2022 年 11 月勒索软件态势分析

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 11 月，全球新增的活跃勒索软件家族有:Royal、BlackBit、Play、PCOK、Somnia 等家族。其中 Royal 勒索软件不仅是本月新增，还是本月双重勒索软件中受害者数量最高的一个家族；PCOK 为本月国内新增家族；Somnia 勒索软件被俄罗斯黑客用于攻击乌克兰。本月，360 解密大师新增对 Coffee 最新变种的解密支持。

以下是本月值的关注的部分热点：

一、LockBit 组织正利用 Amadey Bot 恶意软件进行传播，并对 Continental 汽车公司发起网络攻击。

二、Coffee 新变种重出江湖，袭击国内高校与研究机构

三、新型 Azov 数据擦除器试图陷害安全研究人员

四、Keralty 遭受勒索攻击导致哥伦比亚医疗系统受到影响

五、加拿大食品零售巨头 Sobeys 遭到 Black Basta 勒索软件攻击

基于对 360 反勒索数据的分析研判，360 数字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

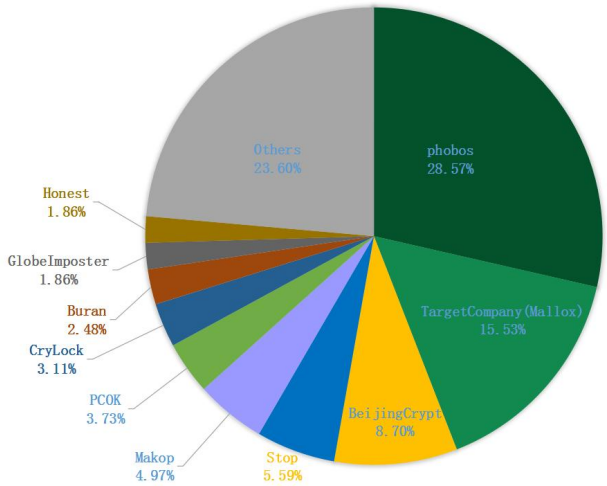
针对本月勒索软件受害者所中勒索软件家族进行统计，phobos 家族占比 28.57%居首位，其次是占比 15.53%的 TargetCompany(Mallox)，BeijingCrypt 家族以 8.70%位居第三。

本月 phobos 勒索家族重回首位，传播方式并未改变，仍采用暴力破解远程桌面，主要流行版本变为后缀为 faust 的变种。

PCOK 勒索软件是本月在国内新增的一款勒索软件，和 phobos 家族一样通过获取远程桌面密码后手动投毒传播。

Coffee 勒索软件在本月底再次活跃，与之前 360 安全大脑年初捕获该病毒时的传播渠道相同，通过 QQ 群文件与邮件针对高校师生进行传播。

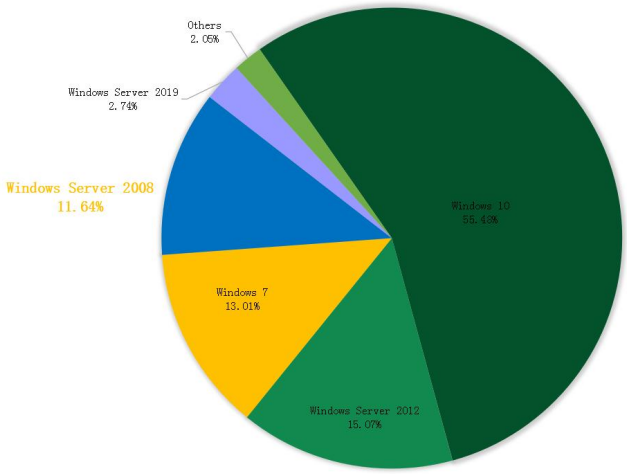
2022年11月反勒索服务处置勒索病毒家族占比



数据来源：360反勒索服务

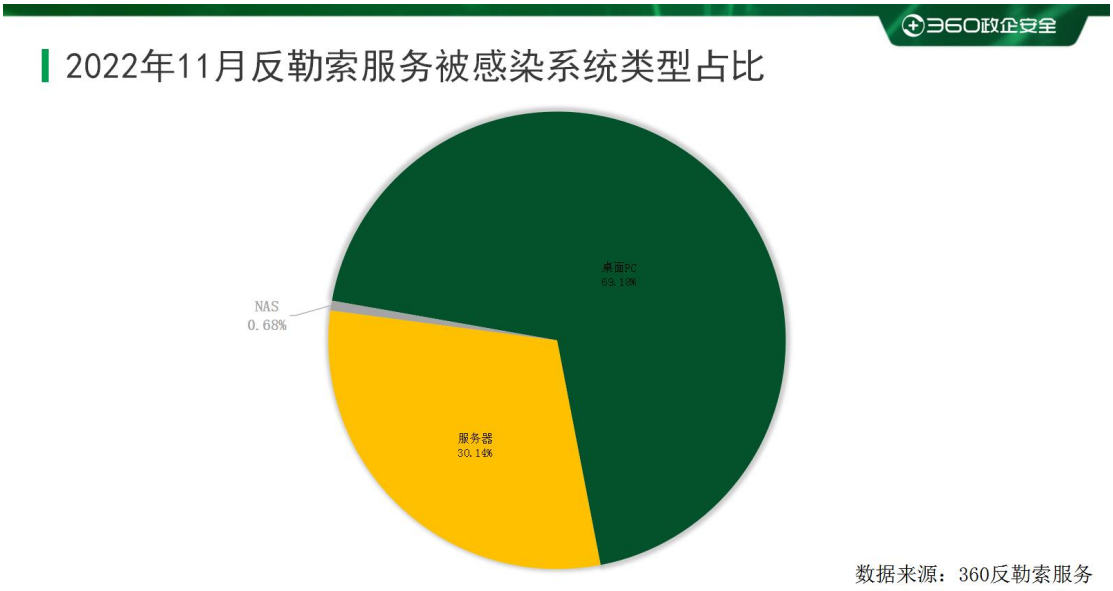
对本月受害者所使用的操作系统进行统计，位居前三的是：Windows 10、Windows Server 2012 以及 Windows 7。

2022年11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 11 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。



数据来源：360反勒索服务

勒索病毒疫情分析

LockBit 组织正利用 Amadey Bot 恶意软件进行传播，并对 Continental 汽车公司发起网络攻击

目前，LockBit 3.0 勒索软件组织正在使用安装 Amadey Bot 的钓鱼电子邮件来入侵设备并在受害设备中投放勒索软件并加密。

据分析，在当前版本的攻击中，攻击者会使用经混淆的 PowerShell 脚本或命令行来在线加载并执行 LockBit 3.0 攻击载荷，使其在主机上运行以加密文件。

Amadey Bot 恶意软件是一种能够执行系统侦察、数据过滤和执行载荷加载的旧病毒。据研究人员研究，2022 年 Amadey Bot 的活动有所增加，并在其最新版本中增加了对抗病毒检测和自动回避的功能，使其的入侵及载荷投放行为更加隐蔽。

本月 LockBit 勒索软件组织还对德国跨国汽车集团 Continental 发起网络攻击。据称，在此次攻击中 LockBit 还窃取了 Continental 系统中的一些数据。攻击者还威胁说，如果该公司在未来 22 小时内不服从他们的要求，他们就将在数据泄露网站上公布这些数据。目前，该团伙尚未公布其从 Continental 网络中窃取的数据及其他细节。

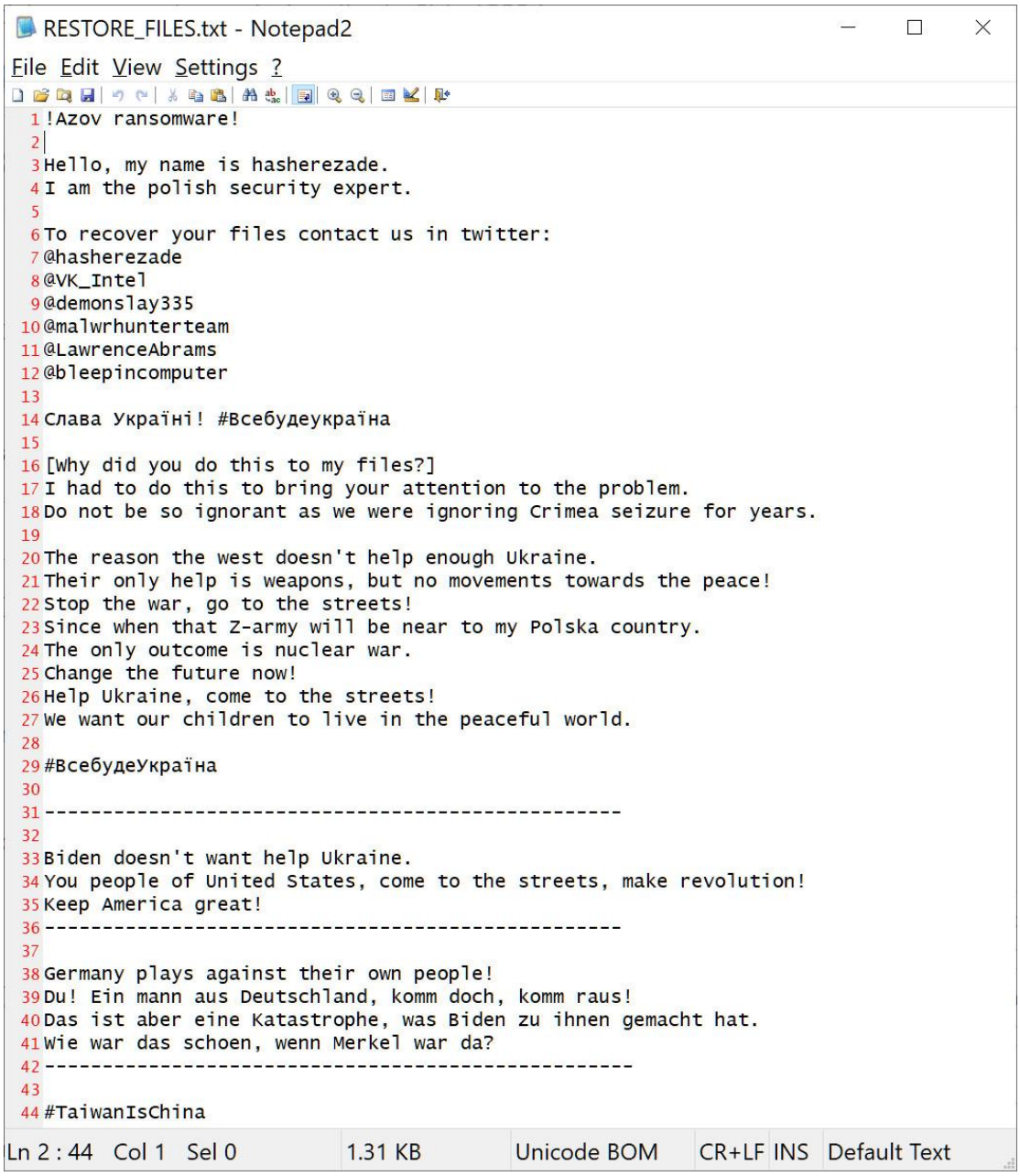
由于 LockBit 表示将公布“所有可用”数据，这可能说明 Continental 尚未与勒索软件团伙进行谈判或已经拒绝了对方的勒索要求。

新型 Azov 数据擦除器试图陷害安全研究人员

一款新型名为 Azov 的数据擦拭器正在通过盗版软件、密钥生成器和广告软件大量传播，同时该软件试图通过虚假消息谎称某安全研究员为其幕后黑手。

该软件的了勒索信息文件名为“RESTORE_FILES.txt”。在信息中，该软件宣称之所以攻击当前设备是为了抗议克里米亚被占领，也是因为西方国家在帮助乌克兰对抗俄罗斯方面做得不够。

此外，由于无法联系攻击者支付赎金，该勒索软件被归类为数据清除器，而不是通常的加密型勒索软件。



Keralty 遭受勒索攻击导致哥伦比亚医疗系统受到影响

11 月底，Keralty 跨国医疗机构遭遇勒索软件攻击，扰乱了该公司及其子公司的网站和运营。

Keralty 是一家哥伦比亚医疗保健提供商，在拉丁美洲、西班牙、美国和亚洲运营着 12 家医院和 371 家医疗中心的国际网络。该集团拥有 24000 名员工和 10000 名医生，为 600 多万名患者提供医疗服务。该公司通过其子公司 Colsanitas、Sanitas USA 和 EPS Sanitas 提供具体的医疗保健服务。

过去几天，Keralty 及其子公司 EPS Sanitas 和 Colsanitas 的 IT 运营、医疗预约及其网站都受到了此次勒索攻击事件的影响。而信息系统的中断直接影响了哥伦比亚的医疗保健系统。当地媒体报道称，患者排队等候治疗超过 12 个小时，一些患者因缺乏医疗护理而

晕倒。

11 月 28 日，Keralty 表示他们遇到了技术问题，但没有透露原因。而根据 Keralty 在 29 日发布了另一份声明证实，此次系统问题是由其网络受到勒索攻击造成的，导致其 IT 系统出现技术故障。

而根据一位名为亚历克斯 •兰德（Alexánder）的推特用户在推特上发布了一张 VMware ESXi 服务器的截图，并附有一张显示“目前已确认这份勒索信息来自于 RansomHouse 家族的勒索软件。

加拿大食品零售巨头 Sobeys 遭到 Black Basta 勒索软件攻击

加拿大食品零售巨头Venus旗下的杂货店和药店自11月初以来一直存在IT系统问题。而在 11 月 7 日发布的新闻中称，Venus 的母公司 Empire 透露：尽管其杂货店仍在营业，但一些服务受到了这些 IT 问题的影响。

该零售商透露：“公司的杂货店仍在营业并为顾客提供服务，目前没有出现严重的中断。然而，一些店内服务出现了间断或延迟……此外，公司的某些药房在开具处方等方面遇到了技术问题。然而，公司仍致力于为所有患者提供医护服务。”该公司还补充称，正在努力解决影响其 IT 系统的问题，以减少门店收到的影响。

据 Sobeys 在其官网上发表的另一份单独声明中补充称所有商店都保持营业，且“没有受到严重干扰”。然而，根据其员工的说法：所有电脑都受到了 Venus 勒索软件影响而被锁定，只有 POS 机和支付系统由于工作在独立网络中而幸免遇难。

黑客信息披露

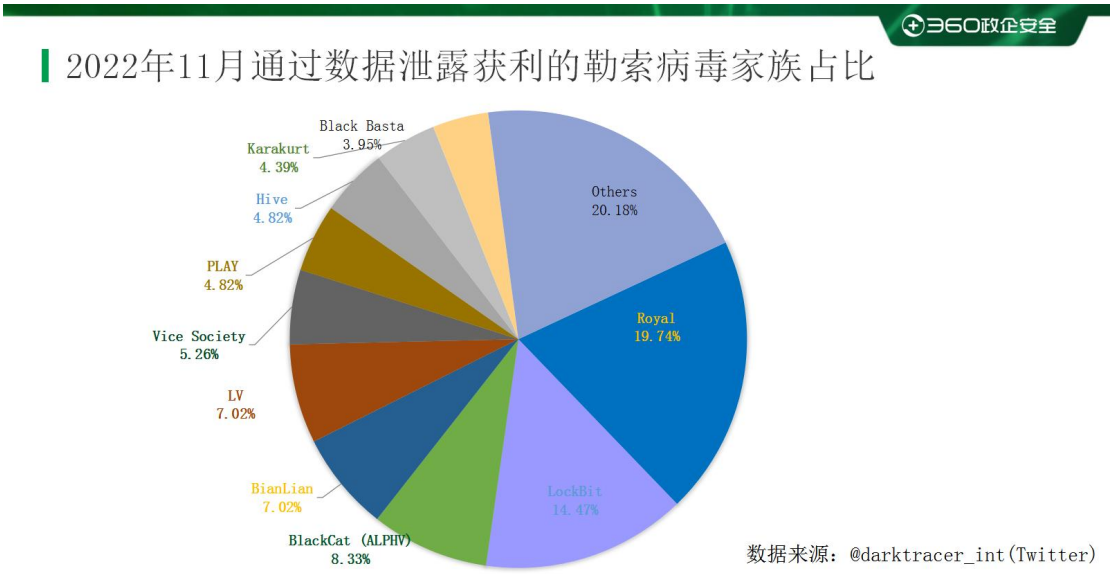
以下是本月收集到的黑客邮箱信息：

milovski@onionmail.org	milovski@tutanota.com	ekingm2023@outlook.com
ryzen@cyberfear.com	quick.connect@zohomail.eu	quick.connect@beeble.com
return_the_job@privatemail.com	back2restore@tutanota.com	back2restore@neomainbox.ch
rastcorp@securetalks.biz	360recover@gmail.com	2mh3k@onionmail.org
lokilocker@onionmail.org	hpsupport@cyberfear.com	hell0s@tutanota.com
hel.b22@tutanota.com	support@fishmail.top	backup@waifu.clu
faragont18@cock.li	admin@encryption-support.com	cuba_support@thesecure.biz
back2restore@neomailbox.ch	back2datten@tutanota.com	jony_recovery@proton.me
@BloodyPandora	jony_recovery@proton.me	@RecoverBlackBit
BlackBitSupport@onionmail.org	datatest777@mailfence.com	datatest777@airmail.cc
barabarabere22@outlook.com	alexgod5566@xyzmailpro.com	godgood55@tutanota.com
HashTreep@waifu.club	RastCorp@securetalks.biz	WARING@cyberfear.com

cyberpunk2077@libertymail.net	cyberpunk2077@firemail.cc	@cyberpunk2077devos
cris_nickson@xmpp.jp	diamondprotonmail.com@proton.me	ryzen@cyberfear.com
pcokdata@tutanota.com	pcokdata@cock.li	DecodeMDR@Outlook.com
Decodemdr@aol.com	Nergontr96@cyberfear.com	localfix@waifu.club
poshix@tfwno.gf	barabarabere22@outlook.com	backshow@my.com
nooli492@gmail.com	nooli492@gmail.com	nooli492@cyberfear.com
ghosthooks@tutanota.com	lastghost@skiff.com	codesystem@cyberfear.com
recoverycompany@elude.in	recoverycompany@tormail.io	backshow@my.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）。



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 229 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 3 个组织/企业未被标明，因此不再以下表格中。

Holler-Classic	Shenzhen INVT Electric Co.,Ltd	Patton
Plascar Participacoes Industriais	Stibbs & Co	colonialgeneral.com
The Summit	RMCLAW	Cates Control Systems
kusd.edu	Vision Technologies	Sunknowledge Services Inc
bankseta.org.za	Itsgroup	Urban
Alcomet	Origin Property Company Limited	PTSC
Conseil departemental - Alpes-Maritimes	Verity cloud	PVFCCo

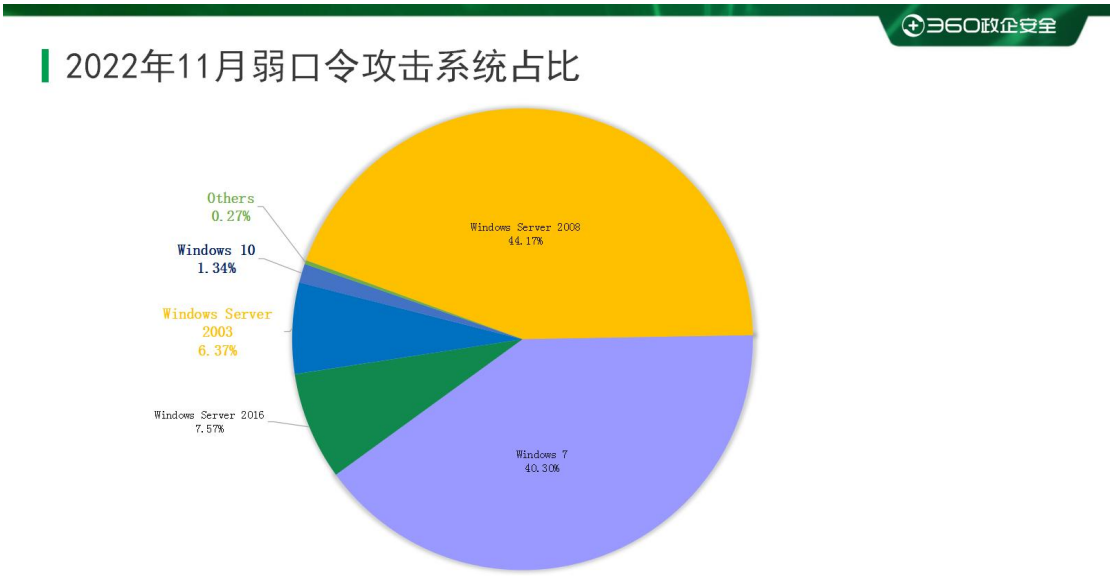
San Benito Consolidated Independent School District	Leadtek	IKEA Morocco
IKEA Kuwait	Tubular Steel Inc	STGi
VANOSS Public School	Power Plant Services LLC	Samrin Services Pvt Ltd
Altec Engineering LLC	Block Buildings LLC	Badger Truck Refrigeration, Inc
Ta Chen Stainless Pipe Co., Ltd	GLEN DIMPLEX GROUP	Law Firm of Friedman + Bartoumian
carone.com.mx	Guilford College	Essent company
Maple Leaf Foods	Myton School	Modular Mining
Centura College	Versah	Gazelle International Ltd
Boon Tool Co	Netaş	Rentz Management
Harry Rosen	Los Angeles Business Journal	Pmc-group
Cincinnati State	Astra Daihatsu Motor (ID)	Norman Public Schools
*u****	lapiamontesa	SMB Solutions
Aeronautics company Canada / UTC Aerospace Systems, Bombardier aerospace partners	Leak Announcement - IT company ITonCLOUD	ryokikogyo.co.jp
ssp-worldwide.com	Schrader-Pacific International	Stratus
SAIPRESS	McGRATH	Nok Air
westmount.org	McAndrews Law Offices	AirAsia Group
norseman.ca	UNITEDAUTO.MX	Virginia Farm Bureau
Giambalvo, Stalzer & Co.	KlamoyaCasino	Naulty, Scaricamazza & McDevitt, LLC
Institute of Science and Technology Austria	Motivating Graphics	ITM
M2S Electronics	Zwijndrecht	IMA Financial Group, Inc.
Cristal Controls	US GOVERNMENT	Lamtec
Agri-Fab	Hydro-Gear	LCMH
Events DC	*CH*****-*A**F** International	zagiel.pl
amend.com.br	linkplus.com.hk	gulfcoastwindows.com
itis-technology.com	Lantek Systems In c	The Keenan Agency Inc
Baysgarth School	scottindustrialsystems.com	THEW ASSOCIATES
Nissan of Las Cruces	Salud Family Health	YASH Technologies
Saurer	Kessing Rechtsanwälte und Fachanwälte in PartGmbB	Midland Cogeneration Venture
CENTRAL BANK OF GAMBIA	Willis Klein	BroadMed Holding
Turner & Associates, LLP	Sterling Battery	Doctors Center Hospital
Vauxhall Motors	nobilityrcm.com	elitemedicalbill.com
MSBS.biz sym	MFAST.com	altapartnersllc.com
Q.E.P	BRAZILIAN PET FOODS	J & D Pierce Contracts Ltd
B Fernandez & Hnos	amarillogeeks.webhop.org	Kreisverwaltung Rhein-Pfalz-Kreis
Aeronautics company Canada	Main & Main Capital Group	MCCROSSAN
CONFORAMA	thecondorgroup.com	chahousing.org

Hartnell College	adnec.ae	sinopecthc.com
oehc.corsica	stavbar.cz	shmcomputers.screenconnect.com
APM Terminals	BauVal	Centrisys cnp
Roxboro	LAW OFFICES OF JOHN T ORCUTT	Adven
waltersandwolf	US AIRPORT	Silverstone
Zender	ALLIANCE AFRICAINE D'ASSURANCES	Ortmeier Maschinen- und Vorrichtungsbau GmbH & Co. KG
Brazen.com	Motional	crtl.com
thaiho.com	GMM Grammy Public Company Limited	TCQ
ROYAL GATEWAY CO., LTD	Cornwell Quality Tools	Sohnen Enterprises
Ivaco Rolling Mills	METRO	ALTEK
Wilken Software Group	Bosselman Energy Inc	Sheehan Family Companies
richard-wolf.com	medibank.com.au	Data-Core Systems
Heart of Missouri United Way	Talas Engineering	CR&R Environmental Services
optiprint.ca	thenet.group	rockworthindia.com
everstrong.com	KEARNEYCO.COM	MITCON Consultancy & Engineering Services Limited
Broto Legal	PETERSON & HANSON	TheBodyShop Indonesia
SOFTEQ.COM	NVIDIA	hettichbenelux.com
Landi Renzo	continental.com	Outsourcing
Northwest Michigan Health Services	Priority Power Management	Happy Sapiens Dental
Camino Real Kitchens	The Benbrook Public Library	Miller Milling
Sunwell Technologies	PowerSoft Development	Midwest Orthopaedic Consultants
Master Medical Equipment	InfoCision Corporation	Wiseyes
Royal Imaging	Whitney Oil and Gas	Panda Power Funds
F.lli Veroni fu Angelo SpA	Pressco Technology	Fishmans
Quantum Plastics	www.maynards.com	CONSUMAX.COM.AR
inexa-ci.com	MARS.COM	tekniplex.be
Popp Hutcheson PLLC	Saint Jean Industries	AWESOME-DENTAL.COM
WICKERSHAMCONSTRUCTION.COM	PARAMOUNT ENTERPRISE INTERNATIONAL	THEHURSTGROUP.CO.UK
ROUGIER	GRUPO SIFU	SUBCARN
KINETIC.PH	SICOTEC	MCV Holding Company LLC
Grandview, MO	YMCA of Metropolitan Washington	Rooks Heath School
Unidad Medica Angloamericana	fiscosaudepe.com.br	Ministry of Transport and Public Works

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了系统安全防护功能，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 2016。

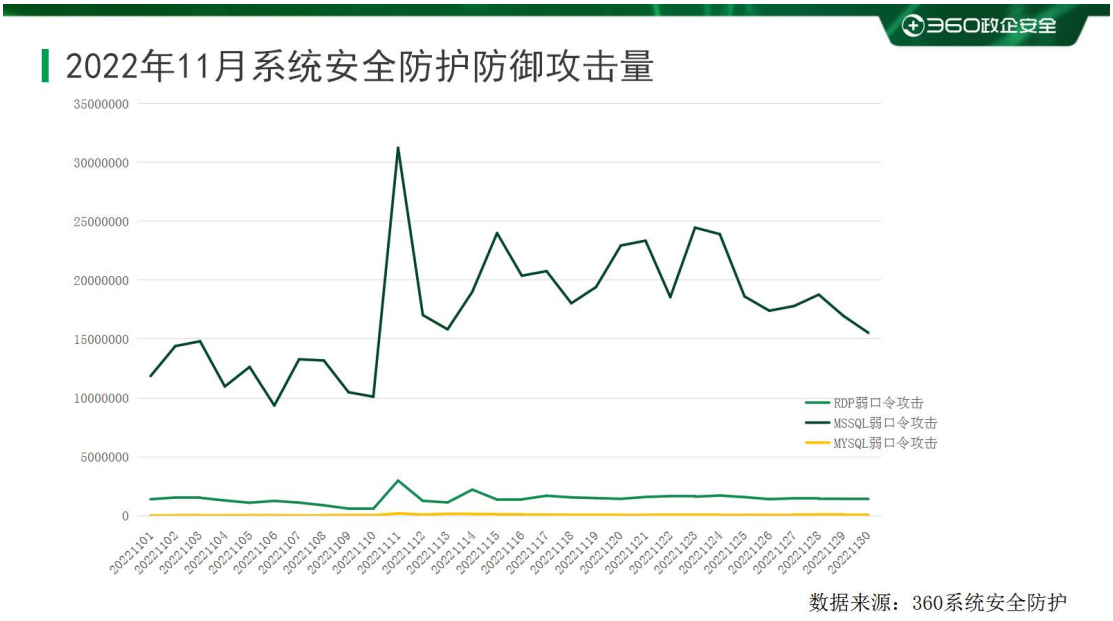


数据来源：360反勒索服务

对 2022 年 11 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11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。



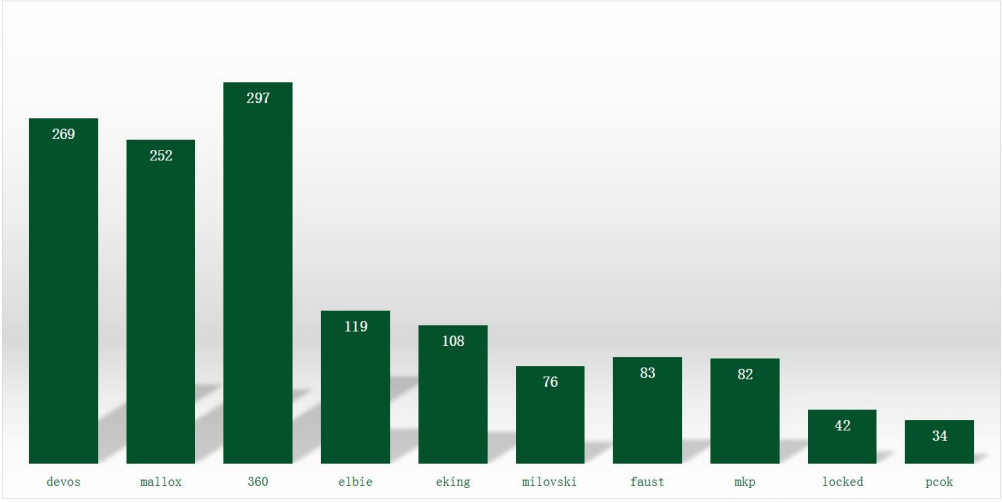
数据来源：360系统安全防护

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。

- 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 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。
- 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。
- elbie：属于 phobos 勒索软件家族，由于被加密文件后缀会被修改为 elbie 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。
- eking：同 elbie。
- milovski:同 mallox。
- faust：同 elbie
- 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。
- locked：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。
- Pock：属于 POCK 勒索软件家族，由于被加密文件后缀会被修改为 POCK 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。

2022年11月360勒索病毒搜索引擎关键词检索量Top10

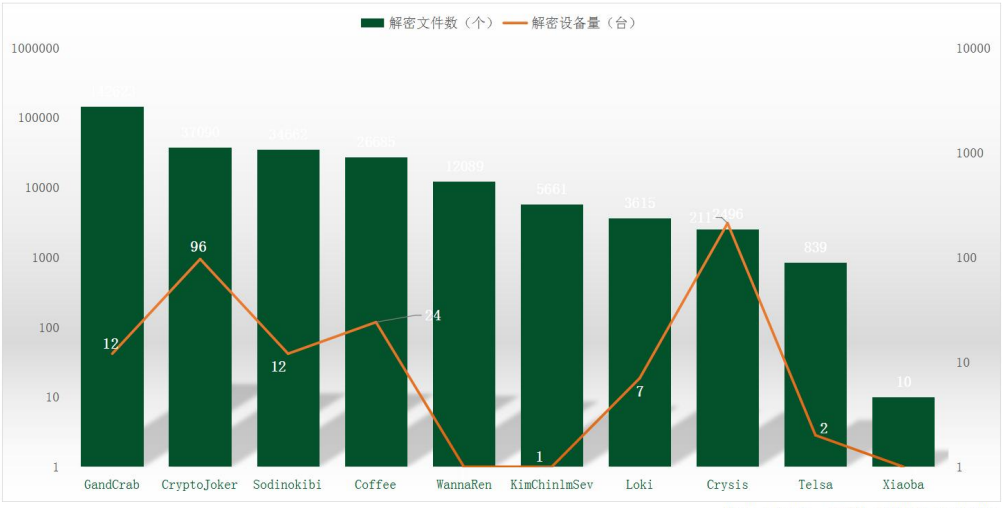


数据来源：360勒索病毒搜索引擎

解密大师

从解密大师本月解密数据看，解密量最大 的是 GandCrab，其次是 CryptoJoker。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 CryptoJoker 家族加密的设备。本月新增对 Coffee 最新变种的解密支持。

2022年11月解密大师解密量



数据来源：反勒索服务统计数据