勒索软件流行态势分析

2023 年 12 月

360数字安全

数 字 安 全 的 领 导 者

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 12 月，全球新增的活跃勒索软件家族有 LIVE、DragonForce、Tisak 等。其中 DragonForce 家族采用多重勒索方式运营， Tisak 家族除加密 Windows 设备外还会攻击 ESXI 服务器。

以下是本月值得关注的部分热点：

1. 美国海军承包商 Austal 在数据泄露后承认遭受网络攻击

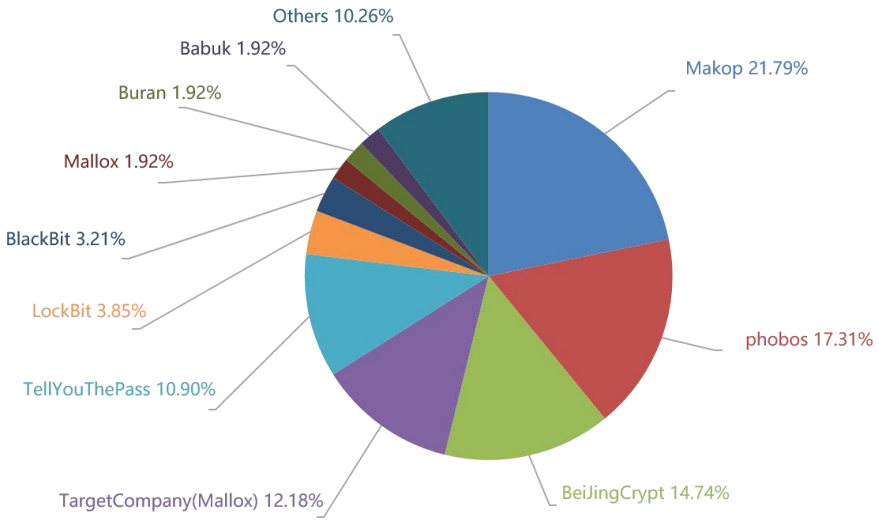
2. Akira 勒索软件团伙声称对 Nissan 澳大利亚的网络攻击负责

3. 育碧表示正在调查有关新安全漏洞的报告

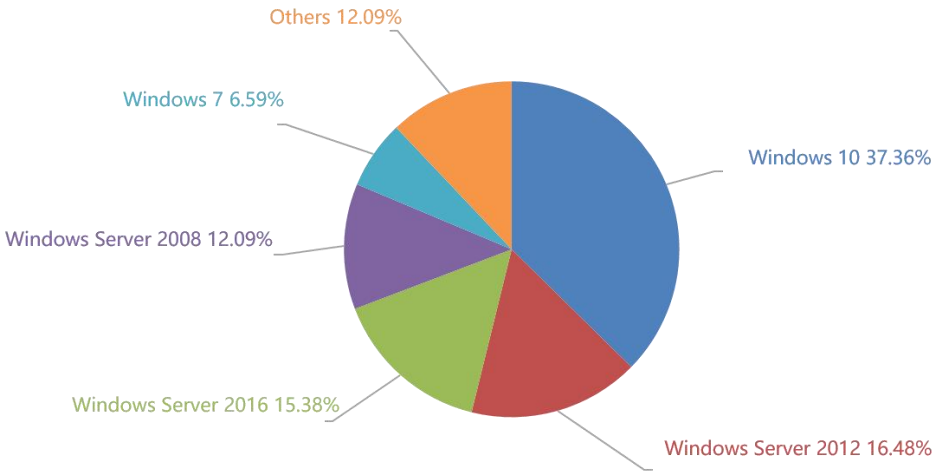
基于对 360 反勒索服务数据的分析研判，360 数字安全集团高级威胁研究分析中心(CCTGA 勒索软件防范应对工作组成员）发布本报告。

感染数据分析

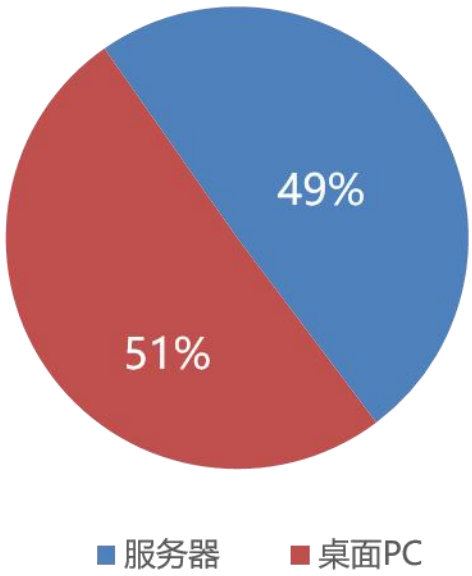
针对本月勒索软件受害者设备所中病毒家族进行统计：Makop 家族占比 21.79%居首位，第二的是占比 17.31%的 phobos，BeiJingCrypt 家族以 14.74%位居第三。



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 Server 2016。



2023 年 12 月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型服务器系统占比与桌面系统基本相当。



勒索软件热点事件

美国海军承包商 Austal 在数据泄露后承认遭受网络攻击

美国造船公司 Austal USA 是美国国防部(DoD)和国土安全部(DHS)的承包商，该公司近期证实遭受了网络攻击，并称目前正在调查该事件的影响。该公司总部位于澳大利亚，专门生产高性能铝制容器。其美国子公司 Austal USA 签订了多项项目合同，其中包括为美国海军建造独立级濒海战斗舰。Austal 还拥有一份价值 33 亿美元的有效合同，为美国海岸警卫队建造 11 艘巡逻艇。

当地时间 12 月 6 日早些时候，Hunters International 勒索软件组织声称入侵了 Austal USA 并泄露了一些信息作为入侵的证据。Austal 方面证实了此次攻击的真实性，并表示 Austal USA 迅速采取行动缓解了这一事件且未对运营造成影响。目前美国联邦调查局(FBI)和海军刑事调查局(NCIS)在内的监管机构已得到通知并将参与调查事件原因以及所获取信息的范围。Austal USA 表示攻击者没有访问或获取到任何个人或机密信息，并称正在与有关当局密切合作，将在了解新信息后继续通知受该事件影响的所有利益相关者。

Hunters International 则威胁将在接下来的几天内公布从 Austal 系统窃取的更多数据，包括合规文件、招聘信息、财务详细信息、认证和工程数据。

Akira 勒索软件团伙声称对 Nissan 澳大利亚的网络攻击

12 月 22 日，Akira 勒索软件团伙声称其侵入了日本汽车制造商日产汽车澳大利亚分公司 Nissan Australia 的内部网络。据 Akira 称，其从该汽车制造商的系统中窃取了约 100GB 的文件。攻击者还威胁要在网上泄露敏感的业务和客户数据——因为日产拒绝向其支付赎金。

“他们似乎对这些数据不太感兴趣，所以我们会在几天内公布这些数据。”勒索软件组织表示称，“档案中包含员工个人信息以及许多其他公众会感兴趣的内容，例如保密协议、项目、有关客户与合作伙伴的信息等。”

目前，日产表示仍在调查该事件的影响以及个人信息是否已被访问。同时称公司正致力于恢复受攻击影响的系统，但并未进一步透露更多信息。

育碧表示正在调查有关新安全漏洞的报告

育碧称正在调查该公司内部软件和开发工具截图在网上被公布后，相关文件是否也遭受了泄露。公司表示在安全研究团体 VX-Underground 分享了疑似是该公司内部服务的屏幕截图后，他们正在调查此次涉嫌数据安全的事件，但并未透露更多信息。

而 VX-Underground 则在推文中表示，一名未知的威胁者称他们已于 12 月 20 日入侵了育碧，还称其计划泄露大约 900GB 的数据。

攻击者声称他们获得了 Ubisoft SharePoint 服务器、Microsoft Teams、Confluence 和 MongoDB Atlas 面板的访问权限，并分享了他们访问其中一些服务的屏幕截图。虽然此次事件让人联想到育碧公司在 2020 年遭到 Egregor 勒索软件团伙攻击的事件，但 VX-Underground 团队并未透露攻击者身份，目前也没有勒索软件团伙声称对此次攻击事件负责。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

datasecurity1@tutanota.com	help@inboxhub.net	bob1997marley@zohomail.eu
datasecurity1@tutanota.com	secure5555@msgsafe.io	bob1997marley@firemail.cc
coca2024cola@zohomail.eu	team@yahooweb.co	samercin@tutanota.com
coca2023cola@libertymail.net	ironsupport@onionmail.org	intelrestore@onionmail.com
intellent.ai@onionmail.org	herkonasladok@onionmail.org	intelrestore@tutanota.com
decryptxxxhelp@xmpp.jp	r0Qp@3M	Ex2@onionmail.org
helpbtcdecrypt@xmpp.jp	ironsupport@onionmail.org	SupportRan2023@proton.me
ambu.lance@tuta.io	team@yahooweb.co	Adminsupport2023@proton.me
Mikesupp77@outlook.com	onionhunter@onionmail.org	whitehelper@skiff.com
kuipersupport@onionmail.org	help5555@msgsafe.io	whitehel@tutanota.com
Blackbit.sup@skiff.com	ironsupport@onionmail.org	briandatahelp@onionmail.org
helpdec10@decoymail.com	iron@techmail.info	briandatahelp@dnmx.org
bkffmonopp@onionmail.org	mcdonaldsdebtzhlob@onionmail.org	pmmneevqkj@onionmail.org
BlackLegion@zohomail.eu	Bigspermhorseballs@onionmail.org	protonis2023@tuta.io
blacklegion@skiff.com	temp515@msgsafe.io	regyhny@tutanota.com
masscan@tutanota.com	engines-1@tutanota.com	ergsdhu@tutanota.com
masscan@onionmail.com	aegisbackupz@gmail.com	Sc.computer1992@Gmail.com
exphelp@tutanota.com	indianguy@onionmail.org	troublemaker113@mailfence.com
helpdec11@onionmail.org	damarans@mail.ru	troublemaker113@tutanota.com
joao21@tutanotacom	damarans@outlookpro.net	tedydecrypt@elude.in
joao21@onionmail.org	sexyhorses@onionmail.org	Morning@mailfence.com

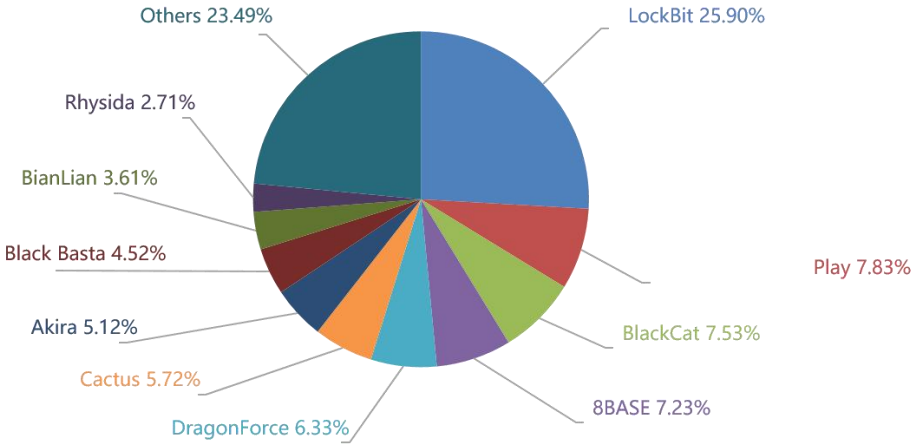
trenbtc@rambler.ru	newdataland@gmail.com	GoodMorning9@cock.li
GrafGrafel@tutanota.com	hackerone@msgden.net	GooodMorning@tutanota.com
deepmind@onionmail.org	richard.rivera@onionmail.org	Goood.Morning1@mailfence.com
StevieWalker@onionmail.org	pisunellakonososeila@onionmail.org	GooodMorning1@tutanota.com
LynwoodWalker@onionmail.org	datacenter@onionmail.com	John.Muller@mailfence.com
jshza78wfawjfawffa@proton.me	it.support@yahooweb.co	JohnMuller88@tutanota.com
HarpyRage@msgsafe.io	head@yahooweb.co	picklock@elude.in
HarpyRage@cock.li	order@cyberfear.com	agentsmith@cock.email
cacar1986@proton.me	thaihorsefuckers@onionmail.org	smith@elud.email
cacar1986@mailfence.com	anilorak@onionmail.org	ag3ntsm1th@tuta.io
dbrecover@cock.li	anilorak@onionmail.org	EmmaGaller@mailfence.com
dbrecover@cock.lu	anilorakbest@onionmail.org	EmmaGaller@tutanota.com
zuzka1819@tuta.io	showrans@mail.ru.show	EmmaGaller@cock.lu
zuzka1819@cock.li	showrans@mail.ru	Eliot.Bing@mailfence.com
locked@onionmail.org	picostrui@onionmail.org	EliotBing@tutanota.com
teodorcarrida@tuta.io	krypto@bingzone.net	JohnKarick@tutanota.com
teodorcarrida@msgden.com	krypto111@skiff.com	MikeClarke@cock.lu
TsaiShen@mail2tor.com	azadi33@smime.ninja	samantha22@tuta.io
dr.pctalk@tutanota.com	azadi33@keemail.me	jounypaulo@mail.ee
hub_you@tuta.io	antistrees2000@keemail.me	jounypaulo@tutanota.com
Dr.lockfiles@gmail.com	jackdecrypt@smime.ninja	pm24@tuta.io
Dr.helpfiles@gmail.com	antistrees2000@keemail.me	dr.files@onionmail.org
bitcoinfun_666@proton.me	fastdec@tutanota.com	dr.file2022@gmail.com
datatrader@onionmail.org	azadi3@outlookpro.net	vyptteam@zohomail.eu
conectme@tutanota.com	Merlin@outlookpro.net	@VyptTeam
camry20222@aol.com	Merlin@cyberfear.com	kilook200@gmail.com
blankqq@tuta.io	Merlin@onionmail.org	aisaragpt@proton.me
liveteam@onionmail.org	Antonia@onionmail.org	aisaragpt@tuta.io
wikilab@techmail.info	Antoni@cyberfear.com	decodoperator1@aol.com
wikilab@keemail.me	resq100@onionmail.org	decodoperator1.1@aol.com
dex.x.d98@tutanota.com	resq100@cyberfear.com	Hw2k0SZdxa@msgsafe.io
enc@cock.li	aesdecrypt@gmail.com	JnSeYvZw34@onionmail.org
lostinrusalt@tuta.io	bnbrans@outlook.com	pGU2NJ4TQk@mail2tor.com
HuiVJope@tutanota.com	alvarodecrypt@gmail.com	Q6uBdWWuu4@proton.me
howtodecryptsupport@cock.li	alvarodecrypt@outlook.com	quvn5llxkk@mailfence.com
unlocker@decoymail.net	alvarodecrypt@gmail.com	TAXASFSHWKASJFBUWBSJA@protonmail.com
king.20lord.20dec@gmail.com	alvarodecrypt@outlook.com	colin_farel@aol.com
lord20@tutanota.com	antistrees2000@keemail.me	unrasolo1970@proton.me
xakep@dark-forum.ru	jackdecrypt@smime.ninja	gameovercreation@cock.li
hackr@dark-forum.ru	recoveryanti@gmail.com	caypishijistor29@gmx.com
backmydata2@protonmail.com	ransupport@onionmail.org	protix@tuta.io
backmydata2@airmail.cc	recoveryfile7@gmail.com	protix@skiff.com

batman12345@tutanota.com	Eliberansmoware@outlook.com	secir@tutanota.com
Drman123@protonmail.com	Electronicrans@outlook.com	kopov@onionmail.org
hsvfrgwsatldzwr@hldrive.com	electronicsrans@gmail.com	helpdec10@decoymail.com
Tisak1998@skiff.com	Tpyrcne@onionmail.org	helpdecfile1@onionmail.org
Tisak1998@cyberfear.com	Tpyrcne@cyberfear.com	compotdecfrest@firemail.de
Filemgr@tutanota.com	ghosttalking@tutanota.com	helpdec11@onionmail.org
Cryptor6@tutanota.com	ghostteam@skiff.com	Decrypt.TM@zohomail.eu
snetinfo@skiff.com	toxiv1@skiff.com	Decrypt.TM@onionmail.org
snetinfo@cyberfear.com	toxiv@tuta.io	wdengminglang@cock.li
mmalcov@aol.com	mxdown@tutanota.com	tianihokeem66@gmx.com
colin_kaan@aol.com	021mail@cock.li	CryptedData@tfwno.gf
djek77d@aol.com	ryandatahelp@onionmail.org	sirattacker@mailfence.com
helpdec10@decoymail.com	returnback@cyberfear.com	sirattacker@proton.me
bkffmonopp@onionmail.org	returnbac@onionmail.org	sirattacker0@tutanota.com
backup@waifu.club	@returnbacc	miami44@gmailvn.net
blak.log@aol.com	ghostone4@tutanota.com	basg@ik.me
DevicData@tutanota.com	coca2023cola@zohomail.eu	bangthlu2@gmail.com
fastintermediary@gmail.com	srvhelp@mail.ee	WhoIsJoeMamma1234@protonmail.com
exphelp@tutanota.com	electronicrans@gmail.com	bambolina2021@virgilio.it
decryptor@cyberfear.com	DevicData@tutanota.com	r.heisler@keemail.me
@coca2023cola	Decipher@mailfence.com	hsharada@skiff.com
henderson@cock.li	buybackdata@mail2tor.com	r.heisler@skiff.com
helprecovery@gnu.gr	arricklu_forlint@tutanota.com	rainbowforever@skiff.com
rdprecovery@skiff.com	black.mirror@qq.com	rainbowforever@tutanota.com
sir.rdprecovery@protonmail.com	Kardon@privatemail.com	ghostsbackup@skiff.com
karasikharry25@gmail.com	conkichinmodl@conkichinmodl.com	summerkiller@tutanota.com
steloj@mailfence.com	Harman@privatemail.com	shadowghost@skiff.com
malkripti@proton.me	bob1997marley@zohomail.eu	lastghost@skiff.com
steloj@rbx.run	bob1997marley@firemail.cc	Rsacrpthelp@skiff.com
howrecover@tutamail.com	ablyteqotg@tutanota.com	ghosts1337@skiff.com
electronicrans@gmail.com	mcrypts@msgsafe.io	ghosts1337@tuta.io
electronicrans@outlook.com	emcrypts@msgsafe.io	mail@help8888.top
whirmx@gmail.com	balckhoues@tutanota.com	jonsrdme@tutanota.com
Whirmx@tutanota.com	balckhoues@onionmail.com	@mr_robot_unlock
ad3for@tutanota.com	decodedata@tutanota.com	everdaygreens@cock.li
17017236812@163.com	hisenberg0ger@tutanota.com	wdengminglang@cock.li
jrpvwqnnud@onionmail.org	hisenberg01ger@skiff.com	QSKhVaBPFv@onionmail.org
jonsrdme@tutanota.com	kondasbason@onionmail.org	VEGtpN4krwJgWeeJ@proton.me
DevicData@tutanota.com	datastore@cyberfear.com	huivjope@tutanota.com
decryptprof@proton.me	back2up@swismail.com	devicdata@tutanota.com
locked@onionmail.org	datastore@cyberfear.com	jopanaxye@tutanota.com
rdprecovery@mail.ee	back2up@swismail.com	sqlback@memeware.net

RDPrecovery@tutanota.com	overkill@onionmail.org	Dr.pctalk@skiff.com
patchworkapt@msgden.net	wgongruntian@airmail.cc	Dr.pctalk@tutanota.com
PatchWorkApt@tutanota.com	help.file@zohomail.eu	dr.pctalk@skiff.com
sendr@onionmail.org	torres@proxy.tg	dr.pctalk@tutanota.com
sendr@tutanota.com	torresproxytg@proton.me	DevicData@tutanota.com
itsupport831@reddithub.com	MikePierce957@gmx.com	datenklause0@gmail.com
support007@mailfence.com	d3crypt_help@proton.me	getbyback@protonmail.com
help@inboxhub.ne	new_day@torguard.tg	

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 332 个组织/企业遭遇勒索攻击，其中包含中国 6 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 4 个组织/企业未被标明，因此不在以下表格中。

Goiasa	chuzefitness.com	Hinsdale School District
Keyser Mason Ball	Kauno Technologijos Universitetas	MSD Information technology
Xerox Corp	Grupo Jose Alves	Independent Recovery Resources, Inc.
Kenya Airways	Blackstone Valley Community Health Care	Studio MF
Clearwinds	Richard Harris Personal Injury Law Firm	zailaboratory.com

contimade.cz	Schoepe Display	ISC Consulting Engineers
eagersautomotive.com.au	American Transportation	The Glendale Unified School District
Erbilbil Bilgisayar (You have 72 hours)	Waldner's	pronatindustries.com
Okada Manilla	Succes Schoonmaak	Colonial Pipeline
Banco Promerica de la República Dominicana	DYWIDAG-Systems	policia.gob.pe
krijnen.be	pecofoods.com	Qatar Racing and Equestrian Club
bellgroup.co.uk	The CM Paula	Graphic Solutions Group Inc (US)
coop.se	parat-technology.com	livanova.com
tridon.com.au	Viking Therapeutics	HMW
Nej Inc	lajollagroup.com	GOLFZON
americanalarm.com	Zone Soft	aw-lawyers.com
Northland Mechanical Contractors	Electrical Connections	midlandindustries.com
gdi.com	navitaspet.com	Travian Games
bachoco.com.mx	vyera.com	Tcman
pbssystems.com	hallidays.co.uk	Burton Wire & Cable
Wesgar Inc.	ATCO Products Inc	Precision Technologies Group Ltd
CVR Associates	Biomatrix LLC	denave.com
hoffmanestates.org	rodo.co.uk	Capespan
Ohio Lottery	E & J Gallo Winery	Becker Furniture World
EPS.RS	kohlwholesale.com	Payne Hicks Beach
Aura Engineering, LLC	New York School of Interior Design	Vitro Plus
FIRST 5 Santa Clara County	www.talbotslaw.co.uk	GVM
Lake of the Woods County	CTS.CO.UK	Planbox
Ultra Intelligence & Communications	www.fenwickelliott.com	bluewaterstt.com
richmont.edu	DSG-US.COM	omegapainclinic.com
coaxis.com	Insidesource	AG Consulting Engineering
Kellett & Bartholow PLLC	hebeler.com	Greater Richmond Transit
Bayer Heritage Federal Credit Union	Nexiga	Kuriyama of America
smbw.com.au	Fred Hutchinson Cancer Research Center	AMCO Proteins
Flash Motors	Spaulding Clinical	SML Group
Tshwane University of Technology	Heart of Texas Region MHMR	stormtech
Abdali Hospital	PCTEL	Garda
Blaine County Schools	Agl Welding Supply	Tri-city Medical Center
PC Market	Grayhill	Tasteful Selections
International Electronic Machines Corp	Leedarson Lighting	Ware Manufacturing
hendelsinc.com	Coca-Cola Singapore	Neurology Center of Nevada
co.pickens.sc.us	Shorts	CIE Automotive
walkro.eu	World Emblem International	National Nail Corp
ontariopork.on.ca	The GBUAHN	citizenswv.com
coastalplainsctr.org	Baden	directradiology.com

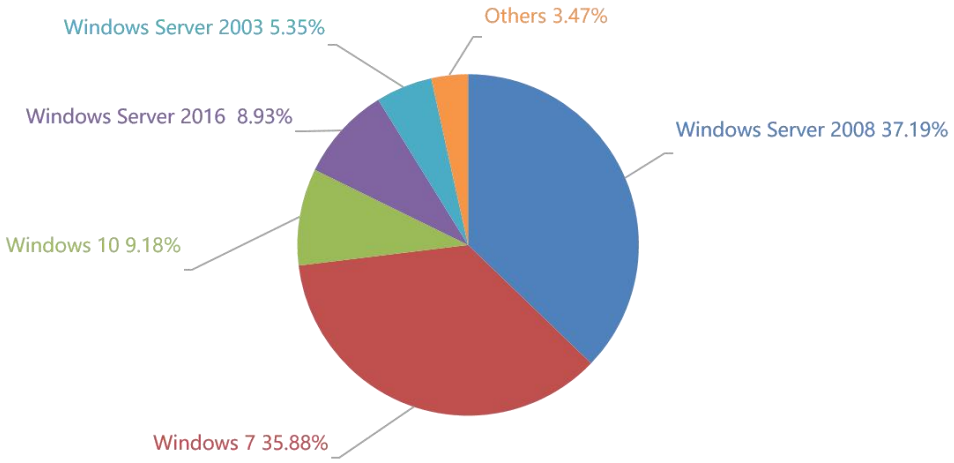
zrvp.ro	Dafiti Argentina	bpce.com
tecnifibre.com	Lunacon Construction Group	signiflow.com
Davis Cedillo and Mendoza Inc	Tglt	usherbrooke.ca
Prefeitura Municipal de Itabira	Seven Seas	hopto.com
bkf-fleuren.de	Decina	Visan
avescorent.ch	Cooper Research Technology	Tryax Realty Management
Bay Orthopedic & Rehabilitation Supply	Greater Cincinnati Behavioral Health	Deutsche Energie-Agentur
zurcherodioraven.com	goldwind.com	Campbell County Schools
quakerwindows.com	converzemedia.com	Compass Group Italia
castores.com.mx	spiritleatherworks.com	Aqualectra Holdings
VF Corporation	bemes.com	Acero Engineering
csmsa.com.ar	Chaney, Couch, Callaway, Carter & Associates Family Dentistry	syrtech.com
ciasc.mx	Commonwealth Capital	labelians.fr
whafh.com	Greenbox Loans Inc.	polyclinique-cotentin.com
hotelplan.co.uk	Hyman Hayes Associates	fpz.com
Nissan Australia	mcs360.com	ACCU Reference Medical Lab
xeinadin.com	JV Driver	Sagent
igs-inc.com	grandrapidswomenshealth.com	Lischkoff and Pitts, P.C.
sterlinghomes.com.au	pcli.com	SMG Confrere
esepac.com	austen-it.com	Calgary TELUS Convention Centre
fager-mcgee.com	dawsongroup.co.uk	astley.
denford.co.uk	ccadm.org	TraCS Florida FSU
goldenc.com	Advantage Group International	laprensani.com
Trabzon Akabat University	altezze.com.mx	aldoshoes.com
Rajamangala University of Technology	thirdstreetbrewhouse.com	mapc.org
Inwi	carolinabeveragegroup.com	skalar.com
VietNam Electricity (EVN)	Tulane University	ussignandmill.com
Zewail City	Dameron Hospital	hnncsb.org
Comtrade	agy.com	elsewedyelectric.com
DELPHINUS.COM	alexander-dennis.com	mirle.com.tw
ACE Air Cargo	Dillard Door & Security	ychlccsc.edu.hk
Kinetic Leasing	cms.law	restargp.com
Owen Quilty Professional	SBK Real Estate	CLATSKANIEPUD
Jon Richard	CACG	Akumin
Concept Data	VAC-U-MAX	Bowden Barlow Law PA
Packaging Solutions	Hawkins Sales	Rosens Diversified Inc
Bladen County Public Library	William Jackson Food Group	Gaido-fintzen.com
smudlers.com	Groupe PROMOBE	Henry County Schools
Yakult Australia	Soethoudt metaalbewerking b.v.	fps.com
Unite Here	REUS MOBILITAT I SERVEIS	Full access to the school network USA
dbmgroup.com	Tim Davies Landscaping	Agamatrix

wkw-group.com	King Aerospace, Inc.	CMS Communications
Di Martino Group	GlobalSpec	Great Lakes Technologies
Rockford Gastroenterology Associates	dena.de	Midea Carrier
HALLIDAYS GROUP LIMITED	bboed.org	nlt.com
Die Unfallkasse Thüringen	SmartWave Technologies	Getrix
NIDEC GPM GmbH	rpassoc.com	Evnhcmc
hunterbuildings.com	shareharris.com	UF Resources
larlyn.com	woodruffenterprises.com	Nida Corp
des-igngroup.com	Mitrani Caballero Ojam & Ruiz Moreno - Abogados	NCCU.EDU
dobsystems.com	The Teaching Company, LLC	Bern Hotels & Resorts
Navigation Financial Group	Memorial Sloan Kettering Cancer Center	Tipalti
Air Sino-Euro Associates Travel Pte. Ltd	airtechthelong.com.vn	Roblox
udhaiyamdhall.com	kitahirosima.jp	Lisa Mayer CA, Professional Corporation
LCGB	tradewindscorp-insbrok.com	royaleinternational.com
CETEC Ingénierie	petrotec.com.qa	inseinc.com
The International School of Management	Holding Slovenske elektarne	HTC Global Services
Employ Milwaukee	Insomniac Games	Dörr Group
Horizon Pool & Spa	greenbriersportingclub.com	IRC Engineering
socadis	phillipsglobal.us	Jerry Pate Energy
Davis Cedillo & Mendoza Inc	Azienda USL di Modena	Austal USA
WELBRO Building Corporation	r-ab.de	St. Johns River Water Management District
RCSB PDB	ipp-sa.com	Iptor
mtsd-vt.org	igt.nl	Centroedile Milano
brintons.co.uk		

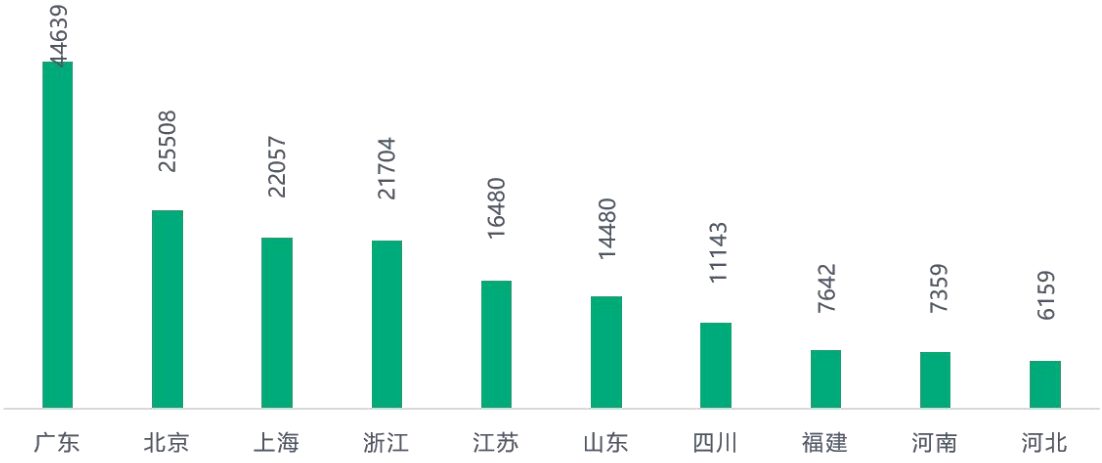
表格 2. 受害组织/企业

系统安全防护数据分析

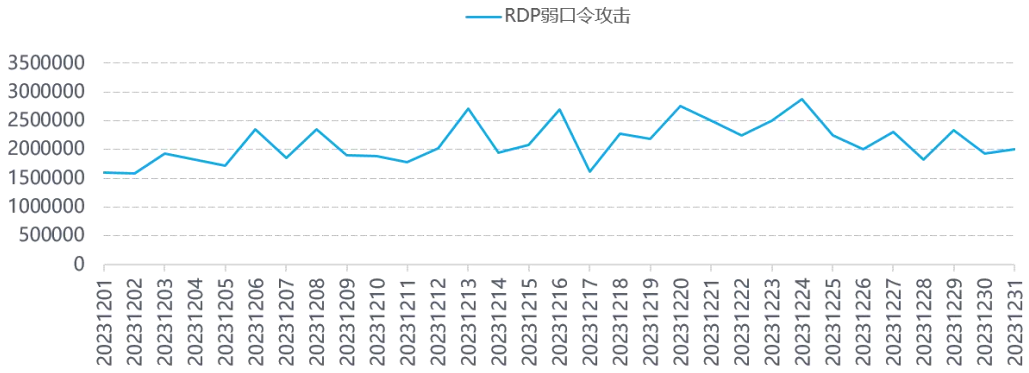
360 系统安全产品，目前已加入黑客入侵防护功能。在本月被攻击的系统版本中，排行前三的依次为 Windows Server 2008、Windows 7 以及 Windows 10。

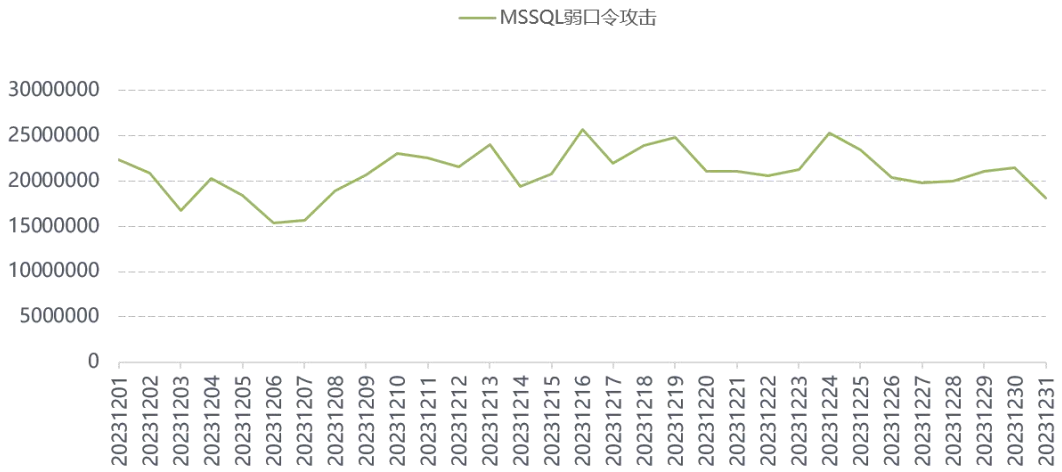


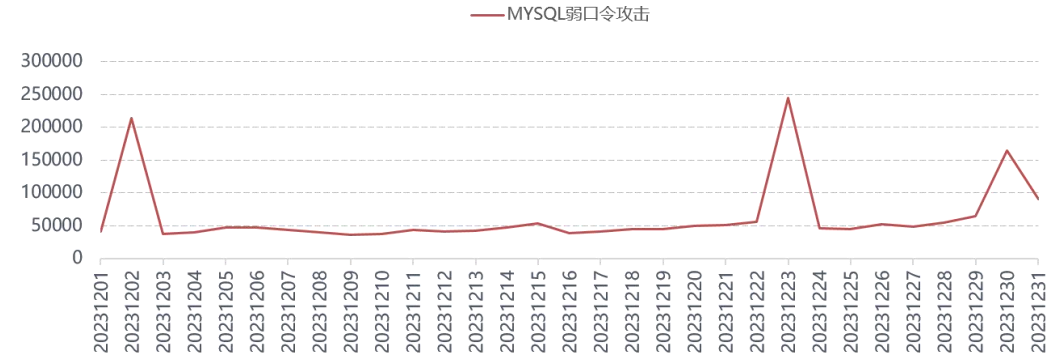
对 2023 年 12 月被攻击系统所属地域统计发现，与之前几个月采集到的数据进行对比，地区排名和占比变化均不大。数字经济发达地区仍是攻击的主要对象。



通过观察 2023 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。

- 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与数据库弱口令成功后手动投毒。
- 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。
- 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。
- mkp：同 wis。
- halo：同 360。

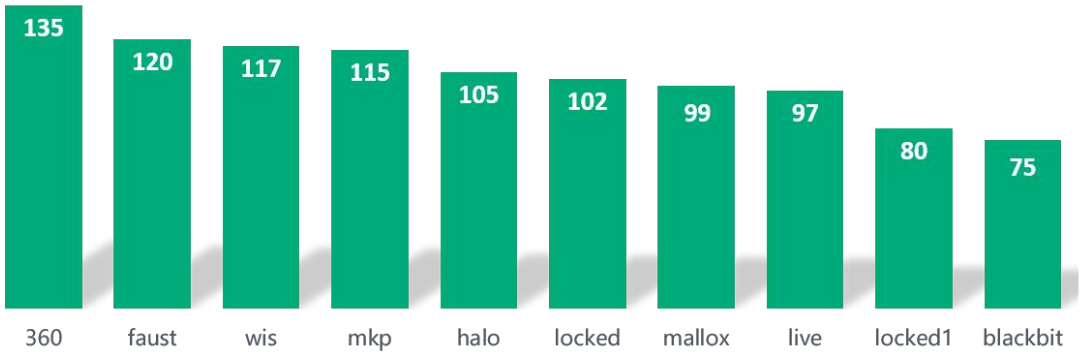
- locked：属于 TellYouThePass 勒索软件家族，由于被加密文件后缀会被修改为 locked 而成为关键词。该家族主要通过各种软件漏洞、系统漏洞进行传播。

- 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 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。

- Live：属于 Live 勒索软件家族，由于被加密文件后缀会被修改为 live 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。

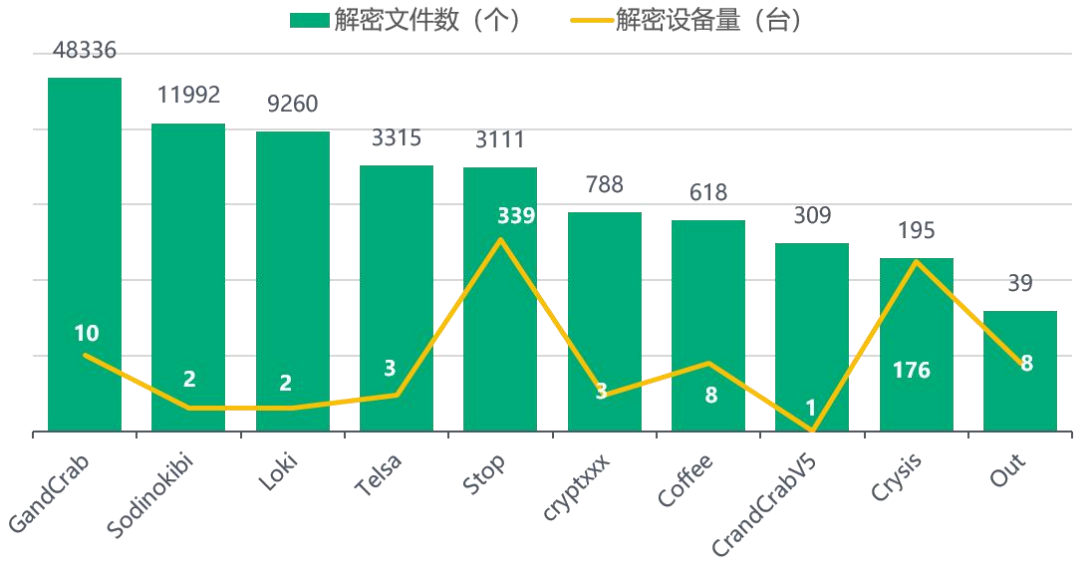
- locked1：同 locked。

- blackbit：属于 Loki 勒索软件家族的分支变种，由于被加密文件后缀会被修改为 blackbit 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。



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 Sodinokibi。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。


解密文件数（个）
解密设备量（台）
48336
11992
9260
3315
3111
788
618
309
195
39
10
2
2
3
339
3
8
1
176
8
GandCrab
Sodinokibi
Loki
Telsa
Stop
cryptxxx
Coffee
CrandCrabV5
Crysis
Out


360数字安全
数 字 安 全 的 领 导 者