2022 年 12 月勒索软件流行态势分析

勒索软件传播至今，360 反勒索服务已累计接收到上万勒索软件感染求助。随着新型勒索软件的快速蔓延，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。勒索软件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 安全大脑针对勒索软件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 12 月，全球新增的活跃勒索软件家族有:Seoul、Lucknite、Blocky、HentaiLocker 等家族。本月没有新增双重勒索软件家族，但 Mallox 勒索软件家族从本月开始在暗网公布受害者数据，目前已对外公布 5 个受害组织或企业的数据。

以下是本月值的关注的部分热点：

一、TellYouThePass 勒索软件再次对国内 OA 服务器发起攻击。

二、以比利时市政部门为目标的勒索软件团伙实际攻击了警察系统。

三、勒索软件攻击迫使法国医院转移病人。

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

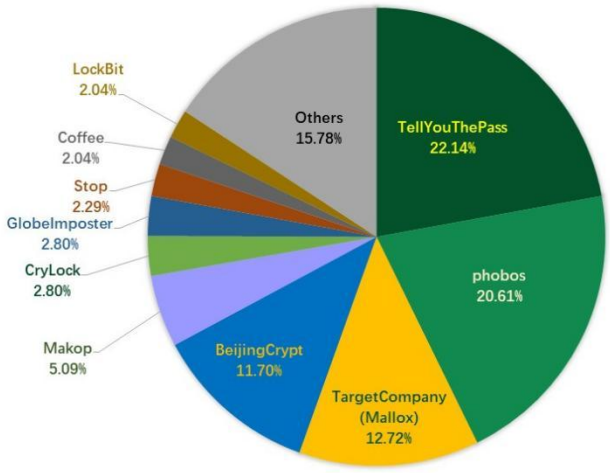
针对本月勒索软件受害者所中病毒家族进行统计：TellYouThePass 家族占比 22.14%居首位，其次是占比 20.61%的 phobos，而 TargetCompany(Mallox)家族则以 12.72%位居第三。

TellYouThePass 勒索软件在最近一年异常活跃，本月中旬，其再次使用高危漏洞，攻击国内 OA 服务器。攻击共持续约 16 小时，造成大量安全防护不当，未打补丁的机器感染该家族勒索软件。

TargetCompany(Mallox)勒索软件今年也动作频频，近期我们监测到，该家族开始在其网站公开被攻击者数据，目前已公布了 5 个受害组织或企业的数据。若受害者收到的勒索提示信息中包含暗网地址，那么可能遭到了数据窃取攻击。若只是邮箱，则有较大概率未被窃取数据。

本月 TOP10 家族中的 CryLock 家族，我们监测到其传播团伙已将它重命名为 Trigona，并建立了独立的赎金谈判网站。

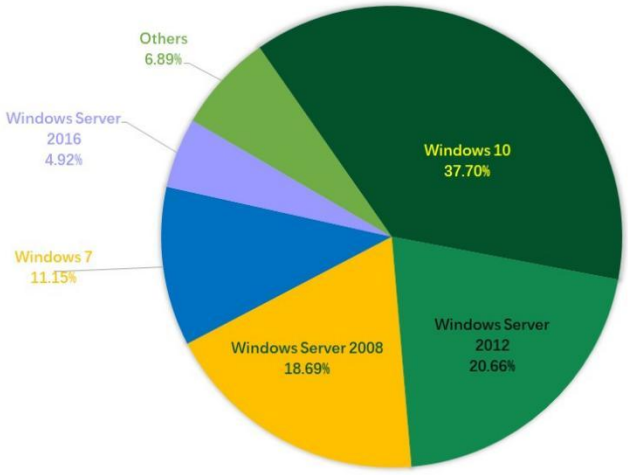
2022年12月反勒索服务处置勒索病毒家族占比



数据来源：360反勒索服务

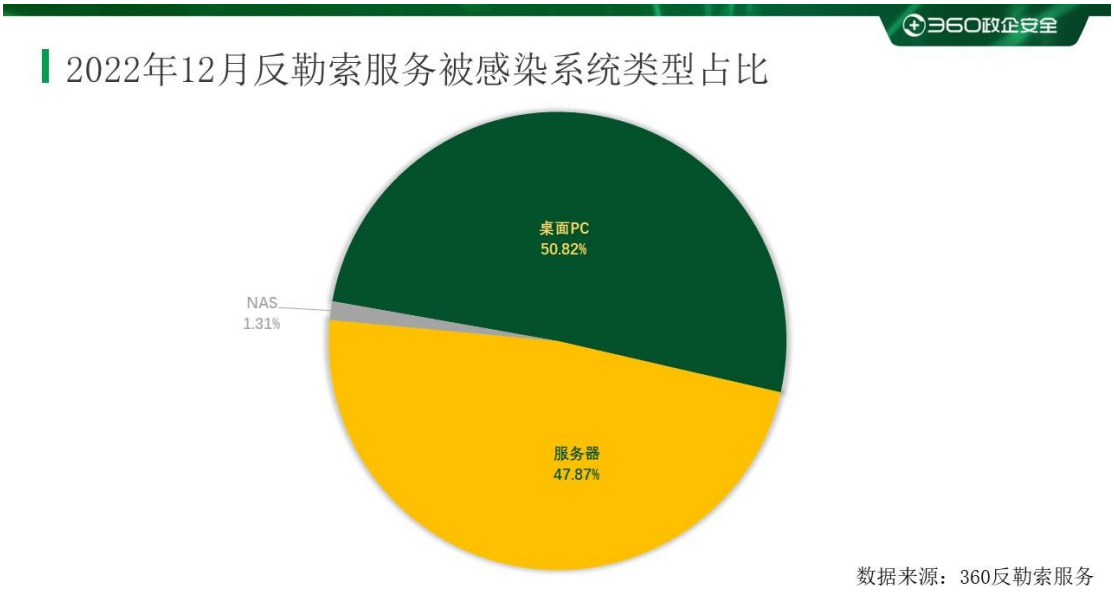
对本月受害者所使用的操作系统进行统计，位居前三的是：Windows 10、Windows Server 2012 以及 Windows 2008。

2022年12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 12 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。



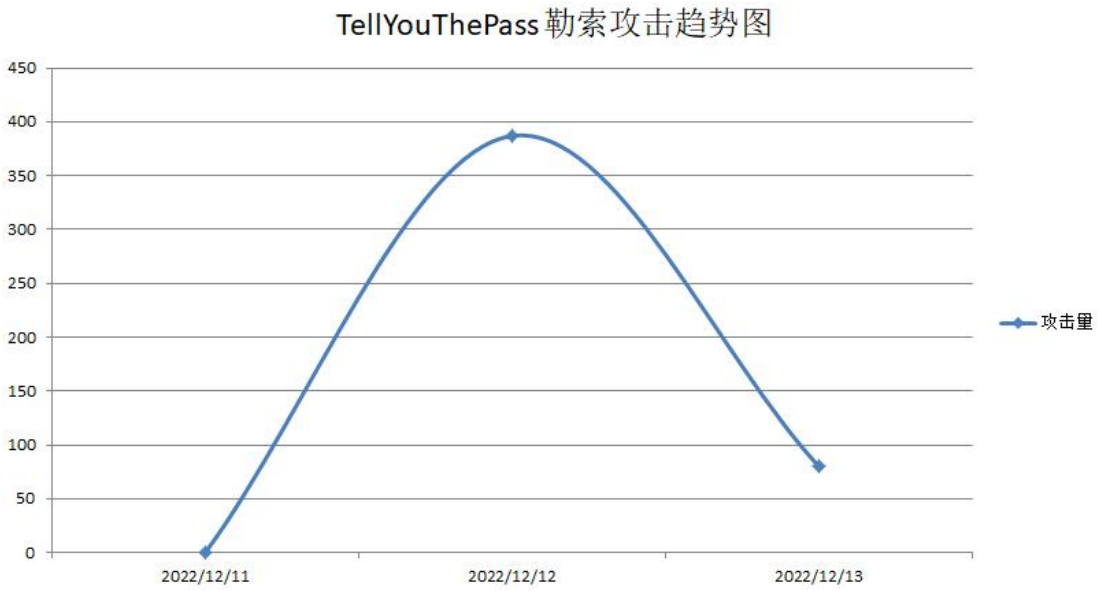
勒索软件疫情分析

TellYouThePass 勒索软件再次对国内 OA 服务器发起攻击

本月，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)监测到 Tellyouthepass 勒索软件利用多个漏洞进行入侵攻击，包括 Atlassian Confluence OGNL 注入漏洞 CVE-2022-26134、用友(Yonyou) GRP-U8 /UploadFileData 接口任意文件上传漏洞、用友(Yonyou) NC accept 接口文件上传漏洞、用友(Yonyou) NC NCInvokerServlet 接口任意代码执行漏洞、致远 OA 漏洞等。

攻击者在 12 月 12 日至 13 日持续发起批量攻击。最早监测到的攻击是在 2022 年 12 月 12 日凌晨 02:31:43，而最近一次攻击则是发生在 2022 年 12 月 13 日 18:47。利用 Web 漏洞入侵后，攻击者直接利用 Web 宿主进程（如 java.exe）进行对系统进行加密并提出勒索。该勒索软件家族通常通过漏洞利用批量扫描进行攻击，受影响较大的是存在 Web 漏洞且对外网映射的服务器。

Tellyouthepass 勒索软件已经不是第一次利用高危漏洞发起攻击：早在 2020 年该家族就已利用永恒之蓝漏洞攻击多个目标，而 2021 年其再次利用 Apache Log4j2 远程代码执行高危漏洞(CVE-2021-44228)攻击了多个目标。

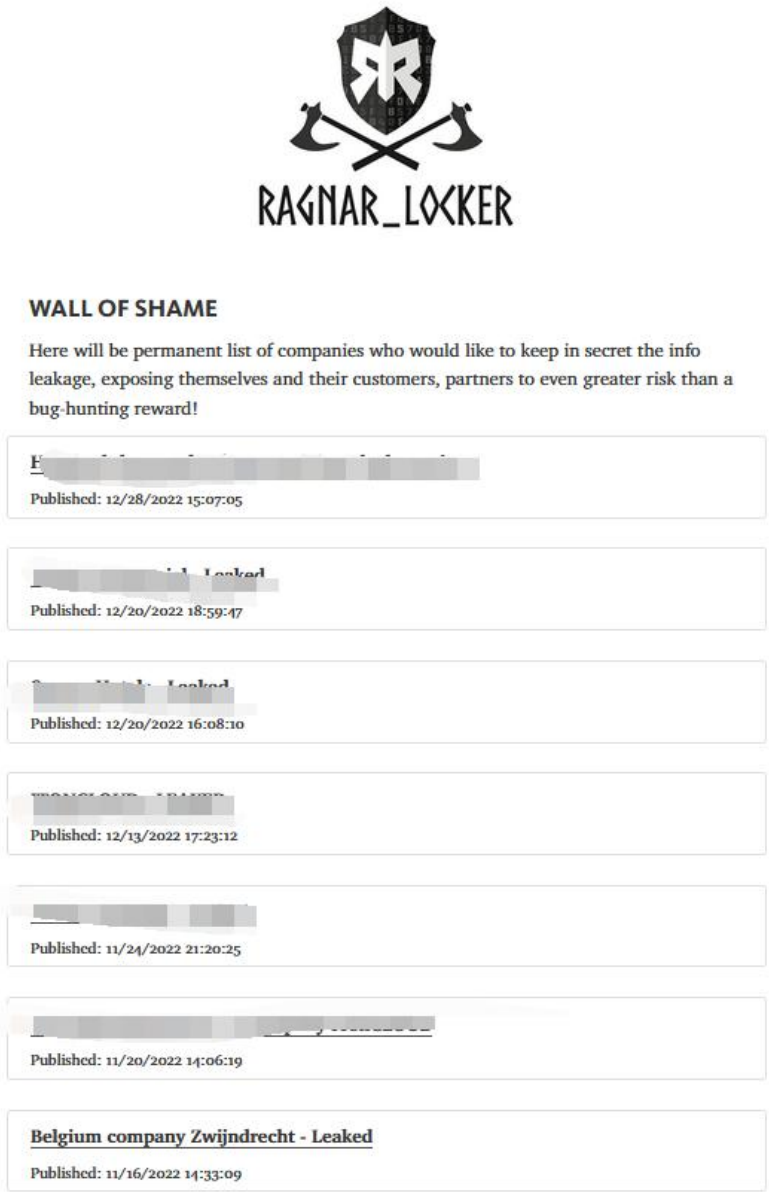


以比利时市政部门为目标的勒索软件团伙实际攻击了警察系统

Ragnar Locker 勒索软件团伙发布了他们认为是窃取自比利时兹维因德雷赫特市的数据，但事实证明是从比利时安特卫普警察部门兹维因德利赫特警察局所窃取到的数据。

据报道，泄露的数据暴露了数千辆汽车牌照、罚款、犯罪报告文件、人员详情、调查报告等信息。而这类数据可能会暴露举报犯罪或虐待的举报人员隐私信息，并可能危及正在进行的执法及调查行动。

比利时媒体称此次数据泄露是此类事件中影响该国公共服务的最大事件之一，暴露了兹维因德利赫特警方从 2006 年至 2022 年 9 月保存的所有数据。



勒索软件攻击迫使法国医院转移病人

位于巴黎郊区的安德雷·米格诺教学医院因 12 月 3 日晚发生的勒索软件攻击，不得不关闭其电话和电脑系统。

据称，这起勒索软件事件背后的攻击者已经要求赎金。但院方并不打算支付。

目前，医院已取消了部分手术。据法国卫生与预防部长弗朗索瓦·布劳恩表示，院方还被迫将 6 名患者从新生儿和重症监护室转移到其他医疗机构。

负责数字转型和电信的部长代表让·诺埃尔·巴罗表示，医院已隔离了受感染的系统来限制勒索软件向其他设备的传播，并向法国国家信息系统安全与防御局（ANSSI）发出了警报。

黑客信息披露

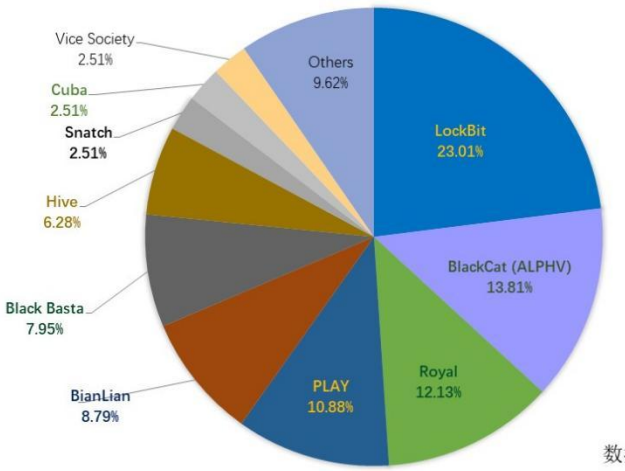
以下是本月收集到的黑客邮箱信息：

textmeforhelp@tutanota.com	localfix@waifu.club	hell0s1@tutanota.com
hell0s@tutanota.com	Trustmebb@keemail.me	Falcon360@cock.li
Forbitlog@privatemail.com	rast@airmail.cc	HashTreep@waifu.club
acbc@tutanota.com	hel.b22@tutanota.com	d0ntw0rry@cyberfear.com
midnight@email.tg	hel.b22@tutanota.com	hell0s@0day.im
acbc@tutanota.com	WARNING@cyberfear.com	sunhuyvchay@messagesafe.io
leonardoboss@onionmail.org	gichugre@tfwno.gf	ekingm2023@outlook.com
back2restore@tutanota.com	back2restore@neomainbox.ch	ekingm2023@onionmail.org
dark_day@cyberfear.com	midnight@email.tg	guan_yu@zohomail.com
writehelp@privatemail.com	gardex_recofast@zohomail.eu	hell0s@0day.im
ingnatnat@tutanota.com	annawong@onionmail.org	service@hellowinter.online
datarecoveryasia@msgsafe.ninja	slect@tutanota.com	Create0day@proton.me
create0day@onionmail.org	hpsupport@privatemail.com	KOKO8@QQ.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软件家族越来越多，勒索软件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软件家族占比，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）。

2022年12月通过数据泄露获利的勒索病毒家族占比



数据来源：@darktracer_int(Twitter)

以下是本月被双重勒索软件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 239 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。其中有 12 个组织/企业未被标明，因此不再以下表格中。

sickkids.ca	hacla.org	QUT
Centro Médico Virgen De La Caridad	AONTTAGL	presco.com
Camst Group	amundson.co.nz	Iowa Public Television
Waterloo Wellington Flight Centre	CPTM	St. Rose Hospital
MITCON Consultancy & Engineering Services	PANOLAM	portodelisboa.pt
ELOTECH	JAKKS Pacific, Inc.	SUMITOMO BAKELITE USA
NO LIMIT MARINE	Emoney	AOAL - Azienda Ospedaliera di Alessandria
Einatec	Centro Turistico Giovanile	ET GLOBAL
Square Yards	TCL Chinese Theatres	Trubee, Collins & Co
www.buildersmutual.com	INTRADO	Inforlandia
HELMA Eigenheimbau AG	Grupo Ibiapina Ltda	pu.edu.lb
FARMS.COM	CR&R	Meyer & Meyer Holding SE & Co. KG
SSI Schäfer Shop	Empresas Públicas de Medellín	Fantasy Springs Resort Casino
Robinson Pharma	STRESSER ASSOCIATES CPA	BroadvisionGroup
Atlatec SA de CV	Republic of Vanuatu	aristopharma.com
excentiahumanservices.org	Myofficeplace Inc.	SEMITEC Corporation
pro office Büro + Wohnkultur GmbH	Bregman Berbert Schwartz & Gilday	Protecmedia

bavelloni.com	Aegea Group companies	Rech Informatica Ltda
Strem Chemicals	thedonovancompany.com	maxionwheels.com
MHMR Authority Of Brazos Valley	SIRIUS SHIPPING	FURETANK
DONSONET	VAS	Alvaria
menziesaviation.com	smithsinterconnect.com	hildinganders.com
ATLAS	Interface	Zehnders of Frankenmuth
Wrapex Industrial	Serena Hotels	MARK-TAYLOR
City Of Huntsville, Texas	North Idaho College	Innovative Education Management
Dixons Allerton Academy	Sae-a	Xavier University of Louisiana
Keralty	Stolle Machinery	JAKKS Pacific Inc
Monte Cristalina S.A.	jka.co.uk	mayflowerdentalgroup.com
agriobtentions.com	womgroup.com	rgvfirm.com
stmc.edu.hk	polyflor.co.nz	businesscentral.org.nz
catalyst-group.co.nz	accuro.co.nz	mercuryit.co.nz
senateshj.com	OPUS IT Services	H-Hotels
Cervecería Regional	Creta Farm	Conform
st-group.com	Australian Real Estate Group Pty Ltd	The Exchange Bank
University Institute of Technology of Paris	TLC	Publicare
Mol	Arsat	JMicron
Universidade Catolica Portuguesa	Leo Hamel Fine Jewelers	UPONOR
Eureka Casino Resort	Emilio Sanchez American School	CIMT College
ZXP Technologies	Jeppesen	Sterling
Vincent Fister	mcft.com	Bailey Cavalieri LLC
Mark-Taylor	Expand Group	TEIJIN AUTOMOTIVE TECHNOLOGIES
Ban Leong Technologies Ltd	Petmate	ITONCLOUD
Pinnacle Communications	PARIC CORPORATION	Schnee Berger
Cetrogar	VFS	ENPPI
veolus.com	luxeprint.com.tw	sentecgroup.com
financierareyes.com.mx	dof.ca.gov	tdtu.edu.vn
rkfoodland.com	jieh.vn	amazing-global.com
k-toko.com	2networkit	Una Seguros
Antwerpen	REC Silicon	sushi-master.ru
KNOX College	dothousehealth.org	biotipo.com.br
koda.com.tw	Aeroproductsco	oltax.com
rhotelja.com	hawanasalalah.com	Maney	Gordon	Zeller, P.A.
Atcore	Dingbro Ltd	A.R. Thomson Group
Altro	Mortons Media Group Ltd	ARRI
Cleveland Brothers	AIRCOMECHANICAL	Panolam Surface Systems
SEACAST	Pella	Landaumedia

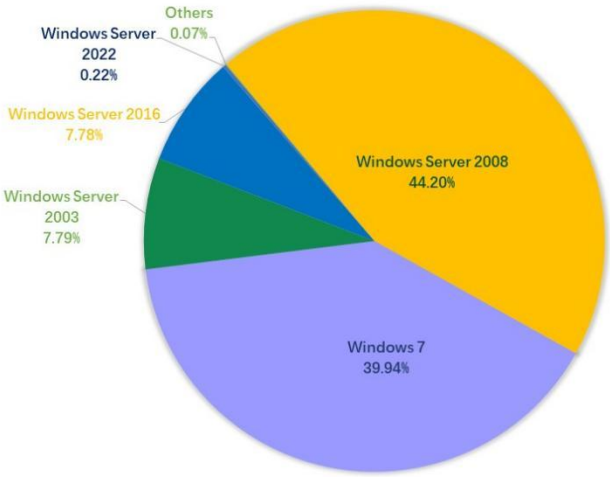
Hilldrup	ChemiFlex	Radical Sportscars
Orotex	Pilenpak	AHT Wisconsin Windows
Acquarius Trust Group	Warren County Community College	Generator-power
V3 Companies	SOTO Consulting Engineers	Requena
Albina Asphalt	Adams-Friendship Area School District	Wrota Mazowsza
UJV Rez	Skoda Praha	MME Group
Highwater Ethanol	Boss-inc	Feu Vert
g4s.com	myersontooth.com	nworksllc
CIBTvisas	BRYCON Construction	NCI CABLING INC
SEED CO LTD	LJ Hooker Palm Beach	morugait
Elias Motsoaledi Local Municiapality	Novak Law Offices	prinovaglobal.com
littleswitzerland.com	Glutz	INTERSPORT
Jubilant	AV Solutions	ZXP Technologies
Aria systems	Realstar Holdings Partnership	Berlina Tbk
Austria Presse Agentur	brunoy.fr	sentenia.net
handrhealthcare.com	Grupo NGN	Philippine Economic Zone Authority (PEZA)
Cappagh Contractors Construction (London) Ltd	Lucchini RS	abilways.com
Trussbilt LLC	Duplicator Sales & Service	All Seasons Global Solutions
Summit	PGT Innovations	thorntontomasetti.com
ckfinc.com	adamjeeinsurance.com	8x8.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，目前已加入黑客入侵防护功能。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。

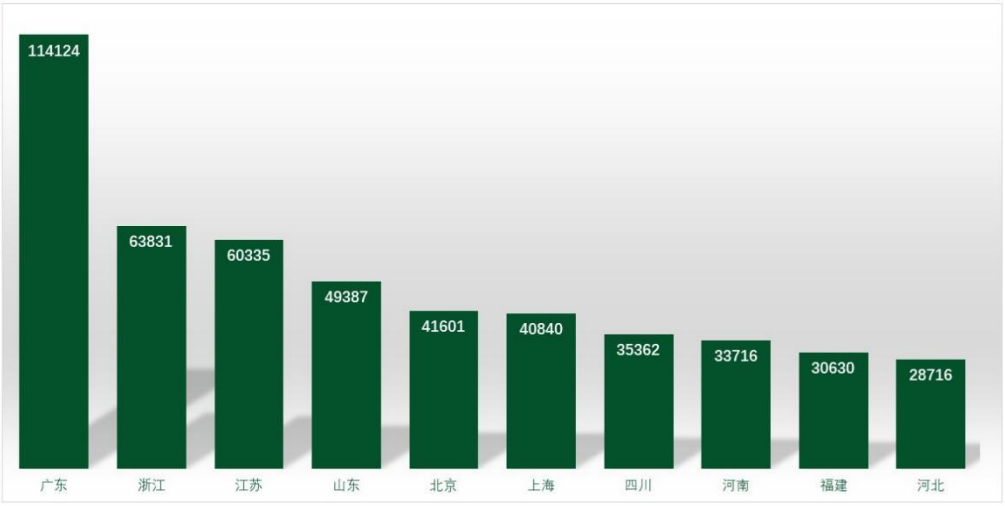
2022年12月弱口令攻击系统占比



数据来源：360反勒索服务

对 2022 年 12 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。

2022年12月全国被弱口令攻击地区TOP10



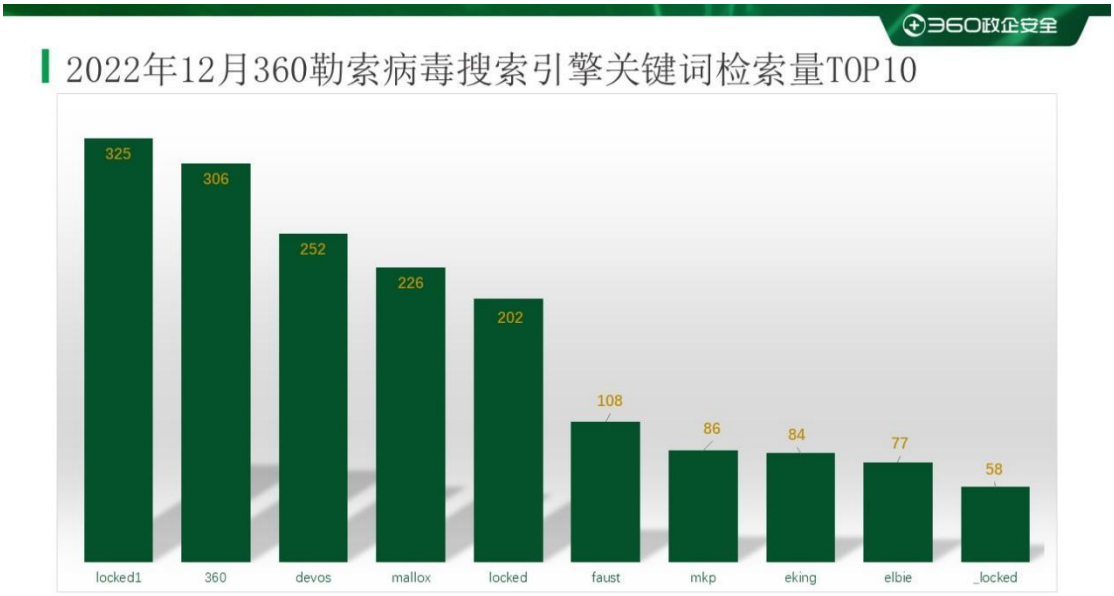
数据来源：360系统安全防护

通过观察 2022 年 12 月弱口令攻击态势发现，RDP 弱口令攻击、MYSQL 弱口令攻击和 MSSQL 弱口令攻击整体无较大波动。

勒索软件关键词

以下是本月上榜活跃勒索软件关键词统计，数据来自 360 勒索软件搜索引擎。

- locked1：属于 TellYouThePass 勒索软件家族，由于被加密文件后缀会被修改为 locked 而成为关键词。该家族主要通过各种软件漏洞、系统漏洞进行传播。
- 360：属于 BeijngCrypt 勒索软件家族，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。
- 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 勒索软件家族，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。
- mallox：属于 TargetCompany(Mallox)勒索软件家族，由于被加密文件后缀会被修改为 mallox 而成为关键词。主要通过暴力破解远程桌面口令成功后手动投毒和 SQLGlobeImposter 渠道进行传播。此外 360 安全大脑监控到该家族本曾通过匿影僵尸网络进行传播。
- locked:同 locked1。
- faust：同 devos。
- mkp：属于 Makop 勒索软件家族，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。
- eking：同 devos。
- elbie:同 devos。
- _locked：属于 Trigona(CryLock)勒索软件家族，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。



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 Loki，其次是 Tesla。使用解密大师解密文件的用户数量最高的是 Crysis 被家族加密的设备(解密文件数较小故未入榜)，其次是被 Stop 家族加密的设备。

数据来源：反勒索服务统计数据