勒索软件流行态势分析

2024 年 12 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。

2024 年 12 月，全球新增的双重勒索软件家族有 Bluebox，目前仅有 3 个受害组织。12 月新增的传统勒索软件家族有 RdpLocker，目前尚未监测到在国内的传播行为。

以下是本月值得关注的部分热点：

- 美国指控俄罗斯-以色列人可能是 LockBit 勒索软件开发者
- Clop 勒索软件声称对 Cleo 数据盗窃攻击负责
- 勒索软件攻击心脏手术设备头部制造商

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：TargetCompany(Mallox)家族占比 25.52%居首位，第二的是 RNTC 占比 23.45%的，BeijingCrypt 家族以 11.03%位居第三。

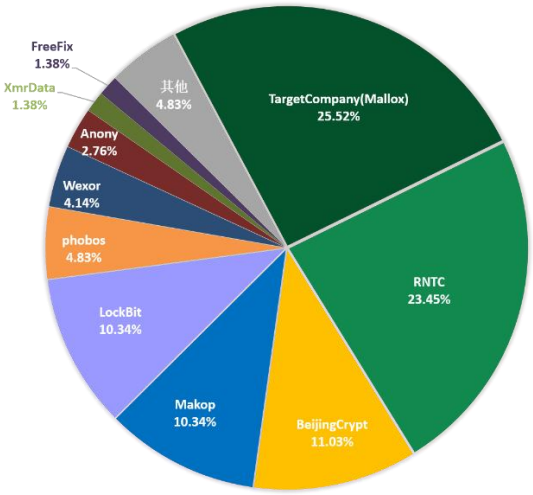

图 1. 2024 年 12 月勒索软件家族占比

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、Windows7 以及 Windows Server 2012。

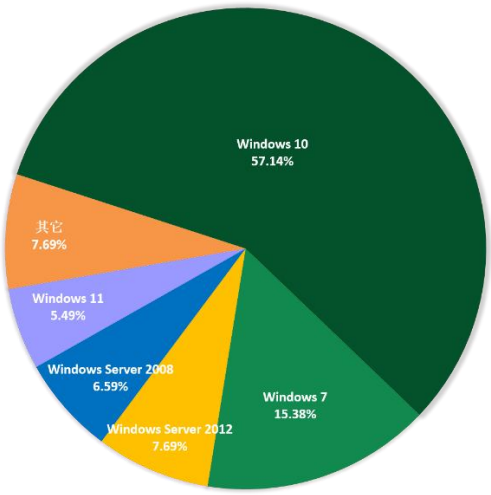

图 2. 2024 年 12 月勒索软件入侵操作系统占比

2024 年 12 月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型桌面 PC 占比大幅度高于服务器平台。

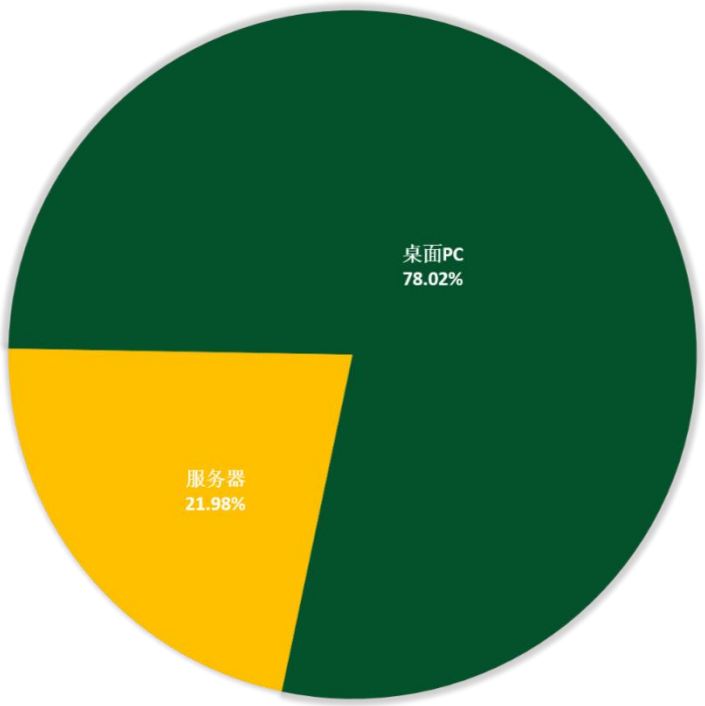

图 3. 2024 年 12 月勒索软件入侵操作系统类型占比

勒索软件热点事件

美国指控俄罗斯-以色列人可能是 LockBit 开发者

美国司法部已指控一名俄罗斯-以色列双重国籍人士涉嫌在开发恶意软件和管理臭名昭著的 LockBit 勒索软件组织的基础设施方面发挥作用。根据 12 月 20 日，新泽西州地区解封的一份刑事起诉书，51 岁的俄罗斯-以色列双重国籍的 Rostislav Panev 据称帮助开发了 LockBit 勒索软件加密程序和攻击中常用的定制“StealBit”数据盗窃工具。

Panev 于 8 月在以色列被捕，彼时他正在等待美国未决的引渡请求。刑事起诉书称，以色列执法部门在他的计算机上发现了一个在线存储库的凭据，其中包含 LockBit 加密程序和 StealBit 工具的源代码。这些存储库还包含 Conti 勒索软件加密程序的

源代码，该源代码是在 Conti 在入侵乌克兰问题上站在俄罗斯一边后被一名乌克兰研究人员泄露的。据信，此源代码已用于帮助创建基于 Conti 加密器的"LockBit Green"加密器。

起诉书还称，Panev 使用黑客论坛的私人消息功能与 LockBit 的主要运营商 LockBitSupp（现在被确认为 Dmitry Yuryevich Khoroshev）进行交流。这些消息是为了讨论需要在 LockBit 构建器和操作控制面板上编码的工作。据称，由于他与 LockBit 勒索软件团伙合作，Panev 在 18 个月内赚取了大约 23 万美元。

据称，在被捕后接受以色列警方审讯时，Panev 承认为 LockBit 勒索软件做编程工作并获得了报酬。如果 Panev 被引渡到美国，他将在新泽西州特区受审。

Clop 勒索软件声称对 Cleo 数据盗窃攻击负责

2020 年 12 月，Clop 利用了 Accellion FTA 安全文件传输平台的 0day 漏洞，影响了近百家组织。在之后的 2021 年，勒索软件团伙利用 SolarWinds Serv-U FTP 软件中的 0day 漏洞窃取数据并破坏网络。2023 年，Clop 利用 GoAnywhere MFT 平台的 0day 漏洞，使勒索软件团伙再次从 100 多家公司窃取数据。然而，根据安全公司给出的一份报告称，该团伙最严重的此类攻击是在 MOVEit Transfer 平台上使用 0day，这使他们能够从 2773 个组织中窃取数据。

目前，尚不清楚有多少公司受到了 Cleo 数据盗窃攻击的影响，也不清楚有任何公司证实通过该平台被入侵。美国国务院的正义奖励计划目前悬赏 1000 万美元，以获取将 Clop 勒索软件攻击与外国政府联系起来的信息。

勒索软件攻击心脏手术设备头部制造商

心脏外科医疗设备制造商 Artivion 近期披露了其在 11 月 21 日遭到了勒索软件攻击，该攻击中断了其运营并迫使其部分系统下线。

Artivion 的应对措施包括使某些系统下线、启动调查以及聘请外部顾问，包括法律、网络安全和法医专业人士来评估、遏制和补救事件。虽然 Artivion 在公告中没有直

接提到勒索软件，但它透露攻击者加密了其一些系统并从受感染的系统中窃取了数据。该公司还补充说，其公司运营、订单处理和运输的中断已基本得到解决，保险范围将涵盖与事件响应相关的费用。

目前，暂时没有勒索软件声称对攻击负责。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

interlock@2mail.co	help@aminyx.com	rdp3120@Firemail.de
swift_1@tutamail.com	datahelper@cyberfear.com	intelligence1spy@gmail.com
swift@onionmail.com	sn33ds3curity@tutanota.com	intelligence1@onionmail.org
OnlyBuy@cyberfear.com	vitollebonzi@gmail.com	crynoxWARE@proton.me
TechSupport@cyberfear.com	TrustFiles@skiff.com	decliv@aol.com
xioxian@onionmail.org	TrustFiles@onionmail.org	returnback24@cyberfear.com
xixian@onionmail.org	rgagfhiuehrf@proton.me	recovery012012@onionmail.org
dear_decript2022@jabbim·.com	creampie@ctemplar.com	Komardau@mailfence.com
Dear_descript2022@jabbim.com	iamy0usavi0r@protonmail.com	calltodec@tutanota.com
sonickwall@tutanota.com	hot90923@gmail.com	sxsxsax-2y9z1ee@proton.me
wangteam@skiff.com	companydata@mail.ru	tongh.za.za@gmail.com
MAGA24@cyberfear.com	thaihorsebleepers@onionmail.org	Zeus@gmail.com
MAGA24@tuta.io	Kindig@cock.li	information@jupimail.com
iracomp4@protonmail.ch	snowacabad1981@protonmail.com	efxs@tutamail.com
flame3135@proton.me	houkumlota1972@protonmail.com	kixtixcy@tuta.io
Zxulansis@onionmail.org	help@restoremydata.pw	kixtixcy@cyberfear.com
Zxulansis@mailfence.com	helprestoremydata@aol.com	rlocked@protonmail.com
zlock3d@gmail.com	restoremydata@onionmail.org	help@jexu.org

表 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）。

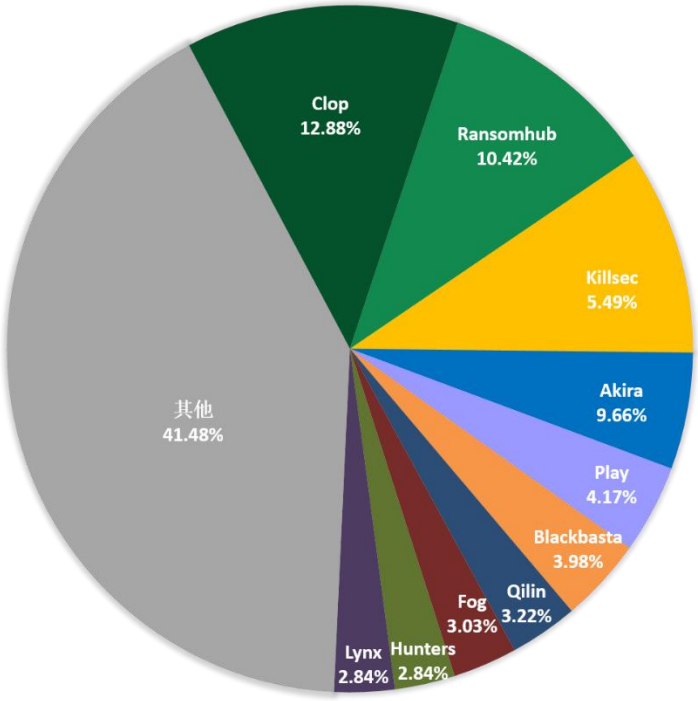

图 4. 2024 年 12 月通过数据泄露获利的勒索软件家族占比

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 528 个组织/企业遭遇勒索攻击，其中包含中国 1 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 76 个组织/企业未被标明，因此不在以下表格中。

Luxury Yacht Group	Astaphans	Haji Husein Alireza
Bettisworth North	Microvision	Mission Constructors , Inc.
McCray Lumber	Trev Deeley Motorcycles	Telecom Namibia
Zeifmans	Development Bank of Jamaica	Inmobiliaria Armas
Allen Carr's Easyway	Archetype Group	leadboxhq.com
royalinsignia.com	The Good Samaritan Health Center of Cobb	Bergerhof

starkvillesd.com	Archie Cochrane Ford	Ainsworth Game Technology Limited
spiro.k12.ok.us	National Atomic Energy Commission	Matandy (matandy.com)
byronunionschooldistrict.us	bender.de	Corporación BJR
multicoasia.com	Verosa LLC	Conrey Insurance Brokers & Risk Managers
dprinvestments.com	fote.com	Aruba Productions
UPR.SG	valveworksusa.com	Lakeside Sod Supply
asesoriacamen.es	wikov.com	Global Insurance Agency LLC
www.psccorporation.com	bathfitter.com	Proyectos y Seguros
IEC + EMCO	Vroninks Ricker Weyts & Sacre-Notaires (notassoc.be)	womenscare.com
Enge Ilha Construção	Reliance Connects (relianceconnects.com)	greenscape.us.com
Hi-Raise Constructions Holding	medion.com	Physicians' Primary Care of Southwest Florida
Megaexit	Smith Tank & Steel (smith-tank.com)	Equity & Advisory
Wosac	OL Products	thanksforthehelp.com
Innois	EMPRESARIA.COM	nedamaritime.gr
Meerapfel Family	IMSPLGROUP.COM	mpdory.com
Engenet Informatica	Cottrell Fletcher & Cottrell P.C.	Orthopaedie-hof.de
Ikav Global Energy	Giordano, DelCollo, Werb & Gagne, LLC.	Ukh-hof.de
Asheville Eye Associates	Skopos	melhorcompraclube.com.br
D&G Enviro-Group	Black Oak Casino Resort	www.bms.com
timely.mn	Fullmer Construction	copresi.es
nigico.gr	bri.co.id	www.lasalleinc.com
Cell C	activedynamics.com	Cipla
Watertown Public Schools	grimaldialliance.com	Consumers Builders Supply
STEG Stadtentwicklung	Freightlinerof Savannah	ECBM
Ire-Omba SpA	massdevelopment.com	Pelstar
Youth Eastside Services	furmanos.com	Pb Loader
Atos (Business Services · France)	Modern Dental Group Limited	Jamaica Bearings Group
VO Baker	Avstar Fuel Systems	Weinberg & Schwartz LLC
falp.org	Groupe-fimar	Milwaukee Cylinder
diazfoodsolutions.es	Tharisa	Davis Immigration Law Office
Inner City Family Health Team (ICFHT.local)	choicemg.com	Séguin Haché SENCRL
Primary Health Services Center	medisecure.com.au	Coffee Beanery
Ober Mountain (OberGatlinburg.com)	redknee.com	C Pathe
Family Help & Wellness	nbleisuretrust.org	bankily.mr
Pergher Notariat	kuritaamerica.com	Hosting.co.uk
Caframo Limited.	chaves	Mint Pharmaceuticals

E-Tank	Kilgore Industries	inia.es
Charlie's Tax Service	A Geradora	Boston Chinatown Neighborhood Center
Pinno Construction	Toscano Law	CK Technology Group
Ramos Law	Polskie Wydawnictwo Muzyczne	Town of Whitestown - NY Highway Department
Rio Negro	A Beautiful Pools Inc	Gulf Petrochemical Services & Trading
MLP Tax & Financial Services	Fireproof Contractors Inc	Matlock Security Services
McCormick & Priore	SpeedLine Solutions (speedlinesolutions.com)	Black Creek Community Health Centre (bcch.local)
Michelle Accesorios	Ouro Verde (ouroverde.net.br)	Arc Community Services Inc
Car Care Plan - Turkey	Heritage Bank	CO-VER Power Technology SpA
Aroma Housewares Co (Aromaco.com)	Brockton Neighborhood Health Center	T&M Equipment
Reutone	Ecritel	RJM Marketing
Supraterra	Joshua Grading & Excavating	Medical Technology Industries, Inc.
Inteleca	South Plains Implement	Precision Walls
Tillamook Country Smoker	Chemitex SA Information	Blue Yonder
itca.edu.sv	www.specialtree.com	LTI Trucking Services
etplaw.com	Lanigan Ryan	pro-mec.com
T Smiles Dental	Welker	Port of Rijeka
sensualcollection.com	eisenhowerlaw.com	Originpath Group
Sistem Informasi Pengelolaan Keuangan Daerah (SIPKD) - Blora Regency	Hatfield Consultants	Pan Gulf Holding
blueyonder.com	favbet	pez.com
SeaLandAire Technologies	Super Vac	casaimports.com
Relate Infotech	CM Buck & Associates	ktpartners.ca
Good Neighbors Credit Union	bushandburchett.com	Brodsky Renehan Pearlstein & Bouquet, Chartered
Anonymous Victim.USA	SWDAKOTAH.COM	Levicoff Law Firm, P.C
Baker Tilly Morrison Murray	Time Machine Inc	Max Trans
Kern Services	FINN	ITO EN
Farrar & Ball	Williams Tank Lines	Standard Calibrations
acwlaw.com	Engineered Tower Solutions	NatAlliance Securities
www.globelink.com.au	Marine Floats	azpay.me
klingler-installationen-gmbh	Waverley Christian College (wcc.vic.edu.au)	SRP Federal Credit Union
Flamco	National Air Vibrator	Aptus Value Housing Finance India Ltd
tsebrakes.com	www.prixet.com	Anonymous Victim.IT
marmon-herrington.com	baseisapis.it	Star Shuttle Inc.

intellinet-es.com	Great Plains Bank	Dorner (dorner-gmbh.de)
www.semfin.com	Cognity (cognity.gr)	hanwhacimarron.com
www.mccoyglobal.com	Diferencial Energia	www.aliorbank.pl
awimc.com	Simmtech Co., Ltd.	frigopesca.com.ec
galatachemicals.com	Acumen Group	USA2ME
9fsfalcons.org	LaSen	NIER Ingegneria S.p.A
n4telecom.com.br	scania.pl	Interspiro AB
linebank.co.id	www.aflak.com.sa	islandphoto.com
SmartLynx Airlines SIA	GNS Cloud	troxlerlabs.com
RODS Surveying (rods.cc)	Concession Peugeot	Donnewalddistributing
Albion College	JSSR Options Co., Ltd. (JSSR)	hobokennj.gov
Rhode Island Departement of Humain Services	Tumeny Payments Limited	FF Steel
Billet Precision	Westfield Fire Department	NTrust
Forum Architecture & Interior Design (forumarchitecture.com)	North Los Angeles County Regional Center	www.d47.org
Gallade Chemical (galladechem.com)	Clarkson Insurance Group	Deloitte UK
Industria e Comercio Jolitex Ltda (jolitex.com)	Midland Turbo	copral.com.br
ptcky.com	First Baptist Church	www.certifiedinfosec.com
adveo.com	Kandelaar Electrotechniek	hamptonsecurities.com
ibericar	Light Speed Design	g-s.co.uk
Sicoob	Levinlaw.com	cafezupas.com
Blome International	American Computer Estimating Inc	westbankcorp.com
BRIGHT BOLT ENTERPRISES INC	MedRevenu Inc	btci.com
Casa Juarez Restaurant Supply Co	Mid Florida Primary Care	beko-technologies.com
Davis Products Company Inc	Anetic Aid	snatt.it
Economy Restaurant Equipment And Supply Company	Tri County Property Management	medicacorp.com
GAMKA SALES CO. INC	Archdiocese of Louisville	lornestewartgroup.com
Greater Michigan Distributors	muswellbrook.nsw.gov.au	vossko.de
GPM Lawn Sprinkler Supply	www.hashem-contracting.com	ISEKI and CO.,LTD
Greene Supply Company	Kazyon	westbornmarket.com
Hammons Supply Company	António Belém & António Gonçalves	www.sefiso-atlantique.fr
J AND S Electrical And Lighting Supply LLC	An independent private assets manager	marietta-city.org
LAMERS ENTERPRISE INC	Luxor Capital Group	EuroDruk
Langford Tool And Drill Co	Myhealthcarebilling	InnoGroup
McCally Tool and Supply	Talascend	Marine Stores Guide
Abrasive Supply Corporation	Sigarth	TRAFILERIE ALLUMINIO ALEXIA S.P.A.
Albert Paper Company	Long Beach Convention Center	Communicare Inc.(US)
Allied Packing And Rubber Inc	Maxus Group	Inland Tarp & Liner

Avana Electrotek	SBW	www.siapenet.gov.br
Badger Popcorn And Concession Supply Company	Sunline	SGS Co (US)
berkotfoods.com	Goins Law	internetway.com.br
Grupo Bébécar	Arnott	www.iscinc93.com
CLARKE CENTRE D'IMAGERIE MEDICALE INC.	Artemis Holding	www.fibrogen.com
GNK Golf	Gills Onions	www.z2data.com
www.groupe-setcar.com.tn	Wintergreen Learning Materials	www.giorgiovisconti.it
Grupo Vargas	AFD	www.kiswire.com
gilariver.org	GBC	www.dalgroup.com
Accolent ERP Software	Southern Acids	www.goethe-university-frankfurt.de
Izmocars	recope.go.cr	www.wsgcpa.com
Genie Healthcare	Brasilmad	Conteg
Frameworks	Estar Seguros, S.A.	InterCon Construction
Schenkelberg - Die Medienstrategen (schenkelberg-druck.de)	cityofmarlow.com	Royce Corporation
Village Community School (vcsnyc.org)	nbkenney.com	ACM_IT
Circle Electric (circleelectric.com)	Biodimed	RDC
tabocas.com.br	Watsonville Community Hospital	IDN
PT Pertamina	Locke Solutions , LLC	Goodwill North Central Texas
Howell Township Public Schools (howell.k12.nj.us)	CW Lighting, LLC	Harel Insurance (Shirbit Server)
EP Holdings (epholdingsinc.com)	Compass Communications	New Age Micro
Khalil Center	Sarah Car Care	Billaud Segeba
Water Utilities Corporation	Interforos Casting	Textiles Coated International
planetgroup.co.il	Tejas Office Products, Inc.	Robson Planning Group, Inc.
JRT Automatisation	Planters Telephone Cooperative (planters.net)	Care Age of Brookfield
www.tekni-plex.com	midwest.com	salesgig.com
austinsfs.com.au	AC Technical Systems	KHKKLOW.com
City of Noblesville	Bianco Brain & Spine	Conlin's Pharmacy (conlinspharmacy.com)
Jet Edge (jetedgewaterjets.com)	Cristal y Lavisa S.A. de C.V.	Avico Spice
Energy Capital Credit Union (eccu.net)	Primary Plus	Down East Granite
ProCaps Laboratories	www.minerasancristobal.com	Wiley Metal Fabricating
Krispy Kreme	NSK Group ROTA	tascosaofficemachines.com
Broker Educational Sales & Training	Rutherford County Schools	shapesmfg.com
Jared Beschel and Associates	Westerstrand Urfabrik AB	everde.com
Hide-A-Way Lake Club	PH ARCHITECTURE	qualitybillingservice.com
Compliance Solutions Inc	Matagrano	costelloeye.com
Leyman Manufacturing	Renée Blanche	McKibbin

federalbank.co.in	Nova Pole International Inc.	apeagers.com
bataviacontainer.com	Hydra-Matic Packing	Alpine Ear Nose & Throat
Banner Day Camp	tectaamerica.com	

表 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。

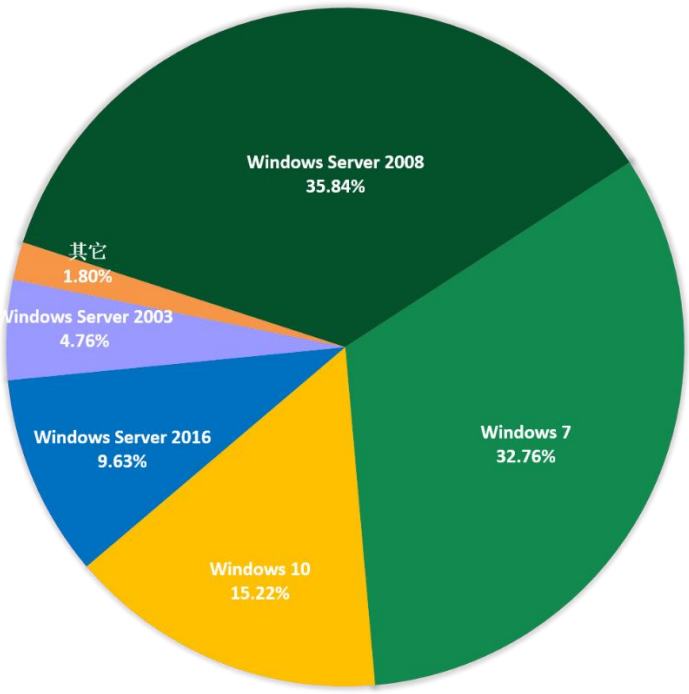

图 5 2024 年 12 月受攻击系统占比

对 2024 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。

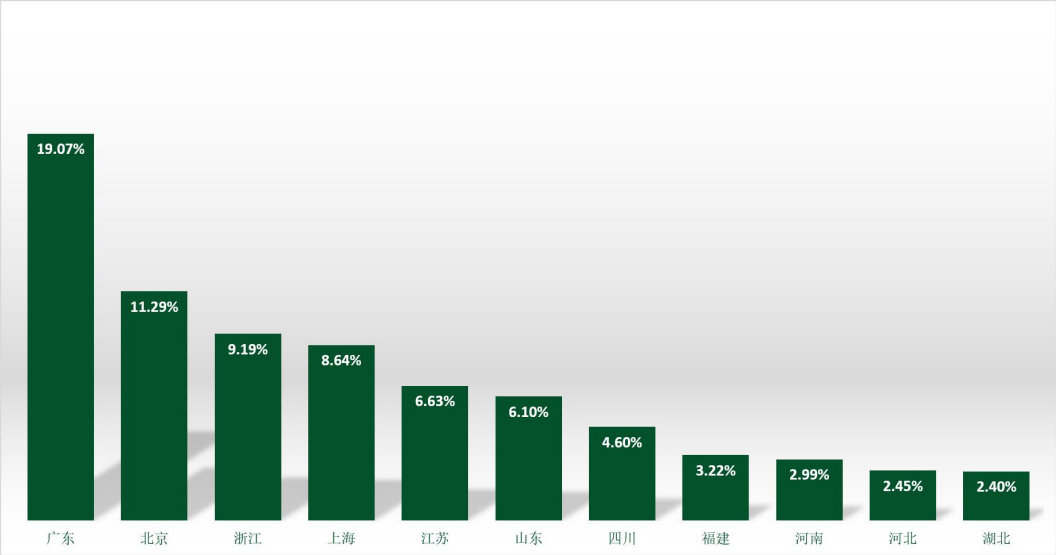

图 6. 2024 年 12 月国内受攻击地区占比排名

通过观察 2024 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。

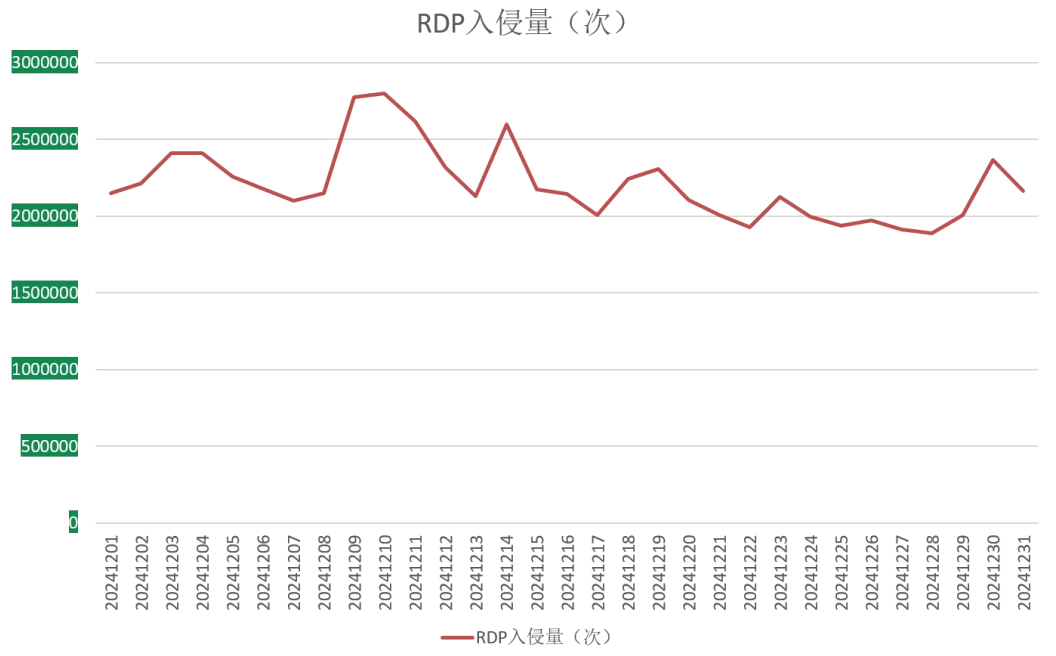

图 7. 2024 年 12 月监控到的 RDP 入侵量

关于 MS SQL 的入侵，12 月 30 日的数据由于一些设备被大量暴破导致数据大幅增高，随后即恢复正常水平。

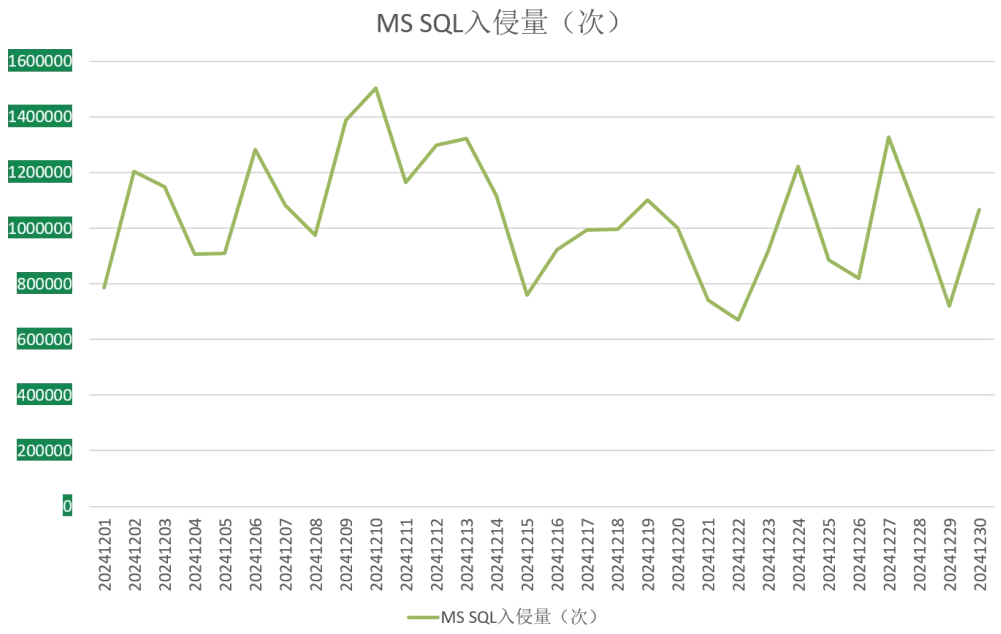

图 8. 2024 年 12 月监控到的 MS SQL 入侵量

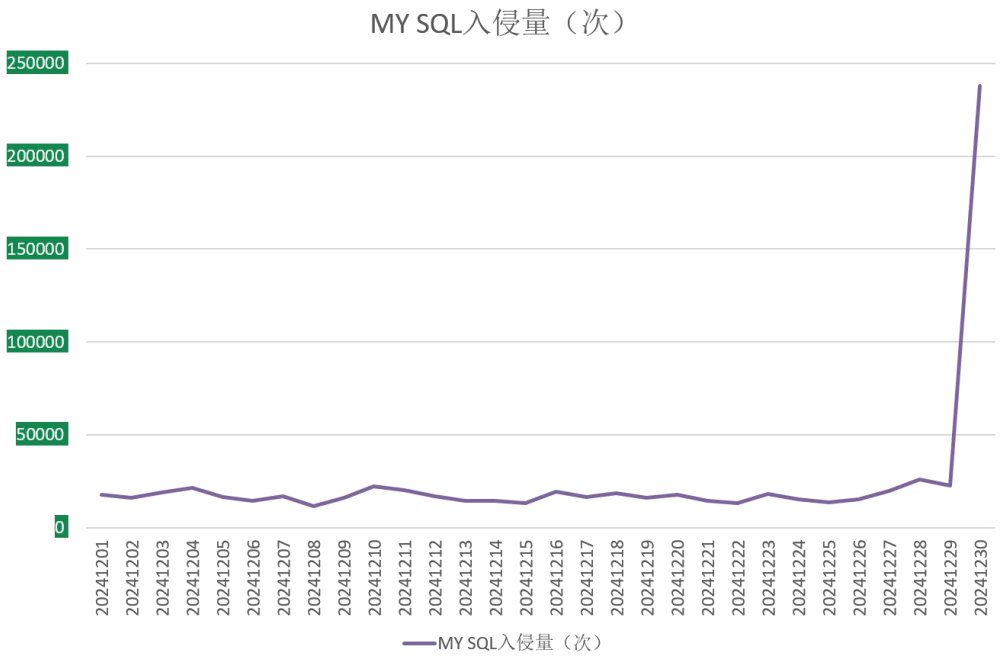

图 9. 2024 年 12 月监控到的 MYSQL 入侵量

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。

- hmallox：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，今年起增加了漏洞利用的传播方式。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。
- wstop： RNTC 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，同时通过 smb 共享方式加密其他设备。
- Weaxor：属于 Weaxor 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，同时通过 smb 共享方式加密其他设备。
- 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。
- baxia：属于 BeijngCrypt 勒索软件家族，由于被加密文件后缀会被修改为 beijing 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。
- bixi：同 baxia。
- rmallox：同 hmallox。
- src：同 mkp。
- devicdata：同 hmallox。

- 888：属于 Nemesis2024 家族，以勒索信中的 Nemesis 家族字段命名。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。

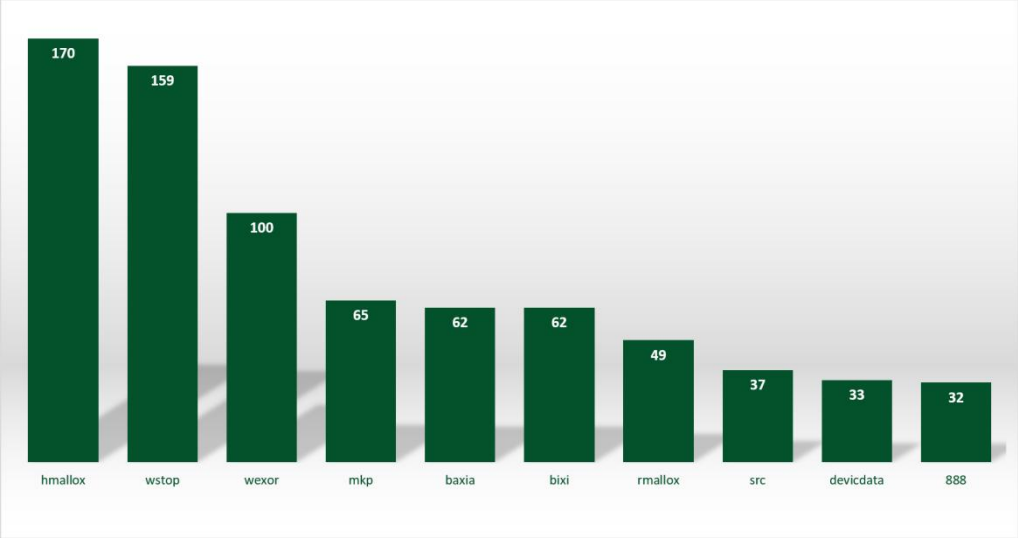

图 10 2024 年 12 月反病毒搜索引擎关键词搜索排名

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 Telsa。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。

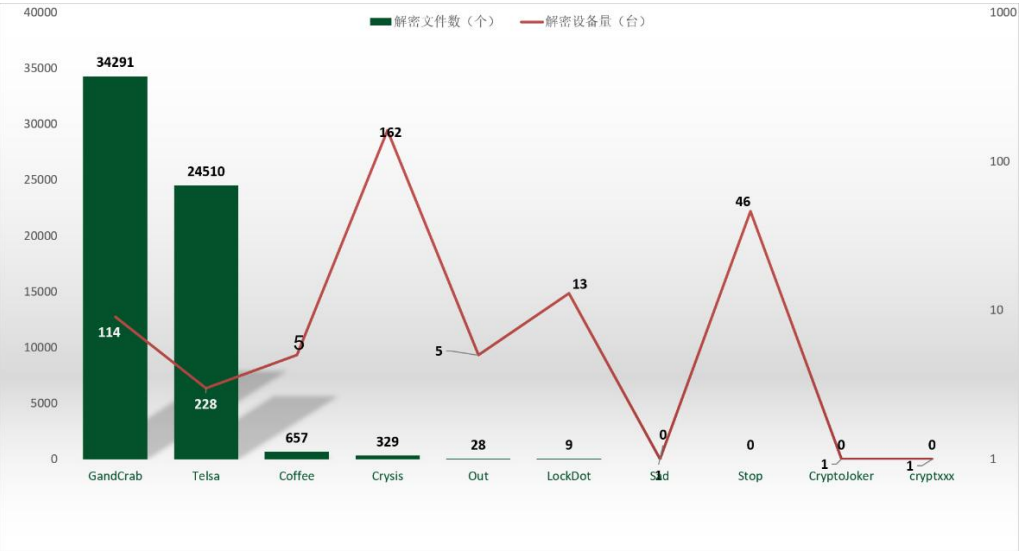

图 11. 2024 年 12 月解密大师解密文件数及设备数排名


360数字安全
数 字 安 全 的 领 导 者
360安全大脑