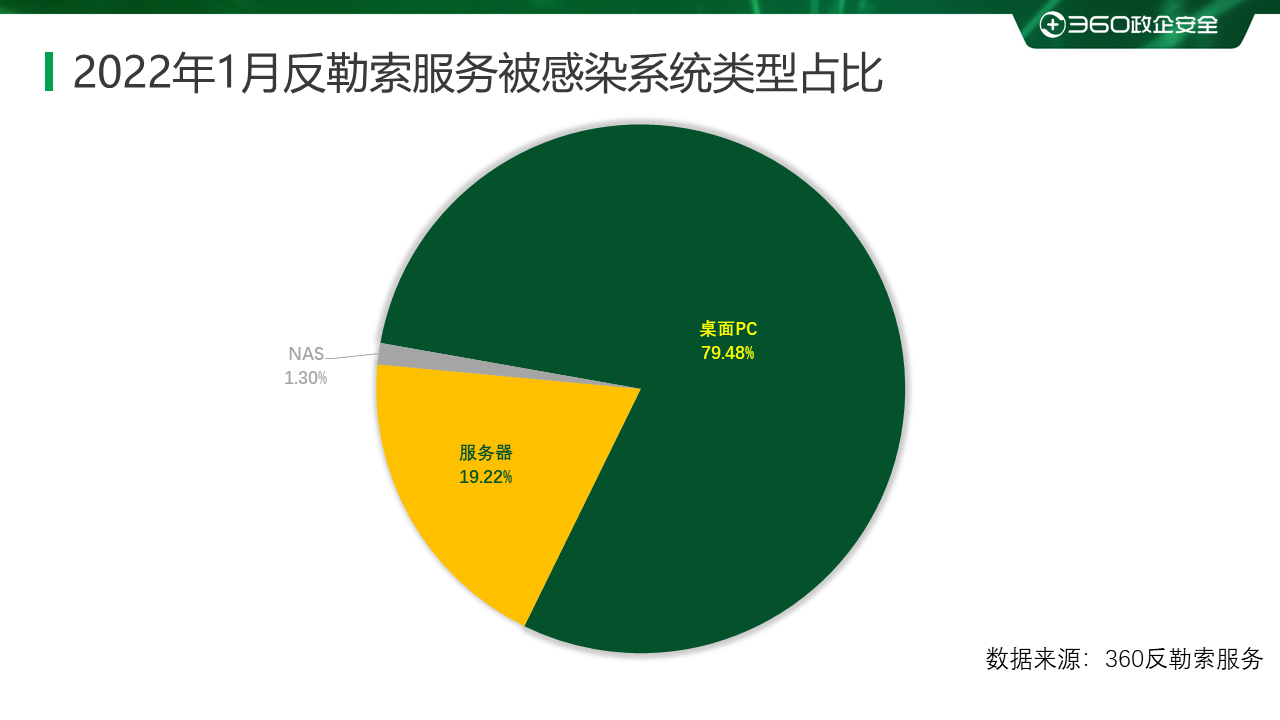
* 本月BeijingCrypt勒索病毒家族的传播量有上升，该家族对其传播渠道进行了扩展，将数据库弱口令攻击方式作为另一主要传播方式。
* 本月扩展传播渠道的还有Mallox勒索病毒家族，本月发现该家族还使用到了匿影僵尸网络。
* 本月首次在国内发现由Babuk泄露代码衍生而来的Rook勒索病毒。



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 7、Windows 10、以及Windows Server 2008。



2022年1月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型仍以桌面系统为主。与上个月相比，无较大波动。

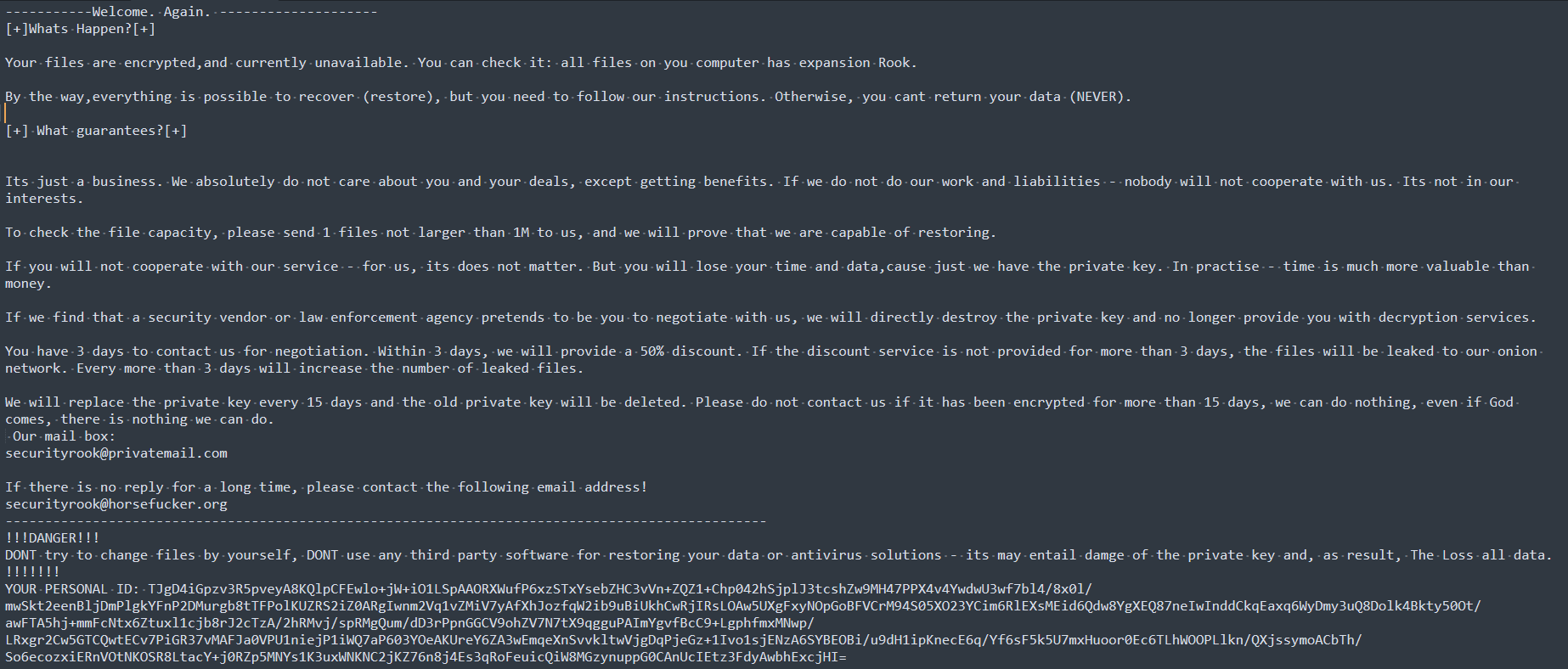


## 勒索病毒事件

### Rook勒索病毒可能会令数据永久丢失

2021年11月360安全大脑监控到由Babuk泄露代码衍生而来的Rook勒索病毒开始采用双重勒索的模式进行传播。截止该家族2022年1月8日最后一次公布受害者名单，已有7个公司/组织遭遇该家族攻击。

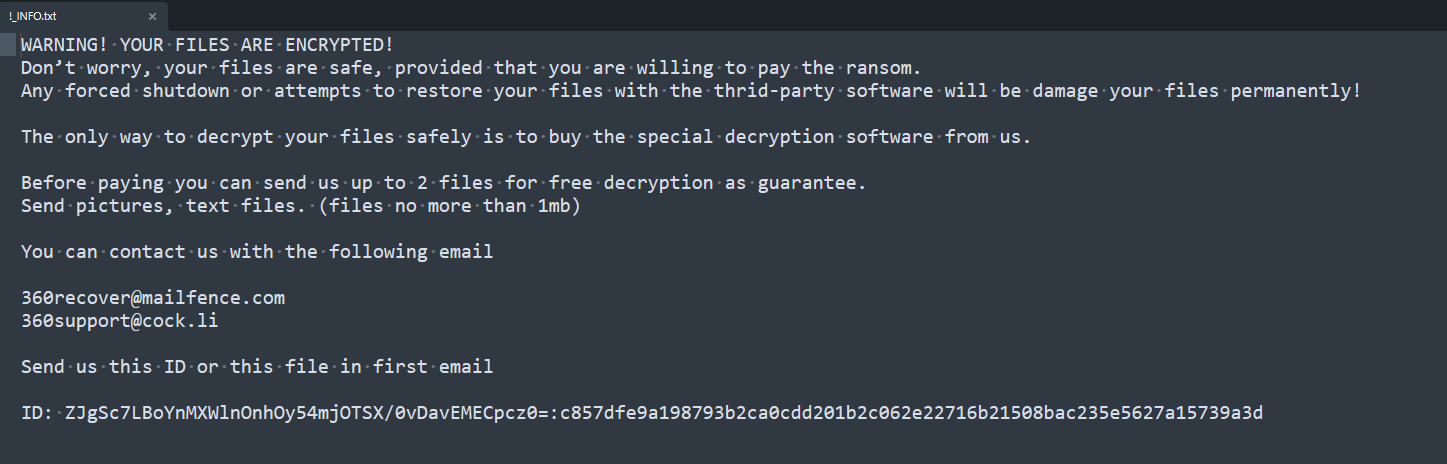
在本月底，360安全大脑监控到该家族通过匿影僵尸网络开始在国内传播，修改被加密文件后缀为.rook,rook2,rook3。从勒索提示信息看，此轮攻击虽提到会将从受害者处窃取到的数据公布到暗网，但该家族的数据泄露网站目前仍无法访问。同时，该团伙称他们将会每15天更换一次私钥，而旧的私钥将被删除。如果文件被加密已超过15天，他们也将无法恢复。



### BeijingCrypt最新变种修改后缀为.360

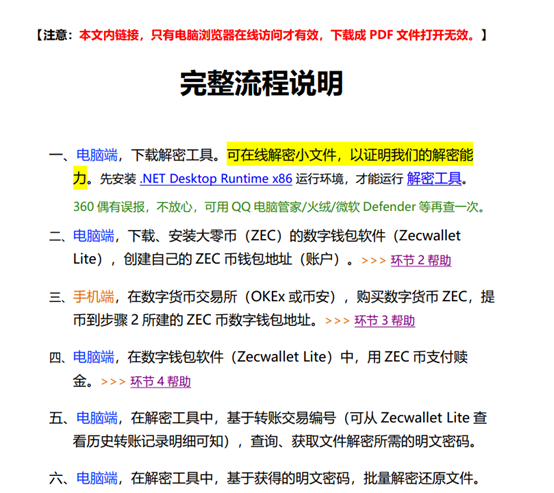
根据360安全大脑数据，发现活跃勒索病毒家族BeijingCrypt出现新变种——被加密文件后缀变为“.360”，黑客的联系邮箱则变更为“360support@cock.li”和“360support@mailfence.com”。

该勒索病毒家族因其早期将文件后缀修改为“beijing”而得名（beijing后缀当前仍在使用）。自2020年6月出现以来，其就利用远程桌面弱口令在国内传播，并在2021年开始传播量越来越逐月上升，最终跃升至国内勒索病毒传播量Top10榜单。目前该家族已经历了genesis、beijing、520、file、360等多个后缀变种且传播越发活跃。在本月，该家族还通过爆破破解获取数据库口令后向受被攻击设备下发勒索病毒。



### 本土勒索病毒家族Coffee开始传播

根据360安全大脑数据，发现国内新出现勒索病毒家族Coffee。该家族以其将加密后的文件后缀修改为coffee.xxxx(x为随机字符)而得名。Coffee病毒是一个具有蠕虫性质的勒索病毒，一般通过软件捆绑和QQ群钓鱼传播，能够感染系统中常用软件，同时还可以主动将自己发往QQ群传播。该家族向受害者索要ZEC（零币）这一较为罕见的虚拟货币作为赎金。其不仅提供了中文的勒索信息，还附带了非常详细且“贴心”的全中文支付教程——指导用户如何对ZEC进行安装、购买和支付。从目前捕获到的信息看，该病毒会向受害者索要价值500美元的ZEC。

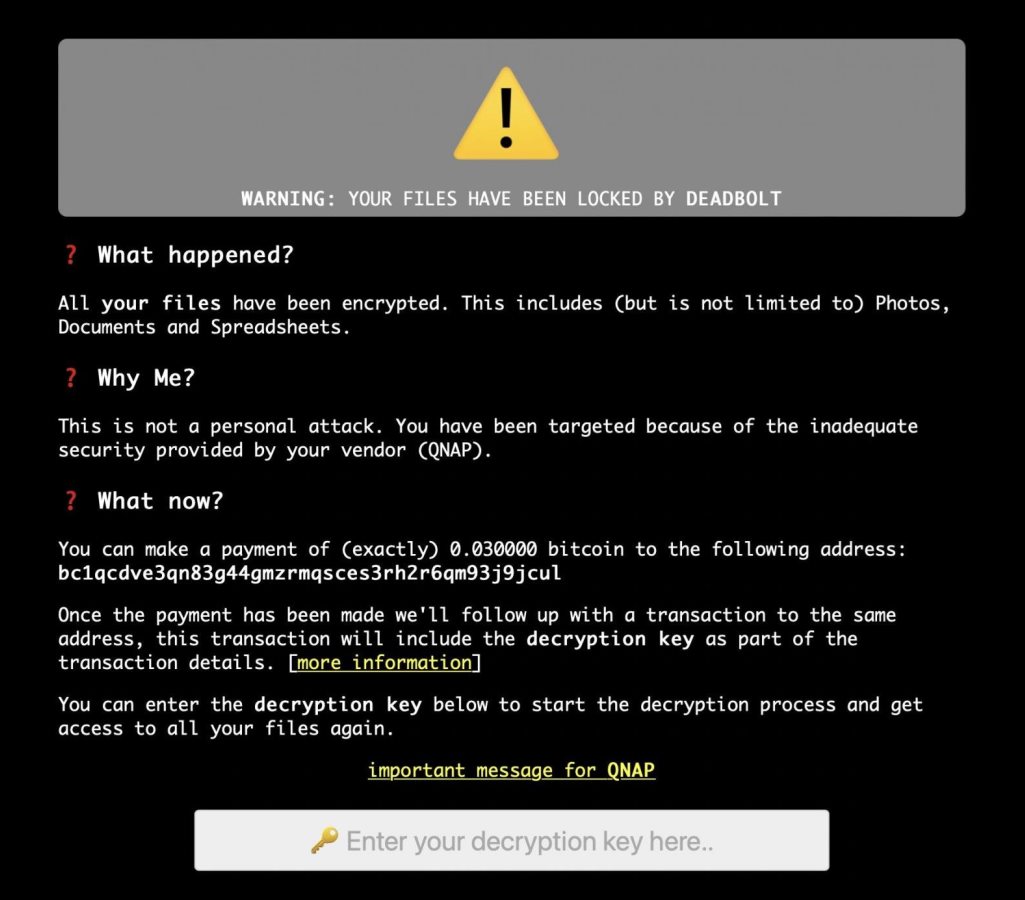


### 新勒索病毒DeadBolt瞄准QNAP设备，索要50 BTC提供万能密钥

新兴勒索病毒DeadBolt声称他们正在使用设备软件的0day漏洞对全球QNAP NAS设备进行加密攻击。

攻击于1月25日开始，中招的QNAP设备会突然发现其文件被加密，设备中存储的文件的文件名会被追加一个名为.deadbolt的文件扩展名。而设备的登录页面会被劫持显示一个勒索页面：内容为“警告：您的文件已被DeadBolt锁定”等。该页面会向受害者索要0.03个比特币作为赎金。

此外病毒还在勒索页面中声称，如果QNAP向他们支付5个比特币，DeadBolt勒索软件团伙将提供0day漏洞的全部详细信息。同时他们还愿意以50个比特币的售价向QNAP出售可以为所有受害者解密文件的主密钥和0day信息。



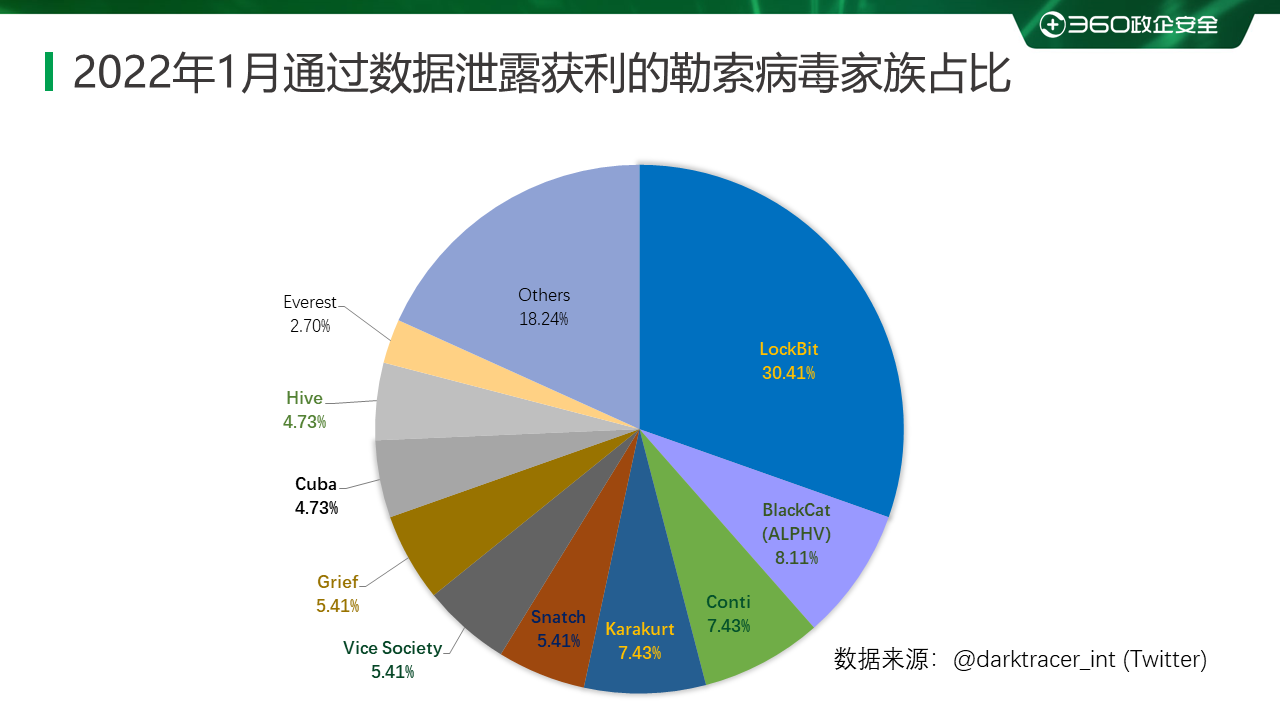
## 黑客信息披露

以下是本月收集到的黑客邮箱信息：

|  |  |  |
| --- | --- | --- |
| mallox@cock.li | qazqwe@onionmail.org | FilesRecoverEN@gmail.com |
| floy2020@cock.l | steriok@mail2tor.com | asiarecoverydata@cock.li |
| Elbowtalk@my.com | phobos\_helper@xmpp.jp | proper12132@tutanota.com |
| zitenmax@cock.li | Myfiles.sir@gmail.com | restaurera@safeswiss.com |
| temloown@tuta.io | decypt20@firemaill.cc | beijing5200@mailfence.com |
| BillScars@gmx.com | keepserver2020@cock.li | jackrasal@privatemail.com |
| qazqwe@msgsafe.io | Jeseekuer@tutanota.com | malloxdatac@mailfence.com |
| ghxyz@fonix.email | anony.alex22@gmail.com | beijing520@horsefucker.org |
| 360support@cock.li | walter1964@mail2tor.com | FobosAmerika@protonmail.ch |
| temloown@gmail.com | ofizducwe111988@aol.com | recoveryfiles@techmail.info |
| monster666@tuta.io | 360helper@mailfence.com | veronikstreem@protonmail.com |
| helpunlock@aol.com | tsuppor@privatemail.com | cigleperation@protonmail.com |
| restaurera@rbox.co | 6lilium6@protonmail.com | securityrook@horsefucker.org |
| support@sysmail.ch | 360support@mailfence.com | securityrook@privatemail.com |
| guan\_yu@tutanota.com | phobos\_helper@exploit.im | isecondhelperforunlockyourfiles@airmail.cc |
| mrpicokins@gmail.com | psychopath7@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）。



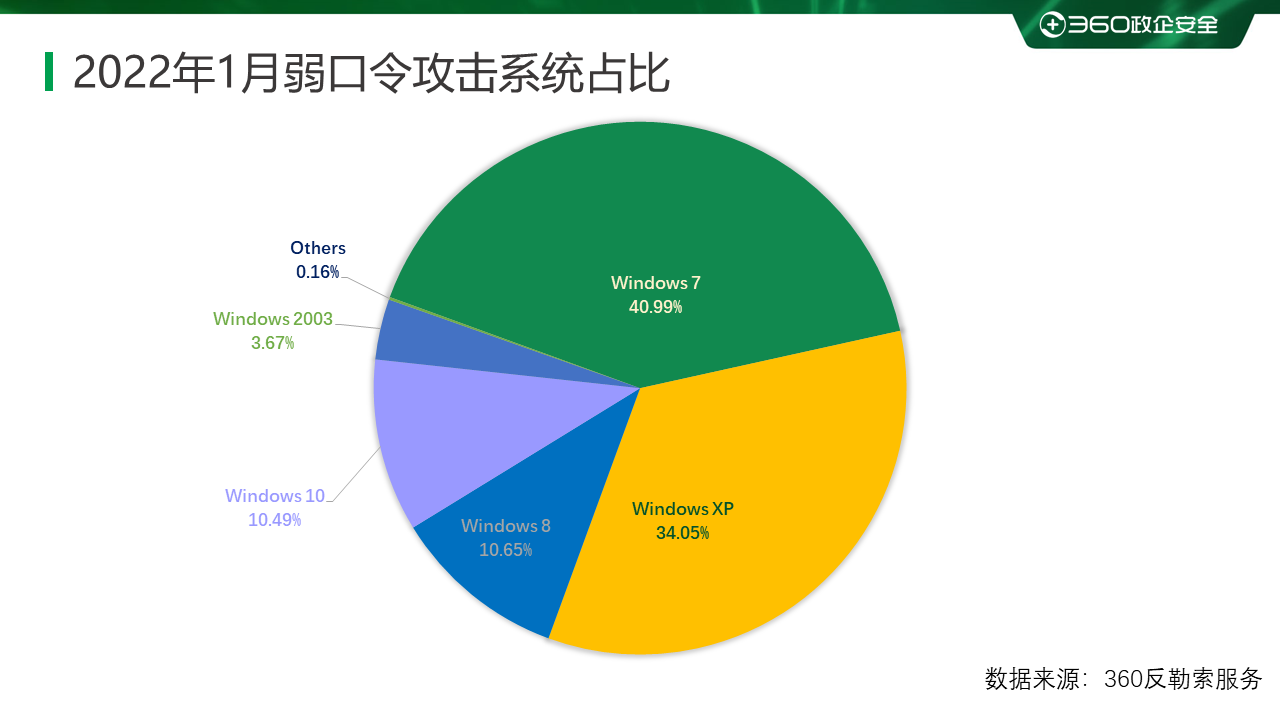
以下是本月被双重勒索病毒家族攻击的企业或个人。若未发现被数据存在泄露风险的企业或个人也请第一时间自查，做好数据已被泄露准备，采取补救措施。本月总共有147个组织/企业遭遇勒索攻击，其中包含中国2个组织/企业在本月遭遇了双重勒索/多重勒索。

|  |  |  |
| --- | --- | --- |
| RRD | Division-D | chervongroup.com |
| XAL | AKIJ GROUP | Atlantic Asphalt |
| Cle | Iwis Group | Maple Lodge Farms |
| DURA | www.paw.eu | Northern Contours |
| EDSI | Gardenworks | Thomson Broadbent |
| STIMM | bayview.com | Bank of Indonesia |
| Subex | Fdcbuilding | harrisshelton.com |
| izo.es | snapmga.com | centralbankfl.com |
| PLACON | bricofer.it | Mecanico Cairo SL |
| HAPOLO | supersave.ca | onlinesalespro.com |
| Arcese | bernheim.org | Hall Cross Academy |
| joda.de | Abdi ibrahim | JALEEL TRADERS LLC |
| ipec.ro | cbibanks.com | fairnessforall.com |
| RIVADIS | NORDFISH SRL | Perennials Fabrics |
| UNICRED | Little Giant | Imperial Logistics |
| Moncler | rightsys.com | lee-associates.com |
| CSEG.CN | aulss6.veneto.it | huntsville4rent.com |
| 48Forty | elitemate.com | salesiancollege.com |
| Arc Com | elmonterv.com | themisautomation.com |
| Sectrio | saintcloud.fr | Vehicle Service Group |
| Optionis | ambau-team.de | Lyon-Waugh Auto Group |
| estpm.fr | optimissa.com | Lewis & Clark College |
| Mtlcraft | mfkmakina.com | lhotellerie-restauration.fr |
| Redbadge | Acuity Brands | northsideplumbing.com |
| Hensoldt | Hanon Systems | securiteassurance.com |
| Regulvar | amerplumb.com | girlguidinglaser.org.uk |
| Mab Group | Amaveca Salud | independentprinting.com |
| efile.com | FrenchGourmet | Butler Community College |
| Safeguard | Weldco Beales | CIG de la Grande Couronne |
| Superfund | empireins.com | SAVANNAH State University |
| TaxNetUSA | Claro Colombia | The City of Pembroke Pines |
| Delinebox | bannerbuzz.com | The Public Safety Credit Union |
| Ezz Steel | Brookson Group | Cree Nation of Waskaganish |
| Huhtamaki | khattarlaw.com | 東京コンピュータサービス |
| aquila.ch | Detroit Stoker | Creative Liquid Coatings INC |
| BainUltra | mcsmorandi.com | Carthage R-9 School District |
| CED Group | Summit College | Premium Transportation Group |
| NanoFocus | Visit Montréal | PAUL BEUSCHER PUBLICATIONS |
| KCA Deutag | plainviewmn.com | Rafael Advanced Defense Systems |
| justice.fr | Shutterfly inc. | ASL Napoli 3 Sud Network Seized |
| heubeck.de | Polen Implement | Butler County Community College |
| laponte.it | Info-Excavation | The Grand Bahama Port Authority |
| vbhlaw.com | thalesgroup.com | Union County Utilities Authority |
| isnardi.it | grupomakler.com | Caribbean Broadcasting Corporation |
| AFG Canada | Florida lawyer‘s | Western Information Management Inc |
| D.F. Chase | Airspan Networks | Durham Cathedral Schools Foundation |
| Strongwell | kentkonut.com.tr | UTC Uniformes Town & Country Inc, Les |
| U.FORM SRL | crossroadshealth | Centre D'Odontologia Integrada Miret-Puig |
| atsair.com | torann-france.fr | NASS USA North American Substation Services |

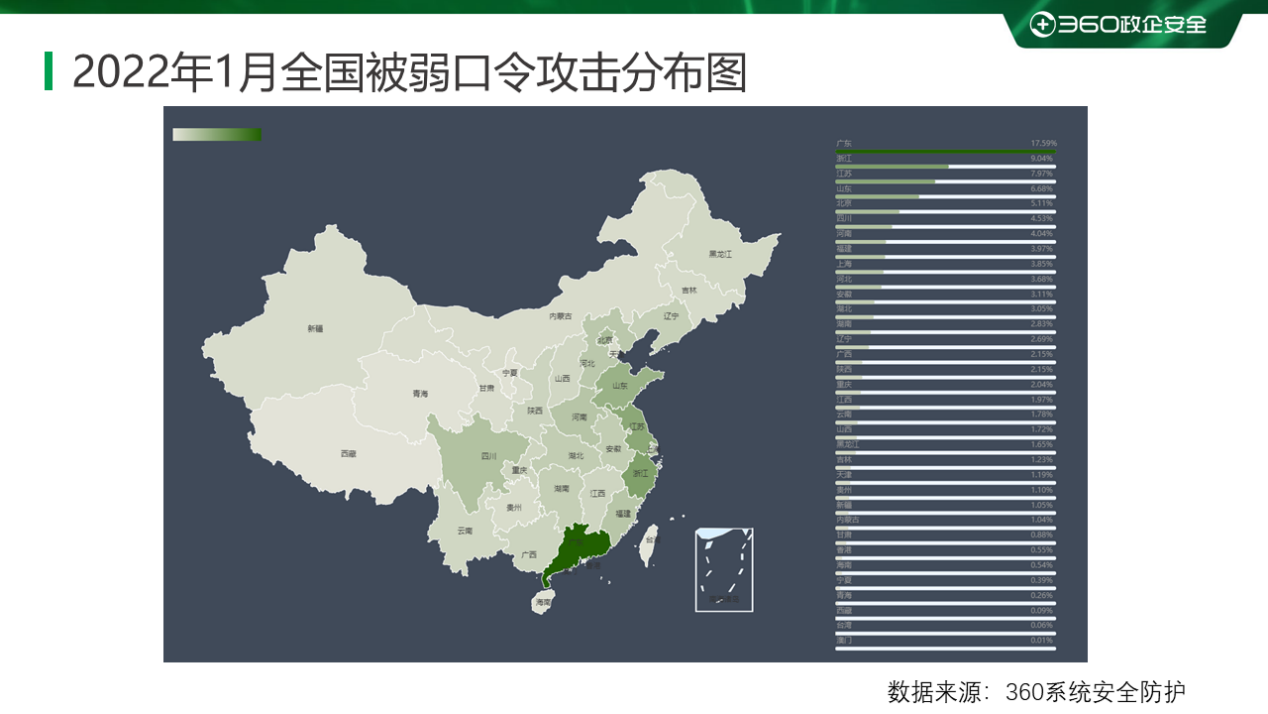
表格2.受害组织/企业

## 系统安全防护数据分析

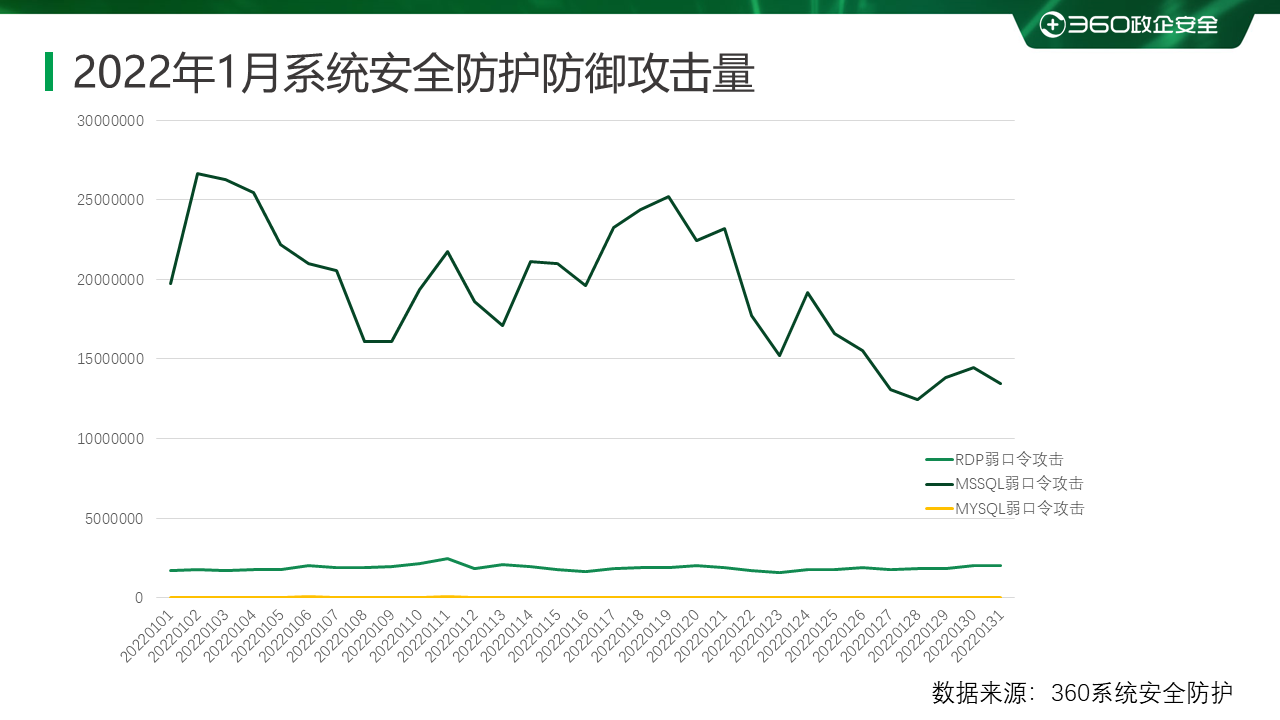
通过将2022年1月与2021年12月的数据进行对比，本月各个系统占比变化均不大，位居前三的系统仍是Windows 7、Windows 8和Windows 10。



以下是对2022年1月被攻击系统所属地域采样制作的分部图，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。



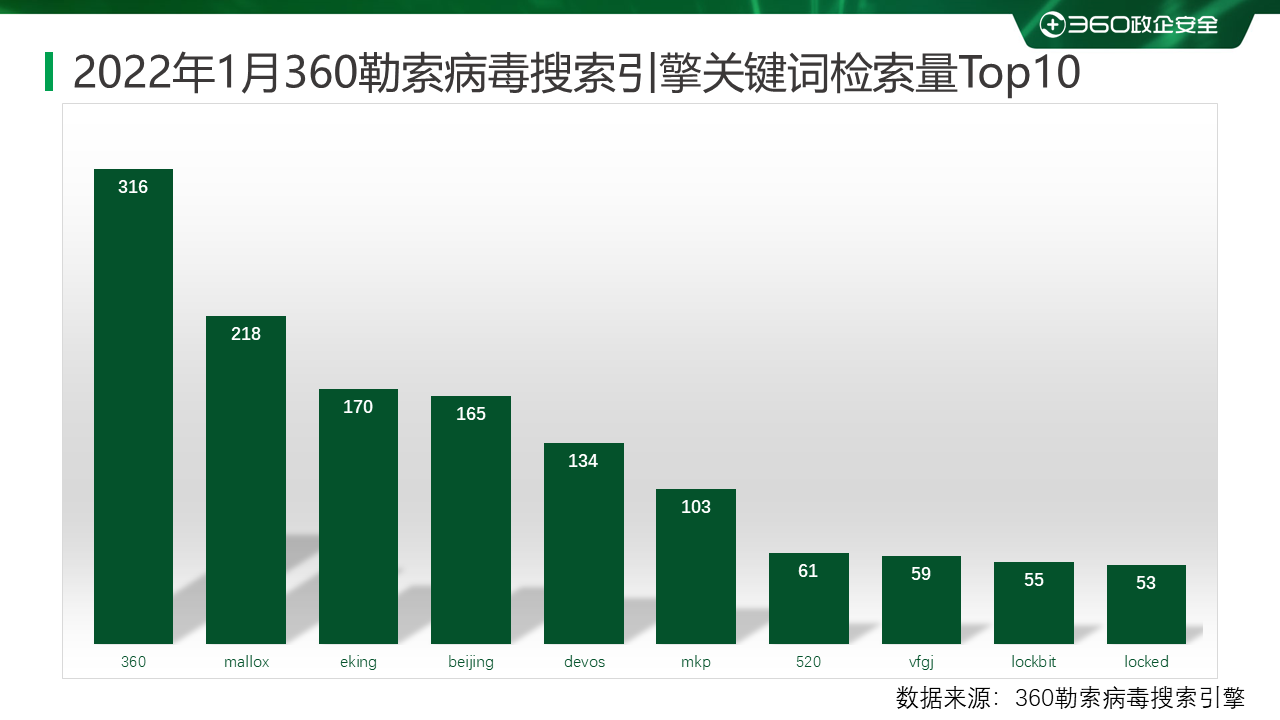
通过观察2021年12月弱口令攻击态势发现，RDP弱口令攻击和MYSQL弱口令攻击整体无较大波动。MSSQL弱口令攻击虽有波动，但无大的变动，整体呈下降态势。



## 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。

* 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。
* mallox:属于Mallox勒索病毒家族，由于被加密文件后缀会被修改为mallox而成为关键词。通过SQLGlobeImposter渠道进行传播。此外360安全大脑监控到该家族本月还通过匿影僵尸网络进行传播。
* 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。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。
* beijing：同360 。
* 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。
* mkp：属于Mako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。
* 520：属于BeijngCrypt勒索病毒家族，由于被加密文件后缀会被修改为520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。
* vfgj:属于Stop勒索病毒家族，由于被加密文件后缀会被修改为vfgj而成为关键词。该家族的主要传播方式为：通过伪装成破解软件或者激活工具诱导用户下载运行进行传播。
* LockBit：LockBit勒索病毒家族，由于被加密文件后缀会被修改为lockbit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。
* 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。



解密大师

从解密大师本月解密数据看，解密量最大的是Sodinokibi，其次是GandCrab。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。

