# 2022 年 4 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，为需要帮助的用户提供 360 反勒索服务。

2022 年 4 月，全球新增的活跃勒索病毒家族有:Onyx、Industrial Spy、BlackBasta、Pipikaki、BlockZ、Phantom、Blaze 等家族，其中 Onyx、Industrial Spy、BlackBasta 均为双重勒索勒索病毒家族。

本月最值得关注的有三个热点：

一、Magniber 勒索病毒再次活跃，大量用户因下载伪装成 windows 10 的更新程序导致文件被加密。

二、新型勒索病毒 Onyx 勒索病毒对大文件进行直接销毁。

三、风力涡轮机公司 Nordex、Snap-on 遭遇 Conti 勒索团伙攻击，同时发现已经黑客利用泄露的 Conti 源码攻击俄罗斯公司。

四、美国牙科协会受到 Black Basta 勒索病毒攻击。

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。

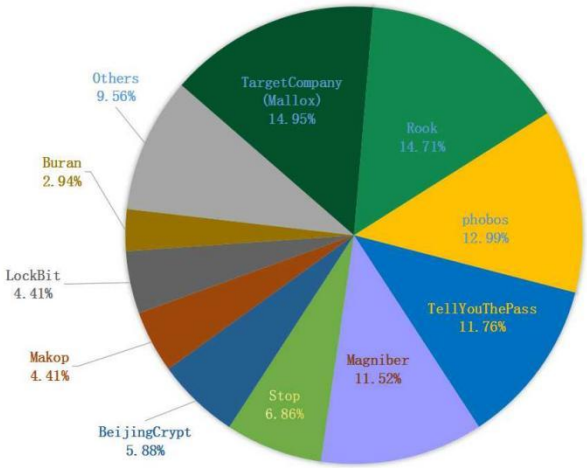
## 感染数据分析

针对本月勒索病毒受害者所中勒索病毒家族进行统计，TargetCompany(Mallox)家族占比 14.95%居首位，其次是占比 14.71%的 Rook，phobos 家族以 12.99%位居第三。

本月传播排名前五的家族，分别采用了不同的传播方式。勒索病毒多样化的同时，传播渠道也在多元化。其中：

- TargetCompany(Mallox)通过暴力破解成功获取数据库口令后、下发远程工具投毒或直接下发勒索病毒，同时具备内网横向移动能力。
- Rook 利用携带恶意代码的第三方软件进行传播，
- Phobos 利用暴力破解远程桌面口令后投毒。
- TellYouThePass 利用多种 Nday 漏洞进行传播。
- Magniber 利用网页挂马，伪装成升级软件等方式进行传播。

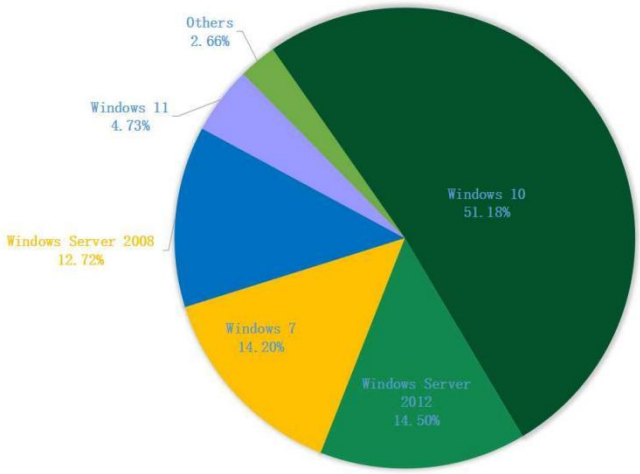
## 2022年4月反勒索服务处置勒索病毒家族占比




数据来源：360反勒索服务

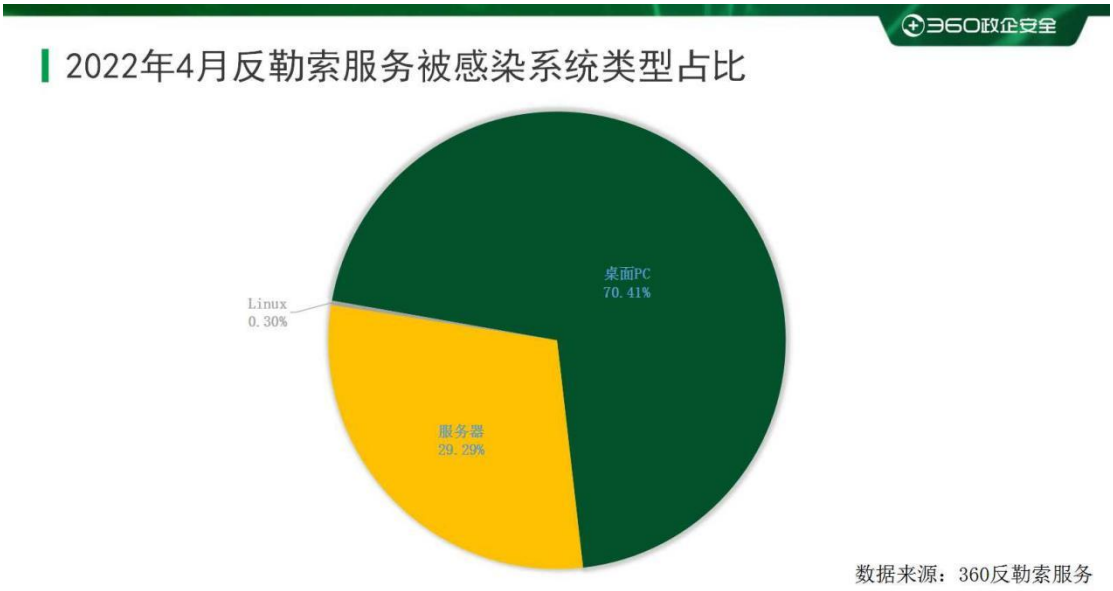
对本月受害者所使用的操作系统进行统计，位居前三的是：Windows 10、Windows Server 2012 以及 Windows 7。

## 2022年4月受勒索病毒影响操作系统占比




数据来源：360反勒索服务

2022 年 4 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。




# 勒索病毒疫情分析

## Magniber 伪装成 Windows 10 升级包进行传播

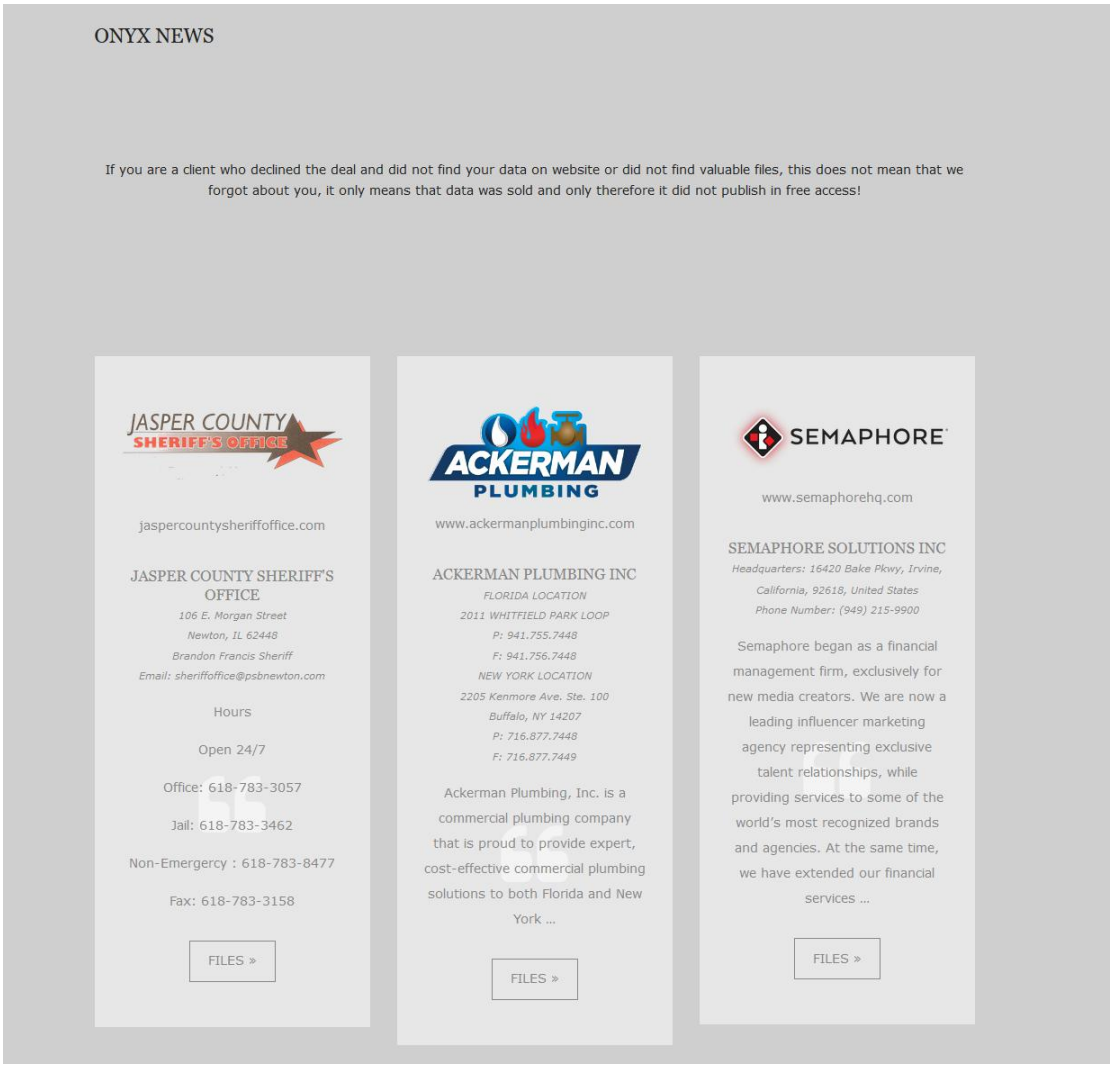
360 安全大脑在 4 月底监控到 Magniber 再次活跃，此次传播不仅利用利用之前的网页挂马，还通过伪装成 Windows 10 升级包诱导用户下载运行。通常受害者是通过论坛、破解软件网站等地方下载文件时跳转到第三方云盘。下载时通常会下载到一个 Windows 10 升级包，还可能会跳转到色情、广告、购物等网站。


被该勒索病毒加密后，文件后缀为随机后缀，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 天内支付赎金只需支付 0.075 个比特币(约等于人民币 18244 元)，超过 5 天赎金将会翻倍。360 安全大脑曾对受害者进行采样跟踪，发现该家族的支付率极低，180 个受害者中仅 1 个受害者支付赎金。

## 新型勒索病毒 Onyx 勒索病毒对大文件进行直接销毁。

新型勒索病毒 Onyx 目前正在广泛传播，其会直接对大文件进行破坏而非加密。这样，即使受害者支付了赎金也无法解密这些被破坏的文件。

与目前大多数勒索病毒一样，Onyx 作者会在加密文件之前从其设备中窃取数据。而这些数据会被用于双重勒索计划——如果不支付赎金，他们便会威胁要公开发布这些敏感数据。目前为止，该勒索病毒团伙已经在其网站上泄露了 6 所机构的数据，其中 5 所出自美国。



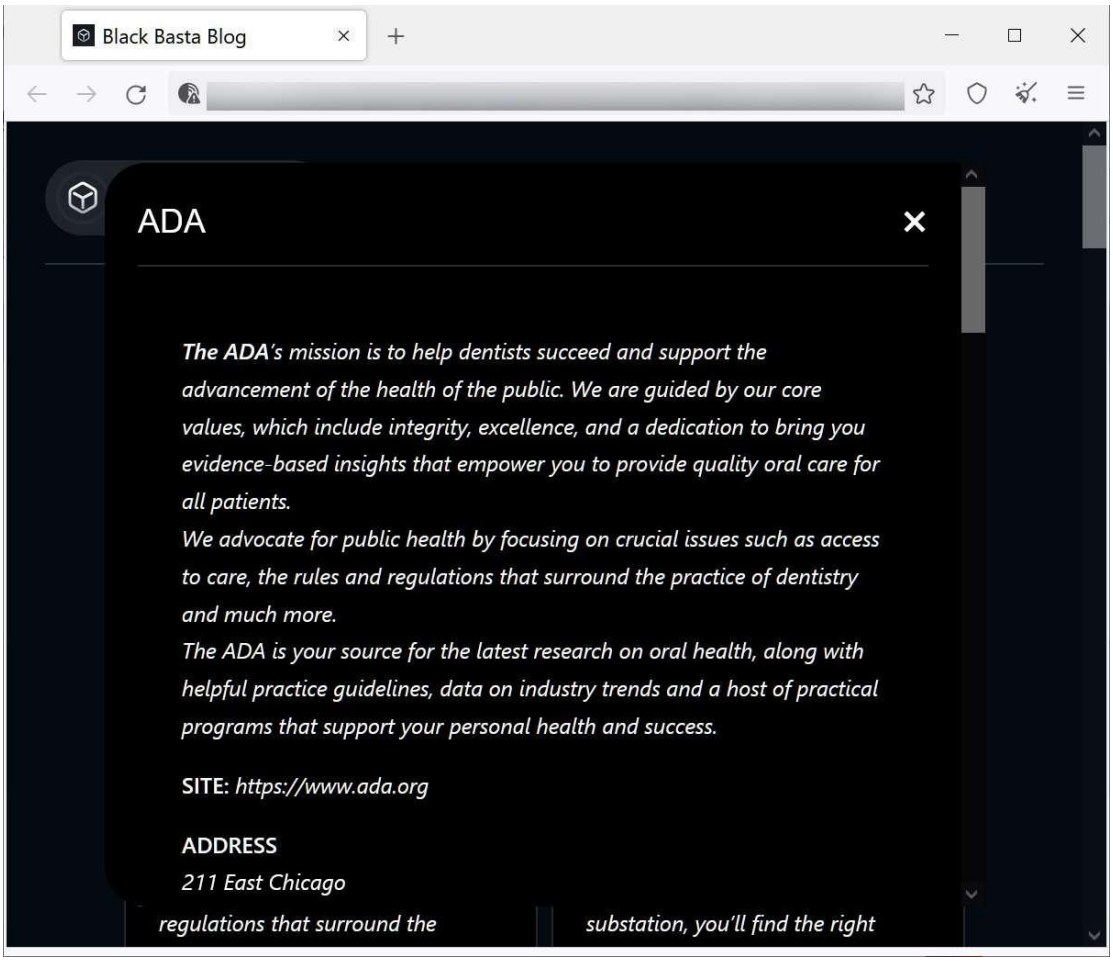

但在加密方面，该勒索病毒的手段则比较“独特”。其会加密文件大小小于 200MB 的文件，但会对大于 200MB 的文件用随机的垃圾数据覆盖其内容，而不是对其进行加密。由于这只是随机创建的数据，因此包括攻击者在内，任何人都无法解密这些被破坏的大文件。即使受害者支付赎金，也只有可能恢复较小的加密文件。

基于源码进行分析，该功能并非编程错误，而是病毒作者有意为之。因此，建议受害者不要支付赎金。

## 美国牙科协会受到 Black Basta 勒索病毒攻击

4 月 22 日，美国牙科协会（ADA）遭受了网络攻击，迫使被攻击的服务器下线。此次攻击严重干扰了其各种在线服务、电话、电子邮件和网络通信等功能。ADA 网站目前仅显示一条公式，表明他们的网站正在努力恢复系统运行。

目前，一个名为 Black Basta 的新型勒索病毒团伙声称对此次攻击事件负责，并已经开始泄露据称是在 ADA 攻击期间窃取到的数据。该团伙的数据泄露网站声称已经泄露了大约 2.8 GB 的数据，同时其还指出这是攻击中被盗数据的 30%。这些数据包括 W2 表单、NDA、会计电子表格以及数据泄漏页面上共享的屏幕截图中有关 ADA 的会员信息。




## Conti 团伙未受源码泄露影响，对多个公司发起勒索攻击

Conti 勒索团伙在俄乌冲突爆发后，内部数据遭到多次泄露，其中包括勒索病毒源代码。近日一名为 NB65 的黑客组织利用 Conti 泄露的勒索病毒源代码创建了自己的勒索病毒，并用于针对俄罗斯组织的网络攻击，窃取他们的数据并将其泄露到网上，并声称这些攻击是由于俄罗斯入侵乌克兰造成的。目前声称受到黑客组织攻击的俄罗斯实体包括文件管理运营商 Tensor、俄罗斯航天局 Roscosmos 和国有的俄罗斯电视和广播电台 VGTRK 等。

Conti 勒索团伙并并未受到数据泄露事件影响，仍在不停的发起勒索攻击，例如：

1. 4 月初，Conti 勒索病毒声对风力涡轮机巨头 Nordex 发起勒索攻击，此次攻击时间导致该公司被迫关闭其 IT 系统同时禁用了对其设备的远程访问权限。
2. 2022 年 4 月 7 日，Snap-on 在其网络中检测到可疑活动后披露了此次数据泄露事件，这导致他们关闭了所有系统一边进行检查和维护。在进行调查后，Snap-on 发现攻击者在 2022 年 3 月 1 日至 3 月 3 日期间就已经窃取了其员工的个人数据。
3. 在线零售和摄影平台 Shutterfly 公布了一起数据泄露事件，其声称此次事件是在遭到 Conti 勒索病毒攻击期间被后者窃取到了涉及员工信息的相关数据。据 Shutterfly 披露，由于勒索病毒攻击，其网络于 2021 年 12 月 3 日遭到入侵。在勒索病毒攻击期间，攻击者将获得了对公司网络的访问权，并成功窃取到了其中的数据和文件。

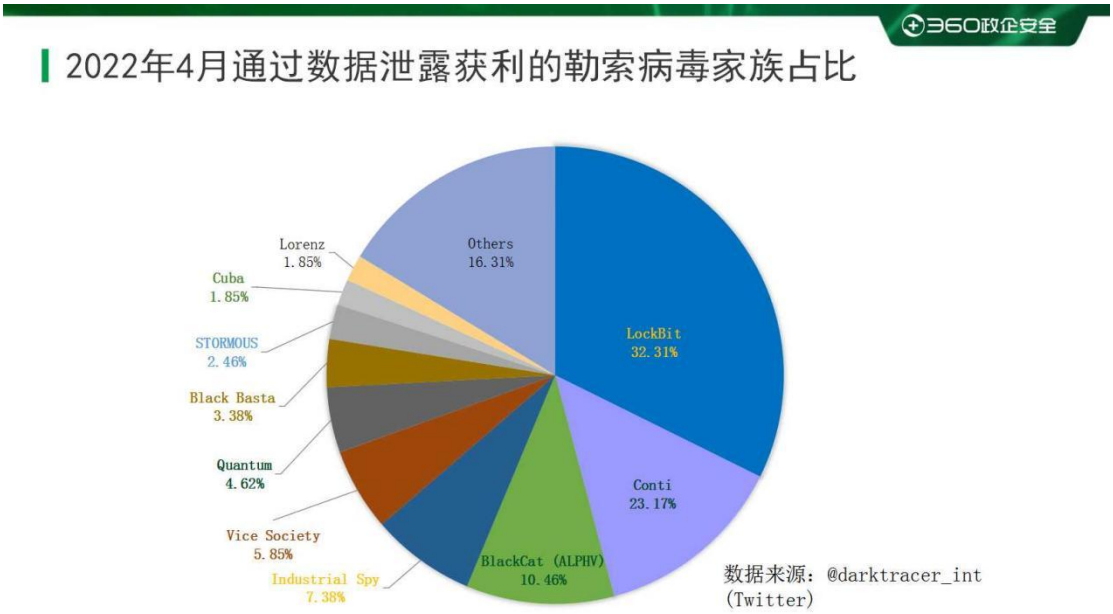
# 黑客信息披露

以下是本月收集到的黑客邮箱信息：

| | | |
|---|---|---|
| fcrecover@cock.li | fcsupport@mailfence.com | mallox@stealthypost.net |
| ironse2022@tutanota.com | 2022blue@mailfence.com | sparemail@onionmail.org |
| Starmoon@my.co | starmoonio@tutanota.com | deviceZz@mailfence.com |
| acookies@tutanota.com | acookies@onionmail.org | consult.raskey@tutanota.com |
| Starmoon@my.com | avos@thesecure.biz | avos@mail2tor.com |
| maxoll@tutanota.com | maxoll@onionmail.org | restoremanager22@onionmail.org |
| Gotoworld@tutanota.com | Gotogoto2020@mailfence.com | consult.raskey@onionmail.org |
| starmoonio@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，该数据仅包括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 325 个组织/企业遭遇勒索攻击，其中包含中国 5 个组织/企业在本月遭遇了双重勒索/多重勒索。

| | | |
|---|---|---|
| SLH | smp-corp.com | fazenda.rj.gov.br |
| IKPT | CAE Services | Maristes Hermitage |
| FCCH | noll-law.com | MAGNAR-EIKELAND.NO |
| Jasec | fec-corp.com | Tucker Door & Trim |
| Fycis | remar.com.ec | eNoah it solutions |
| Sonae | quito.gob.ec | azcomputerlabs.com |
| Dober | Est Ensemble | MARTINELLI GINETTO |

| | | |
|---|---|---|
| Henry | Attica Group | Favoris Holding AG |
| LACKS | Elgin County | Ragle Incorporated |
| Axxes | kdaponte.com | PhoenixPackagingPA |
| Jasec | valoores.com | multimmobiliare.ch |
| NECSUM | Metrobrokers | produitsneptune.com |
| ekz.de | wilshire.com | Morrie's Auto Group |
| in2.ie | NECSUM TRISON | cassinobuilding.com |
| mpm.fr | beckerlaw.com | get-greenenergy.com |
| DeeZee | Visotec Group | inglotcosmetics.com |
| Eminox | ssi-steel.com | farmaciastatuto.com |
| AIT.th | meijicorp.com | greenexperts.com.tw |
| Lowell | DJS associate | network-contacts.it |
| Hufcor | CJ Pony Parts | Boswell Engineering |
| Oralia | cyberapex.com | IMA Schelling Group |
| ekz.de | Simply Placed | produitsneptune.com |
| ksb.com | breadtalk.com | Stratford University |
| Del Sol | Success Neeti | Simonson-Lumber Inc. |
| iar.com | Wocklum Group | Abrams & Bayliss LLP |
| JetStar | genieroute.be | ght-coeurgrandest.fr |
| Advizrs | rosagroup.com | Concepts in Millwork |
| vgoc.ca | Keicorp(ICPM) | Delhi Heights School |
| Danaher | toothbuds.com | feuerschutzbockel.de |
| Mattlel | wiegaarden.dk | International Centre |
| ksb.com | Midea Carrier | Fonseca Supermarkets |
| xfab.com | SOGEGROSS SPA | Attica Holdings S.A. |
| Worksoft | sagefruit.com | Deutsche Windtechnik |
| Eurofred | fraunhofer.de | Stratford University |
| wenco.cl | MOTIVE-ENERGY | Mossbourne Federation |
| ALAM LMS | ALMANIE GROUP | DavislandscapeLTD.com |
| wania.at | cronos.com.ar | Musco Sports Lighting |
| LW Group | asp.messina.it | Wally Edgar Chevrolet |
| sep2.com | avion-tech.com | Frey and Winkler GmbH |
| FlipChip | Alliance Steel | Suhl. City in Germany |
| MANUFAST | premierbpo.com | Advantage Direct Care |
| WKPZ Law | enviroplas.com | Ackerman Plumbing Inc |
| For Peru | Gemeente Buren | Basler Versicherungen |
| Elgin_Ca | spirit-ord.com | Davis Law Group, P.C. |
| Al Bijjar | Keyano College | Mossbourne Federation |
| ambiq.com | westminster.de | North View Escrow Corp |
| procab.se | gva-atencia.es | baugeschaeft-boltin.de |
| tnmed.org | ledesma.com.ar | inland-engineering.com |
| Nordex SE | SSW Consulting | McKenzie Health System |
| ihbrr.com | Innotec, Corp. | allcountysurveying.com |

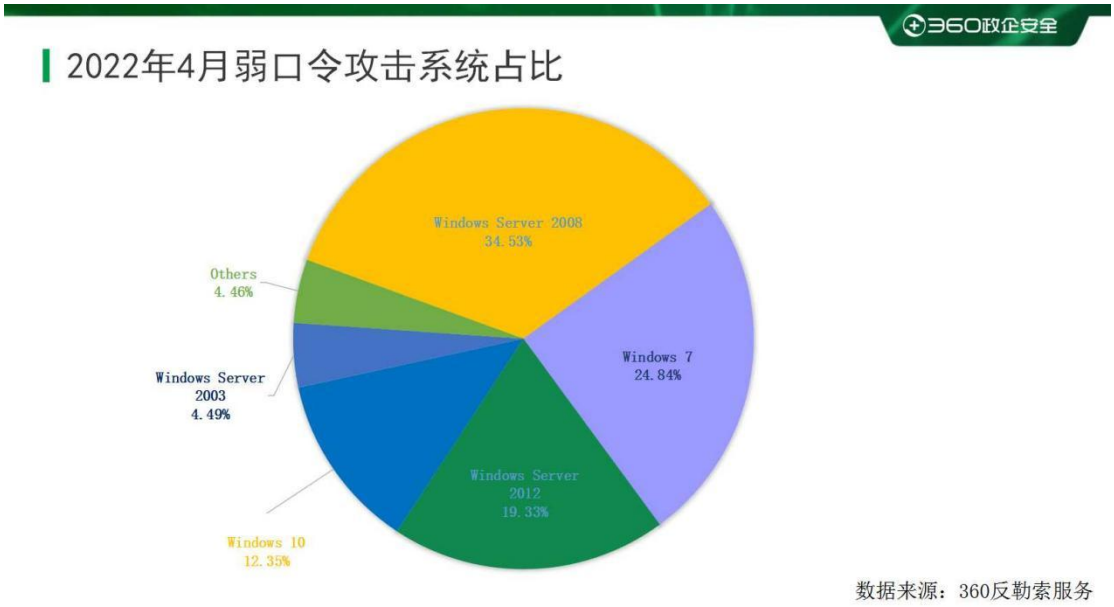
| | | |
|---|---|---|
| Tavistock | Valley Rentals | Woningcorporatie ZAYAZ |
| Broadleaf | Drive Products | Alimentos y Frutos S.A. |
| sadeco.fr | TÜV NORD GROUP | Agile Sourcing Partners |
| unholz.ch | LECHLER S.p.A. | empresariosagrupados.es |
| panasonic | schriesheim.de | hispanoamericano.edu.mx |
| a-r-s.com | simplilearn.net | Monterey Mechanical Co. |
| TRUSTFORD | huntongroup.com | Building Plastics, Inc. |
| CORFERIAS | keisei-const.jp | Semaphore Solutions Inc |
| FRISA.com | Cjk Group, Inc. | Schaumburg Park District |
| Coca-Cola | ijmondwerkt.com | enclosuresolutions.co.za |
| La Nación | radmangroup.com | soharportandfreezone.com |
| emucor.es | Newlat Food SPA | C&C FARMERS' SUPPLY CORP |
| Prophoenix | ruthtaubman.com | Alliant Physical Therapy |
| incegd.com | Trace Midstream | La SCP MOREAU & ASSOCIÉS |
| lekise.com | liceu.barcelona | lifestylesolutions.org.au |
| ingesw.com | hydromaxusa.com | alfa-finrase Crypto Rusia |
| Secova Inc | ospreyvideo.com | compagniedephalsbourg.com |
| daumar.com | simplilearn.net | oldenburgdeurbewerking.nl |
| jannone.it | innotecgroup.com | Prima Sole Components Spa |
| PERBIT.COM | PT Pertamina Gas | lifestylesolutions.org.au |
| e-pspl.com | AM International | Mercadocar Mercantil Ltda. |
| NuLife Med | groupe-corbat.ch | Camden City School District |
| tpdrug.com | polyplastics.com | Basra Multipurposr Terminal |
| applya.com | Elevate Services | clinique.cob-osteopathie.fr |
| lerros.com | Wolfe Industrial | Avamere Family of Companies |
| tgs.com.ar | SUPREME SERVICES | Grosvenor Engineering Group |
| ardeche.fr | gordoncounty.org | glenbrookautomotivegroup.com |
| Metagenics | Enoah Isolutions | United States of America GOV |
| bet9ja.com | ascotlloyd.co.uk | TIC International Corporation |
| goldbet.it | GIBSON HomeWares | Dennis Gartland And Niergarth |
| rnrinc.com | CASTGROUP.COM.BR | Tehama County Social Services |
| eksltd.com | M+R SPEDAG GROUP | Plauen Stahl Technologie GmbH |
| FRANSABANK | Autumn Transport | Barakat Travel and Private Jet |
| huesser.ch | 7generations.org | Standard Building Supplies Ltd |
| Prophoenix | GOLDENDUCK GROUP | Jiangsu Kaili Carpet Co., Ltd. |
| incegd.com | Stratton Finance | Associazione Bancaria Italiana |
| ccfsinc.com | warrengibson.com | Domingues and Pinho Contadores |
| tvothai.com | j-w-anderson.com | heartlandhealthcareservices.com |
| racsa.go.cr | innotecgroup.com | Instituto Meteorológico Nacional |
| reitzner.de | Co-opbank Pertama | Florida International University |
| 888VOIP.COM | www.tigergroup.ae | Barwick Bathroom Distribution LLP |
| MILLS GROUP | Calvetti Ferguson | Pacific Maritime Industries Corp. |
| Auction.com | fazenda.rj.gov.br | Centre Hospitalier de Castelluccio |

| | | |
|---|---|---|
| cos.rmb.com | Reckitt Benckiser | Confcommercio - Alessandria - Home |
| consfab.com | www.oil-india.com | Centre Hospitalier de Castelluccio |
| kpcg.com.hk | mdindiaonline.com | North Carolina A&T State University |
| Atlas Copco | verifiedlabel.com | WAYNE FAMILY PRACTICE, ASSOC., P.C. |
| scoular.com | Hi Tech HoneyComb | Levantina, Ingenieria y Construccion |
| DC ADVISORY | tokyo-plant.co.jp | SSK Ingeniería Y Construcción S.A.C. |
| bazzisrl.it | AFJCONSULTING.NET | Big Horn Plastering of Colorado, Inc. |
| Petro Serve | ORBITELECTRIC.COM | Laiteries Reunies Societe cooperative |
| The H Dubai | groupemeunier.com | Service Employees' International Union |
| ccfsinc.com | get-entkernung.de | Importador Ferretero Trujillo Cia. Ltda |
| kdaponte.com | Ackerman Plumbing | National Rehabilitation Training Center |
| valoores.com | studiobrazzale.it | Small Industries DevelopmentBank of India |
| Metrobrokers | Co-opbank Pertama | LARON an otp industrial solutions company |
| wilshire.com | www.tigergroup.ae | Ministerio de Hacienda - República de Costa Rica |
| Attica Group | unWired Broadband | Calvetti Ferguson |
| diasorin.com | | |

表格 2. 受害组织/企业

# 系统安全防护数据分析

360 系统安全产品，针对服务器进行全量下发系统安全防护功能，针对非服务器版本的系统仅在发现被攻击时才下发防护。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 2012。




对 2022 年 4 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。


数据来源：360系统安全防护

通过观察 2022 年 4 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。


数据来源：360系统安全防护

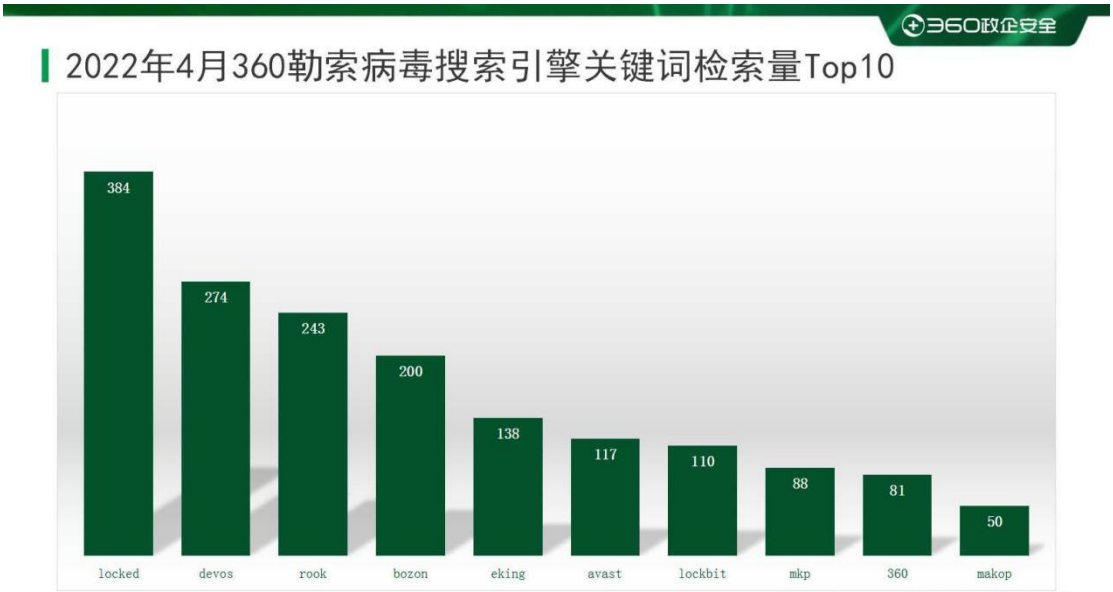
# 勒索病毒关键词

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。

- 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。
- 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。
- 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。

- bozon:属于 TargetCompany(Mallox)勒索病毒家族，由于被加密文件后缀会被修改为 bozon。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。
- 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。
- Avast：同 bozon。
- lockbit:属于 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。被该家族加密还可能涉及数据泄露的风险，该家族有一个大型团伙，其攻击手法多样化，不仅仅局限于弱口令爆破，还包括漏洞利用，钓鱼邮件等方式进行传播。
- 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。
- 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。

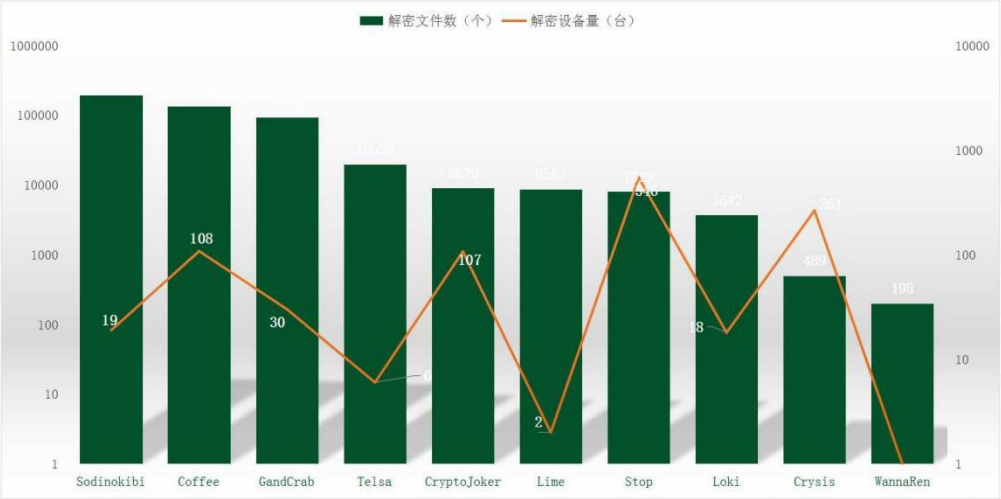



数据来源：360勒索病毒搜索引擎

# 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 Coffee。使用解密大师解密文件的用户数量最高的是被 Stop 家族加密的设备，其次是被 Coffee 家族加密的设备。

## 2022年4月解密大师解密量




数据来源：反勒索服务统计数据