

勒索软件流行态势分析

2023 年 11 月



勒索软件传播至今，360 反勒索服务已累计接收到数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 全网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。

2023 年 11 月，全球新增的活跃勒索软件家族有 MEOOW LEAKS 和 Lambda，其中 MEOOW LEAKS 家族采用多重勒索方式运营，而 Lambda 则采用较为传统的加密勒索方式运营。

以下是本月值的关注的部分热点：

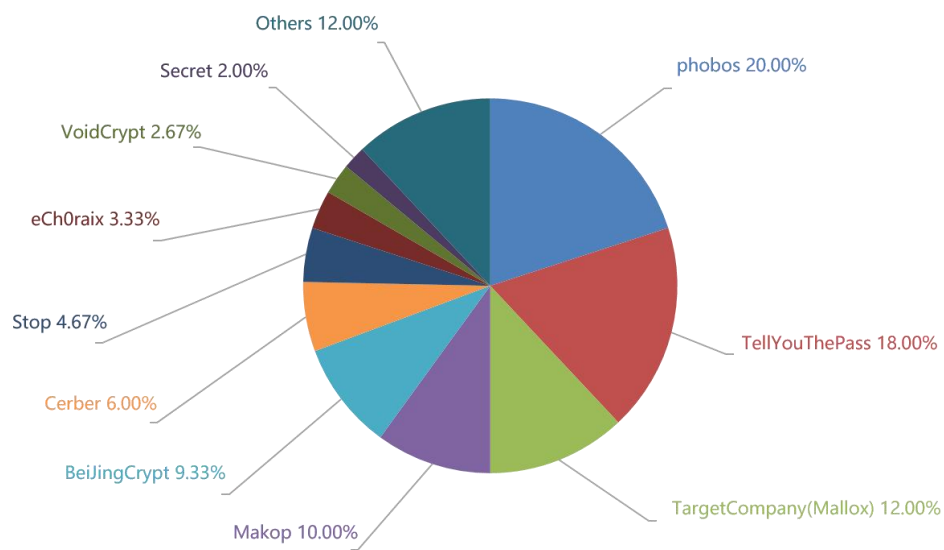
1. LockBit 勒索软件肆虐网络，多家知名企业中招
2. Cerber 新变种 LOCK3D 勒索软件借助漏洞多平台传播
3. TellYouThePass 借助 Web 服务漏洞卷土重来

基于对 360 反勒索服务数据的分析研判，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。

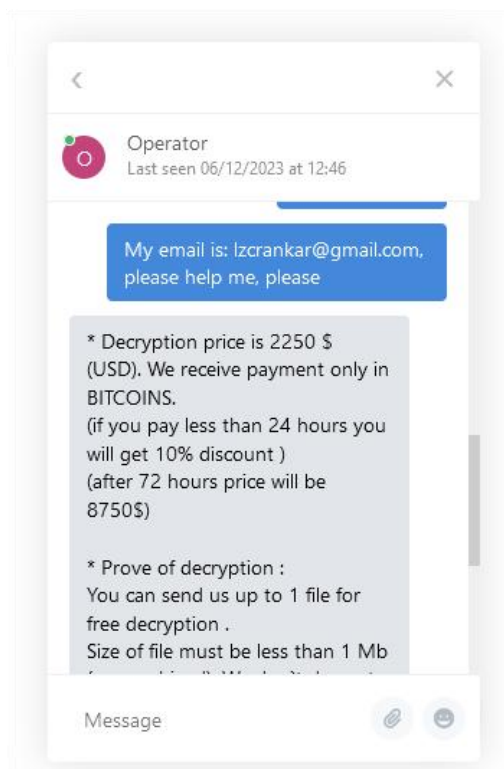
感染数据分析

针对本月勒索软件受害者设备中所中病毒家族进行统计：Phobos 家族占比 20%居首位，第二是占比 18%的 TellYouThePass，TargetCompany(Mallox)家族以 12%位居第三。

其中位居第二的 TellYouThePass 本月再度利用 web 应用类漏洞进行大范围传播。

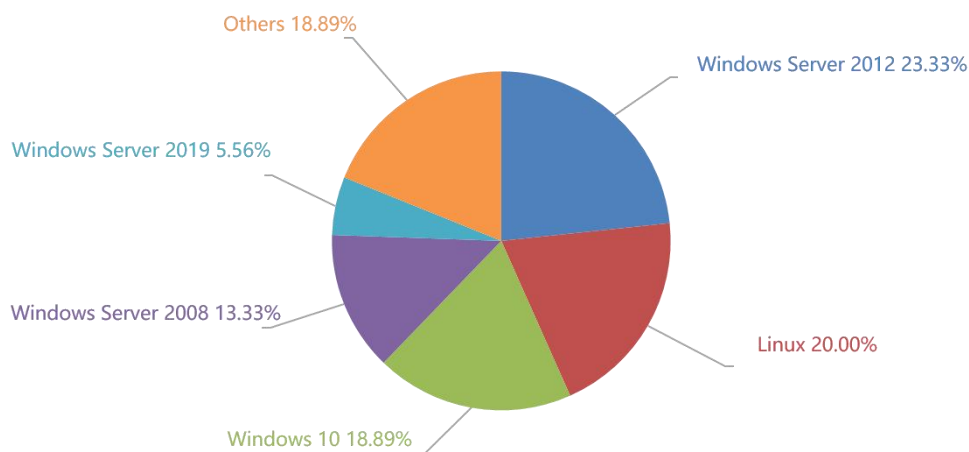


需要特别指出的是：虽然并未跻身 Top10 榜单，但一款名为 Lambda 的新兴勒索软件于本月首次被检测到在国内活跃。该家族主要针对组织/企业进行攻击，受害者可使用勒索提示信息中的暗网地址和 ID,与黑客进行赎金谈判。该家族向受害组织/企业索要价值\$2250 的比特币(超过 72 小时将上涨至\$8750)，且仅支持比特币交易。

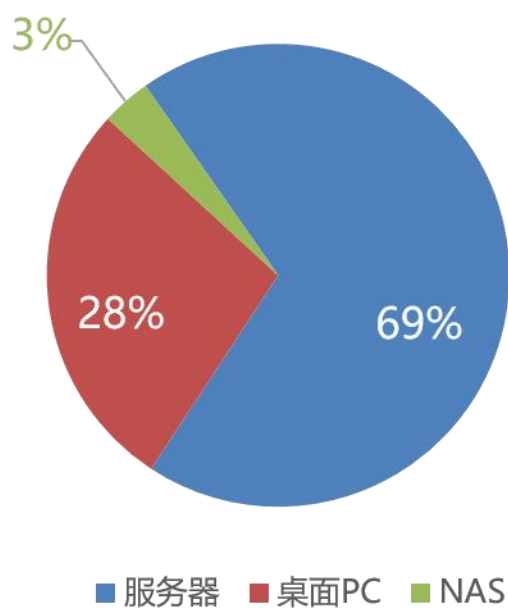


对本月受害者所使用的操作系统进行统计，位居前三的是：Windows Server 2012、Linux 以及 Windows 10。

Linux 平台受害者激增且受多个活跃家族影响，需 Linux 管理员加强漏洞修复与安全管理。



2023 年 11 月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型服务器系统占比远高于桌面系统，偶有 NAS 平台感染。服务器系统占比超过桌面系统，主要是受到 TellYouThePass 活跃家族影响，该家族目前主要通过服务器部署的 web 应用漏洞传播。



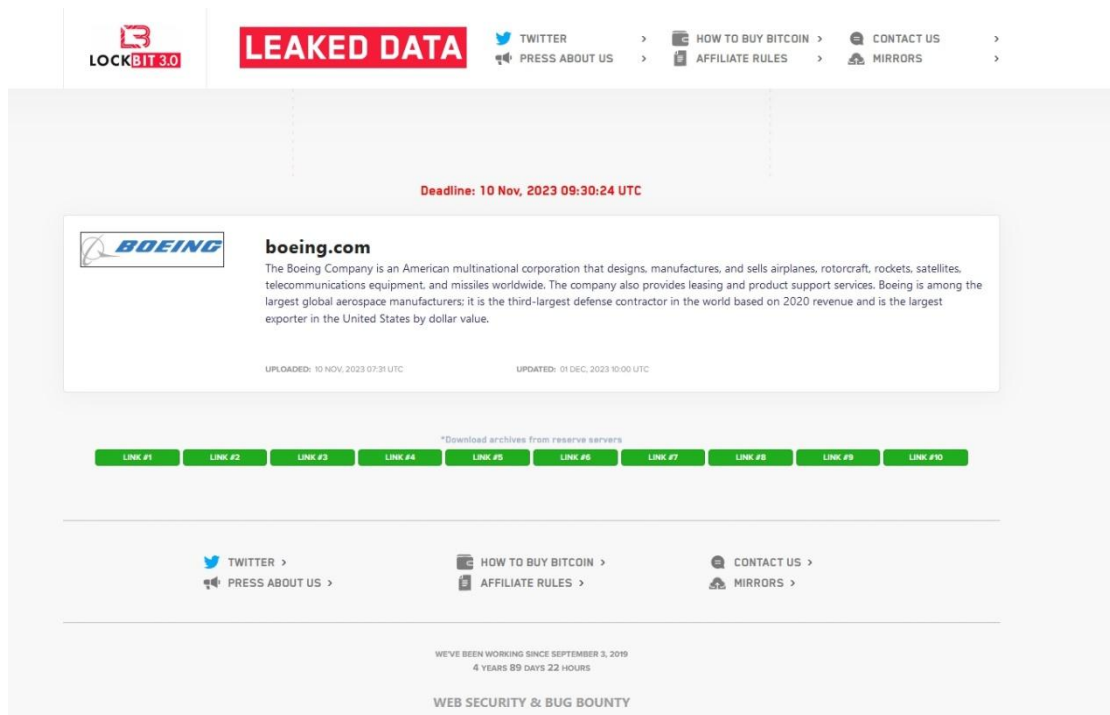
勒索软件热点事件

LockBit 勒索软件肆虐网络，多家知名企业中招

进入 11 月，当下主要活跃勒索软件家族之一的 LockBit 再度肆虐网络，并导致多家国内外知名企业中招。航空航天巨头波音公司也成为了本轮攻击的受害者。波音自称正在调查一场影响其零部件和分销业务的网络攻击，之前 LockBit 勒索软件团伙便声称他们攻入了该公司的网络系统并窃取到了数据。

波音公司表示此次事件并未影响其飞行安全，并称已经与执法和监管机构合作展开调查。目前，波音的服务网站已关闭，并在页面上展示消息称页面关停是由“技术问题”引起的。

虽然波音公司方面并未证实 LockBit 的说法，但该团伙在暗网搭建的数据泄露页面已删除了波音的相关数据。而 LockBit 团伙则在删除数据前表示：“如果波音公司不在最后期限内与团伙联系，便会泄露和发布大量敏感数据。”……“目前为了保护该公司数据，我们不会公布详细列表或样例，但在截止日期之后，我们便不会再有所保留。”



此外，国内某大型跨国公司在美的金融分支机构也受到了本轮 LockBit 攻击的影响。据英国《金融时报》报道：有市场参与者于 11 月 9 日透露中国某公司的金融服务部门遭到勒索软件攻击，这次攻击导致其金融服务公司代理的美国国债结算业务被阻断，一些股票交易也受到影响。另据交易消息人士称：包括对冲基金和资产管理公司在内的市场参与者，因为此次系统中断而被迫改变了交易途径。此次攻击对美国国债市场的流动性产生了一些影响，但并未损害市场的整体运作。以上消息也得到了证券业和金融市场协会的印证。

安全研究组织表示“该公司目前无法连接到 DTCC/NSCC 系统。该问题正影响其所有清算客户。”由于此次攻击，该公司无法代理其他市场参与者进行美国国债结算交易。

有安全专家表示，这家中国公司的 Citrix 服务器在周一最后一次上线，并且未针对已被披露的 NetScaler 安全漏洞（又称“Citrix Bleed”漏洞）进行修补，而该服务器现在已离线。

目前，该公司在国内的母公司回应称，遭受攻击的是其金融服务业务，该业务独立于集团主体业务之外。同时强调总公司及其他境内外关联机构的系统没有受到此次事件的影响，其纽约分部也没有受到影响。

Cerber 新变种 LOCK3D 勒索软件借助漏洞多平台传播

近期，接到大量 Linux 系统用户反馈，电脑中的文件被勒索软件加密，被加密后的文件后缀均为.LOCK3D。经分析，这些用户感染的均是隶属于 Cerber 家族的勒索软件。本轮攻击主要是通过 Confluence 数据中心和服务器中的不当授权漏洞进行传播（漏洞编号为 CVE-2023-22518）。受该漏洞影响而遭到攻击的平台，覆盖了 Linux 与 Windows 等主流服务器操作系统。

根据 360 安全大脑捕获的攻击信息显示，攻击者会通过该 Confluence 漏洞调起 cmd 进程并创建 powershell 进程来加载攻击载荷。最终，从 193.176.179.41 服务器上下载 Cerber 勒索软件的主体功能文件，并将其保存到临时文件夹中，进而命名为 svcPrvinit.exe。完成后，附加参数“-b 9”以达到静默执行该进程而不显示窗口的目的。

根据相关数据扫描，目前暴露于互联网中并运行有带漏洞的 Confluence 服务的设备约有 20 万台，但受到攻击的数量目前不详。根据以往经验推算被入侵的设备量级目前应该在数千台左右。而国内受影响情况总体来说目前并不严重。

TellYouThePass 借助 Web 服务漏洞卷土重来

一直以来 TellYouThePass 勒索软件都是借助各类网络服务的漏洞入侵系统后实施勒索攻击。本月 TellYouThePass 再次借助 Apache ActiveMQ 服务的关键远程代码执行漏洞发动攻击入侵网络。被利用的漏洞编号为 CVE-2023-46604，是由 ActiveMQ 可扩展开源消息代理中的一个严重错误导致，该漏洞允许未经身份验证的攻击者在存在漏洞的服务器上执行任意 Shell 命令。

虽然 Apache 于 10 月 27 日便发布了安全更新来修复该漏洞，但依然有网络安全公司发现至少从 10 月 10 日起便有攻击者已经开始利用其作为 0day 漏洞部署远控类恶意软件。而在 Apache 发布了针对该漏洞的更新补丁后，又有安全机构发现攻击者利用该漏洞部署 HelloKitty 和 TellYouThePass 两款勒索软件来加密受害设备，本轮漏洞攻击也带来了“自 Log4Shell 漏洞被曝出后，TellYouThePass 活跃量的再度激增”。

此外，TellYouThePass 的这一波猛攻同时还利用了国内某安防管理平台的漏洞。其所涉及的漏洞基本可以锁定为该公司部分安防管理平台产品所带有的安全漏洞。这些漏洞均为任意文件上传漏洞。由于这些综合安防管理平台对上传文件接口校验不足，导致攻击者可以利用漏洞将恶意文件上传到平台，并最终获取服务权限或引发服务异常。不过这些漏洞已被该公司于 2023 年 6 月进行修复，并发布相关公告对其用户进行安全提示。

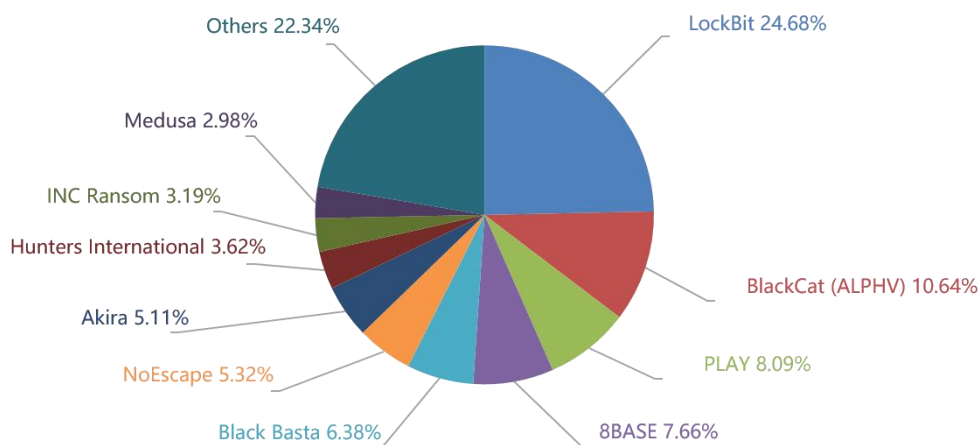
黑客信息披露

以下是本月收集到的黑客邮箱信息：

datastore@cock.lu	nyrgios@airmail.cc	backup20email@tutanota.com
7Rnn7AvDNk@onionmail.org	nyrgios@onionmail.org	xavax@tutanota.com
yourlovelysupp@mail2tor.com	nergal@xmpp.jp	lealir@tutanota.com
yourlovelysupp@xmpp.jp	shanova@mailfence.com	keishagrey994@outlook.com
drebtips@gmx.com	banuda@skiff.com	sn.tchnews.top@protonmail.me
findithere@disroot.org	banuda@tuta.io	funny385@swisscows.email
Deep_in_Deep@tutanota.com	decryptprof@proton.me	funny385@proton.me
fileopen@onionmail.org	service@helloworldtom.online	russellrspeck@seznam.cz
openfile@firemail.at	jrpwqnnud@onionmail.org	russellrspeck@protonmail.com
Detpyrcne@Cyberfear.com	TwoHearts911@protonmail.com	Mailz13MoraleS@proton.me
decryptors@cocaine.ninja	recoverymanager@cock.li	datasto100@tutanota.com
antidata@tuta.io	pcabcd@countermail.com	snatch.vip@protonmail.com
teligent@onionmail.org	abcd-help@countermail.com	unlock@rsv-box.com
ithelp07@yousheltered.com	supportpc@cock.li	unlock@support-mult.com
ithelp07@securitymy.name	goodmen@cock.li	rey14000707@gmail.com
rec_rans@aol.com	gosupp@email.cz	gagnondani225@gmail.com
AbeKerluke@onionmail.org	auguste.royal@aol.com	swikipedia@onionmail.org
ContessaWuckert@onionmail.org	emanuelscratcherd@aol.com	xxx@mail2tor.com
v-society.official@onionmail.org	mesaezzoris@gmail.com	karasikharry25@gmail.com
readdecoding@outlook.com	bowen.bord@aol.com	servicedigilogos@protonmail.com
retunbac@onionmail.org	stuart.wittie@aol.com	managersmaers@tutanota.com
adventures@onionmail.org	phobos_helper@xmpp.jp	pcsupport@skiff.com
adventures@airmail.cc	staff@vx-underground.org	pctalk01@tutanota.com
terofatsrv@proton.me	veracrypt@foxmail.com	spicy01@tuta.io
terofatsrv@tutanota.com	Whitehelper@skiff.com	recoverydatas@bk.ru
Mesacorp_@outlook.com	obamka@tuta.io	serverrecoveryhelp@gmail.com
3442516480@qq.com	nikminch@bk.ru	thenewskings@protonmail.com
1169309366@qq.com	blackout@cumallover.me	datasecurity1@tutanota.com
elvisp@techmail.info	rhysidaeverywhere@onionmail.org	datasecurity1@tutanota.com
elvisp@cyberfear.com	rhysidaofficial@onionmail.org	coca2024cola@zohomail.eu
liam_bernell@zohomail.eu	rahmud1954@cock.email	coca2023cola@libertymail.net
liam.bernell@onionmail.org	backups@airmail.cc	

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 470 个组织/企业遭遇勒索攻击，其中 3 个中国组织/企业在本月遭遇了双重勒索/多重勒索。另有 12 个组织/企业未被标明，因此不再以下表格中。

Rudolf GmbH & Rudolf Venture Chemicals Inc	Kwik Industries, Inc.	Ackerman -Estvold
Bauwerk Boen Group	HAESUNG DS CO Ltd	Meindl
Covenant Care	ATC SA	Conditioned Air
DePauw University	WellLife Network Inc.	Citron WorkSpaces
andersonandjones.com	edc.dk	Inclinator
Science History Institute	Select Education Group	Crown Supply Co
Verdecora	villanuevadelaserena.es	fawry.com
Chetu	Consilium staffing llc	amberhillgroup.com
AQIPA	hsksgreenhalgh.co.uk	califanocarrelli.it
New River Community Technical College	krblaw.com	Michael Garron Hospital
jacobsfarmdelcabo.com	Chung Hwa Chemical Industrial Works	Orion Township Public Library
skalar.com	SUMMIT VETERINARY PHARMACEUTICALS LIMITED	sheehyware.com

Lydall, Inc.	Informist Media	foley.k12.mn.us
Bergeron LLC	planethomelending.com	Avianor Group
REV Engineering	communitydentalmc.org	OE Federal Credit Union
ALPS Ltd	uchlogistics.co.uk	gitiusa.com
Alpura	citycontainer.dk	allenoverly.com
Teleflora	FEAM Maintenance	NeoDomos
Great Valley School District	thewalkerschool	Bakrie Group & Bakrie Sumatera Plantations
masterk.com	goodhopeholdings.com	Indah Water Konsortium
Servicio Móvil	Epstein Law	Truck Bodies & Equipment International
King Edward VII's Hospital	Admilla ELAP	www.advimg.com
tcw.com	Toyota Financial	www.adventhealth.com
Incisive Media	adyne.com	www.srmcfl.com
GOLDMUND	owensgroup.uk	BioPower Sustainable Energy Corporation
Wild Republic	chicagotrading.com	cozwolle.nl
Groupe Apex-Isast	Decatur Independent School District	Certified Mortgage Planners
Leezer Agency	Guardian Alarm	h-tube.com
Cimbali National Accounts	SCOLARI Srl	nicecloud.nl
Fortiss LLC	Yamaha Motor Philippines, Inc.	torrescpa.com
hi-schoolpharmacy.com	Cardinal MetalWorks	tt-engineering.nl
nal.res.in	ADH Health Products Inc	BITZER
dawsongroup.uk	EOS	triflex.nl
New River Community & Technical College	THK Co., Ltd.	Park Ohio
Byfod	SWISHSMILES.COM	Apollo Aerospace Components
Retailer Web Services	kwhfreeze.fi	Supply Technology
China Petrochemical Development	Gallagher Tire, Inc.	secci.ca
Sparex	MODERNGRAB, S.A.	acawtrustfunds.ca
Continental Shipping Line	Storey Trucking Company, Inc.	Hopewell Area School District
MooreCo	APREVYA	panaya
AMERICAN INSULATED GLASS	Lanificio Luigi Colombo S.p.A.	prime-art
Elston-nationwide	MERRILL Technologies Group	ccdrc.pt
Thillens	Ontario Pork	Aceromex
SinglePoint Outsourcing	Parsons Investments	Japan Aviation Electronics Industry, Ltd.
First Housing Development	MeridianLink	sacksteinlaw.com
JD Sprinter Holdings 2010 SL	Premise Health	EFU Life Assurance
Odalys Vacances	Trademark Property	good-lawyer.com
Axiom Construction & Consulting	Nomot	kbrlaw.com
Medi-Market	Global Technologies Racing Ltd	eyephy.com
FYIdoctors	Thompson Candy	United Africa Group Ltd.
Giti Tire	Road Scholar Transport	Mount St. Mary's Seminary
Wema Bank PLC	KaDeWe	GO! Handelsschool Aalst
Es Saadi	Wyatt Detention Center	SMH Group

North Texas Municipal Water District (US)	Guntert & Zimmerman	howlandlaw.net
First Financial Security	ConSpare	UTI Group
Bangkok University	Gnome Landscapes	GEOCOM
NC Central University	maytec.de	MultiMasters
Yanfeng	cmcsheetmetal.com	concretevalue.com
Law Offices of John E Hill	rekord.de	Power Broker (Zycomp Systems)
Fischione Instruments Inc.	boulangerieauger.com	Comfloresta
stsaviationgroup.com	agromatic.de	Currax Pharmaceuticals
InstantWhip	mk Technology Group	Weidmann & Associates
Vertex Resource Group	SheelaFoam	Unimed Blumenau
carrellblanton.com	Naftoport	Leaguers
Huber Heights	4set.es	Zon Beachside
New River Community & Technical College	Naftor	Canadian Psychological Association
sillslegal	Grupa Pern	Corsica-Ferries
Honey Birdette	NAFTOSERWIS	penanshin
Zenithpharma	SARMATIA	Assurius.be
Back Roads	SIARKOPOL	unique-relations.at
Equaldex	diagnostechs	letillet.btprms.com
Vanderbilt University Medical Center	Execuzen	ospedalecoq.it
Standard Filter	Lander County Convention & Tourism Authority	springeroil.com
Katsky Korins	Southeastern Orthopaedic Specialists	szutest.cz
AlJaber Engineering	Carespring	studio483.com
ALAB laboratoria	Warren General Hospital	brlogistics.net
kenso.com.my	shopbentley.com	bresselouhannaiseintercom.fr
Energy China	ASM GLOBAL	nfcc.gov.my
TALENTUM Temporal SAS	tarltonandson.com	sansasecurity.com
carriereindustrial.com	St. Lucie County Tax Collector's	emiliacentrale.it
Albert, Righter & Tittmann architects, inc.	portadelaidfc	duconind.com
ribolia.com	NSEIT LIMITED	mat-antriebstechnik.de
nrtw.org	Moneris Solutions	nckb.com
preidlhof.it	Homeland Inc.	egco.com
Lincoln Office	TCI Co., Ltd.	benya.capital
Granger Medical Clinic	muellersystems.com	global-value-web.com
LCA Consultores	msim.de	aseankorea.org
TJM PRODUCTS PTY. LTD	Putzel Electrical Contractors Inc	infosysbpm.com
Spectrum Solutions LLC	Mpr Lifts	tko.co.th
des-ae.com	aegean.gr	GeoPoint Surveying
unidesign-jewel.com	Owens Group	APERS
Eckell Sparks Law Firm	IDESA group, S.A. De C.V.	tasl.co.th
officinaverdedesign.it	DrilMaco	abhmf.com
Trylon TSF Inc.	thewalkerschool.org	Livability

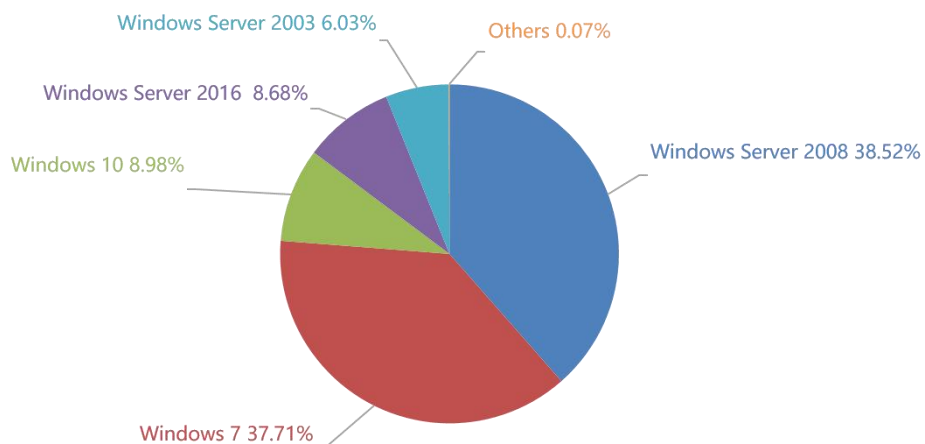
DM Civil Co.	modafabrics.com	unimed.coop.br
Ingo Money Inc	wombleco.com	translink.se
Nicole Miller	hotelemc2.com	jewell.edu
Pro Metals LLC	digitaldruck-esser.de	Medjet
Springfield Area Chamber of Commerce	cityofclarksville.com	Deegenbergklinik
B+P Gerüstbau GmbH	carsonteam.com	Builders Hardware and Hollow Metal, Inc.
Fidelity National Financial	hotel-ampere-paris.com	microtrain.net
McHale Landscape Design	glynncounty.org	labor force Inc
Custom Engineering & Fabrication, Inc.	plati.it	Bankofceylon.co.uk
Alspec	Pricesmart	Agile Display Solutions
IQ Supply Solutions	roth-werkzeugbau.de	JDRM Engineering
NESPOLI GROUP	heinrichseegers.de	Craft-Maid
Community Hospital	vital.co.za	Hilyard's
therobisongroup.com	creatz3d.sg	North Dakota Grain Inspection Services
merz-elektro.de	loiret.fr	Gsp Components
art-eco.it	aten.com	Ricardo
ds-granit.fr	gattoplaters.com	Bry-Air
APVL ingénierie	synnex-grp.com	bindagroup.com
Cold Car Spa	quifatex.com	shimano.com
La Contabile Spa	PAR Group Co	lafase.cl
DMC Luxembourg	MHM Health	HENRY SCHEIN
Hills Legal Group Ltd	estes-express.com	Contact Cottrell and McCullough
Brown's Bay Packing Company	Dragos Inc.	psmicorp.com
Hahn and Clay, Inc.	planning.org	imancorp.es
Imperiali AG	floortex.com	AF Supply
floydskerenlaw.com	Bartec Top Holding GmbH	aniel.fr
bnpmedia.com	ayakitchens.com	Groupe Faubourg
Crystal Lake Health Center	browardfactory.com	bolides.eu
Verhelst	boslogistics.eu	serenicar.fr
Petersen Health Care	Mariposa Landscapes, Inc	HAL Allergy
Paul Stuart	morningstarco.com	R N Wooler & Co Ltd
martinique.no	Azienda Ospedaliera Universitaria Integrata di Verona	Schwob AG
phihydraulics.com	aei.cc	Bluewater Health
qautomotive.com.au	Yale Appliance	Hôtel-Dieu Grace Healthcare
St Edmund's College & Prep School	Sinotech Group Taiwan	Chatham-Kent Health
helifrusa.com	Action Santé Travail	Erie Shores HealthCare
Plastic Molding Technology Inc.	Garr Silpe, P.C.	Windsor Regional Hospital
Enware Australia Pty Ltd	Ezi Floor Products	degregoris.com
Rc Moore Inc	Rudolf Venture Chemical Inc	kitprofs.com
sabre.co.uk	Magsaysay Maritime	imprex.es
Hampton Newport News CSB	Battle Motors (CraneCarrier, CCC)	vitaresearch.com
nybravestfcu.org	SALUS Controls	sanmiguel.iph

agrovi.dk	gotocfr.com	steelofcarolina.com
arenaproducts.com	Autocommerce	raumberg-gumpenstein.at
etude-villa.fr	City Furniture Hire	Detroit Symphony Orchestra
brownintegratedlogistics.com	Koh Brothers	Software Systems
British Library	Cogdell Memorial Hospital	Hawkeye Area Community Action Program, Inc
Tackle West	Pilot Thomas Logistics	summithealth.com
U.L. COLEMAN COMPANIES	Simons Petroleum	gannons.co.uk
Autonomous Flight	Maxum Petroleum	gsp.com.br
The DMC	ggarabia.com	TANATEX Chemicals
onyourmark.org	Jeffcoat Mechanical Services Inc	Town of Iowa
nealbrothers.co.uk	Scheidt GmbH	Traxall France
generalrefrig.com	Ingeniería FULCRUM	Armstrong Consultants
PruittHealth	TXWES.EDU	JAI A/S
ajcfood.com	Identification Products	Schöler Fördertechnik AG
CENTRE D'AUTO P.R.N. SALABERRY IN	M.R. Williams	Vinovalie
McCray & Withrow	DESIGNA Verkehrsleittechnik	SWEETLAKE LAND & OIL CO INC
Metro MPLS	The Supply Room Companies	

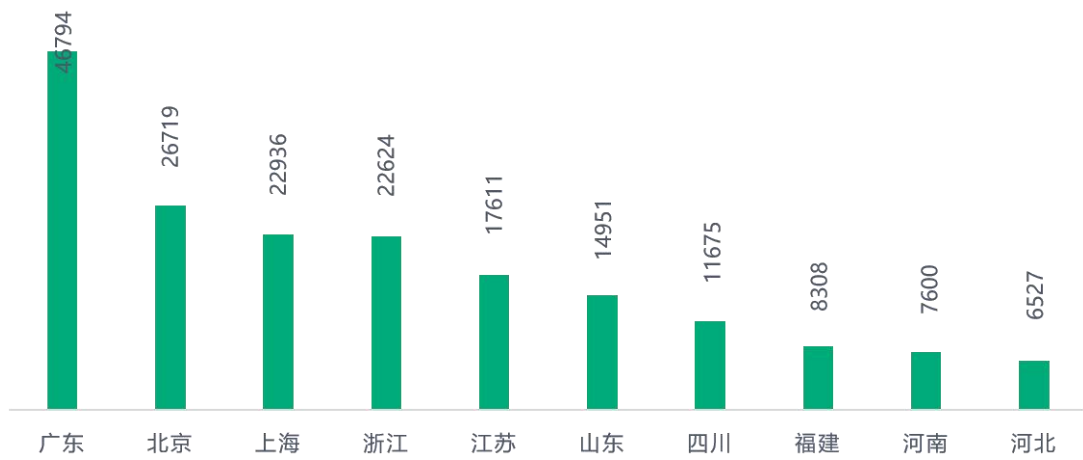
表格 2. 受害组织/企业

系统安全防护数据分析

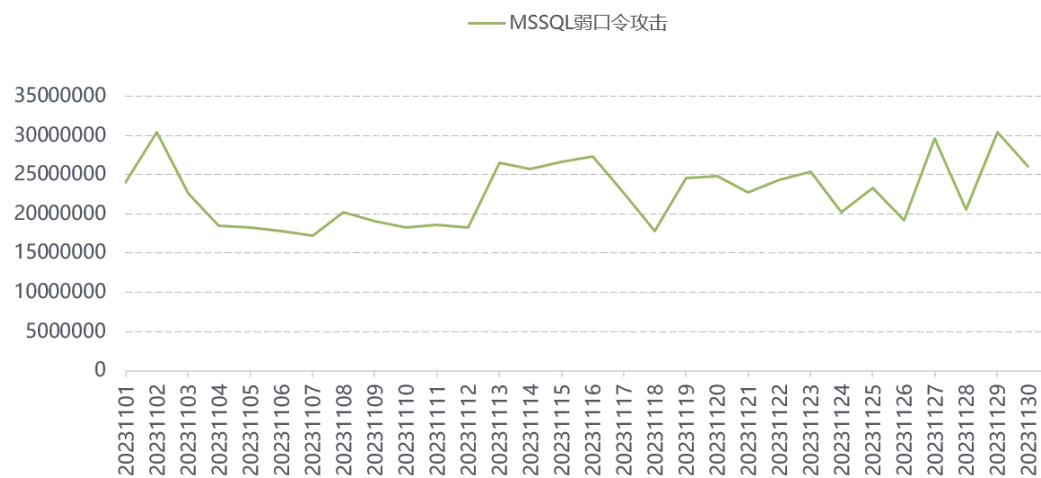
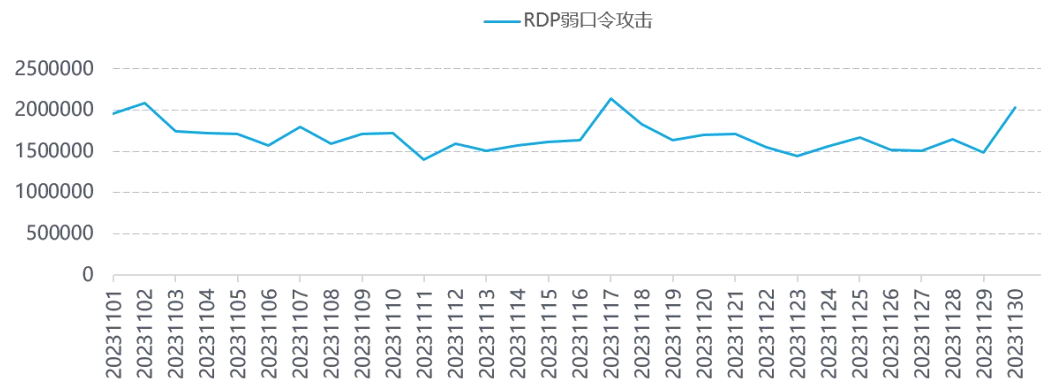
360 系统安全产品，目前已加入黑客入侵防护功能。在本月被攻击的系统版本中，排行前三的依次为 Windows Server 2008、Windows 7 以及 Windows 10。

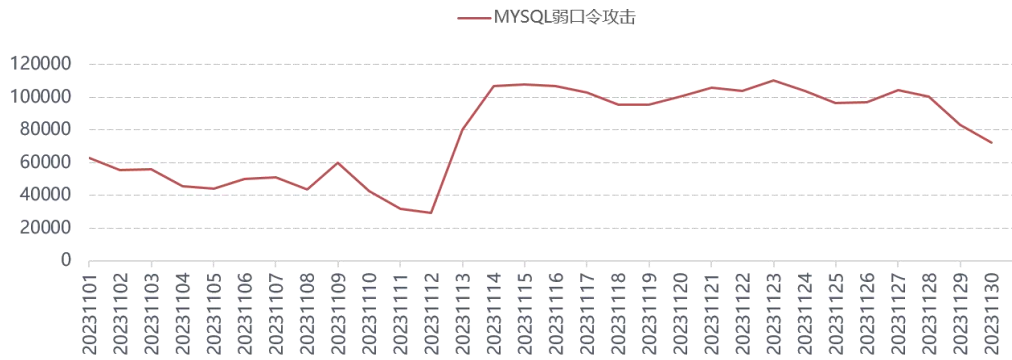


对 2023 年 11 月被攻击系统所属地域统计发现，与之前几个月采集到的数据进行对比，地区排名和占比变化均不大。数字经济发达地区仍是攻击的主要对象。



通过观察 2023 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。



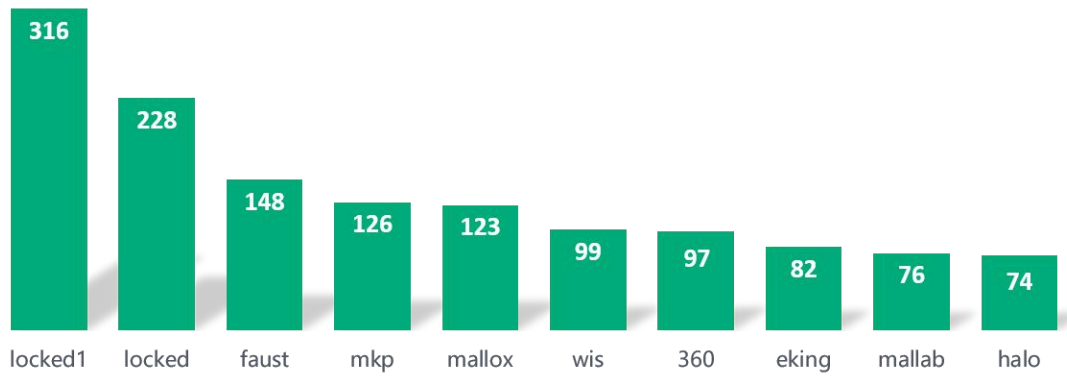


勒索软件关键词

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。
- locked: 同 locked1。
- faust: 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。
- 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。
- 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，本后缀为 10 月新增变种。主要通过暴力破解远程桌面口令成功后手动投毒和 SQLGlobelImposter 渠道进行传播。此外 360 安全大脑监控到该家族也曾通过匿影僵尸网络进行传播。
- wis: 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。
- 360: 属于 BeijingCrypt 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。

- eking: 同 faust。
- mallab: 同 mallox。
- halo: 同 360。



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 OpenMeV2。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。

