

勒索软件流行态势分析

2025 年 12 月



三六零数字安全科技集团 | 高级威胁研究分析中心

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，为需要帮助用户提供 360 反勒索服务。

2025 年 12 月，全球新增的双重勒索软件有 MintEye、MS13-089、Sicari、Osiris、Dark Shinigamis 家族，传统勒索软件家族新增 MiddCrypto、Marabu 等多个家族。

其中 MiddCrypto 家族通过钓鱼方式进行传播，通过植入付费软件的注册机程序进行传播。该勒索软件采用 .NET 进行编写，加入了大量混淆与环境检测试图绕过安全软件识别。在经过其云控的复杂条件筛选与用户画像识别后进行加密，加密后会从云端下载二维码引导受害者支付解密赎金。360 反勒索团队在接到用户反馈后第一时间进行了分析并提供了解密方案。Marabu 家族则是一个使用 Rust 语言编写并同时大量使用了 AI 辅助进行代码生成的勒索家族，该家族主要攻击 Linux 平台。

本月国内热门的 Top1 家族 Weaxor 家族进行了一次变种，主流加密后缀变更为 .rx，攻击方式依旧是利用 Web 漏洞发起攻击，并通过注入系统进程轮询加载漏洞驱动，与安全软件做内核对抗。

以下是本月值得关注的部分热点：

- 1** LockBit5.0 强势回归
- 2** 新型 DroidLock 可锁定安卓设备并索要赎金
- 3** PornHub 因黑客窃取高级会员活动数据而被勒索

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：Weaxor 家族占比 32.65% 居首位，第二的是 Wmansvcs 占比 24.49%，Beast 家族以 10.2% 位居第三。

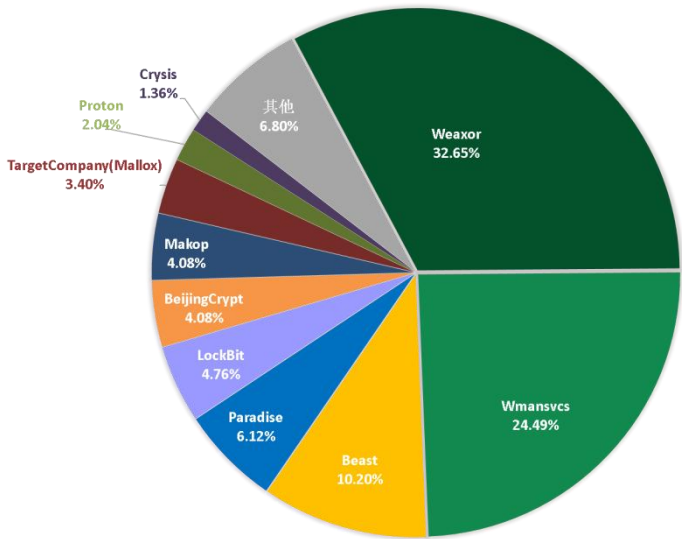


图 1. 2025 年 12 月勒索软件家族占比

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、Windows Server 2012 以及 Windows Server 2016。

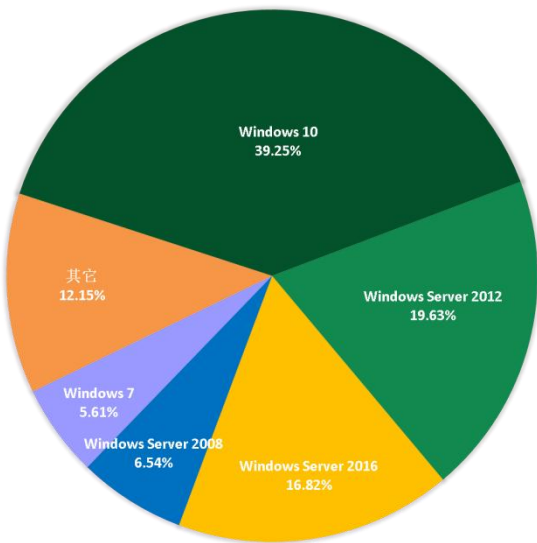


图 2. 2025 年 12 月勒索软件入侵操作系统占比

2025 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与桌面 PC 完全持平。

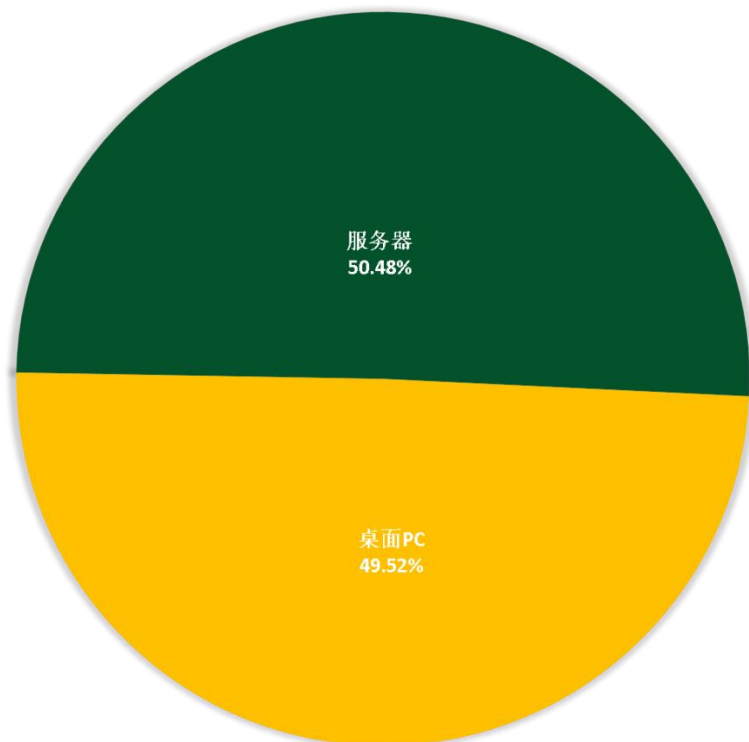


图 3. 2025 年 12 月勒索软件入侵操作系统类型占比

勒索软件热点事件

LockBit5.0 强势回归

12 月初，LockBit5.0 版本发布页面正式回归。在此期间 360 已捕获了该版本的大量在野样本。仅在短短一周内 LockBit5.0 就发布了 41 个受害者的勒索信息，其中涉及 2 家中资企业。其实 LockBit 家族长期以来并未因境外监管机构取缔而消亡，其自身与衍生家族在国内常年传播，并攻击了大量中小企业与个人用户。本次针对大型企业暗网勒索发布页的强势回归，需引起广大企事业单位重视。

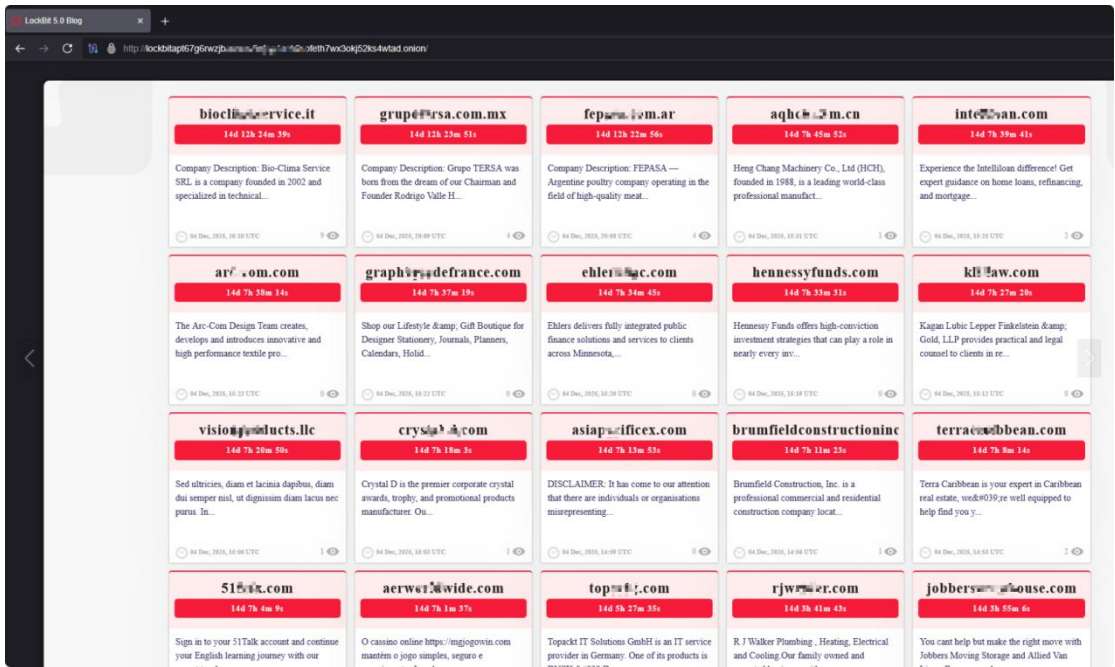


图 4. LockBit5.0 暗网主页

早在今年 9 月份,LockBit5 新版招募合作伙伴期间就曾经预告过新版将增加更多攻击形式。在本轮攻击中 360 反勒索服务也第一时间证实了新的攻击形式：即采用多轮人工参与的电诈模式，由此前的广撒网式钓鱼升级为定向钓鱼攻击。

此前各国公开的权威安全报告中（官方机构 / 安全厂商 / CERT 通报），很少有明确披露真实具体的 LockBit 定向钓鱼(spear-phishing)案例细节——比如具体受害者、邮件内容、攻击邮件链路等。官方大部分说明是基于技术分析与 ATT&CK 术语层面的合理推断或可能性，而非公开“某某公司被 LockBit 通过定向钓鱼攻陷”的具体、可核

查的实例。



图 5. LockBit 勒索软件利用定向钓鱼方式入侵系统

新型 DroidLock 可锁定安卓设备并索要赎金

DroidLock 是一种新发现的 Android 恶意软件，专门针对西班牙语用户。该恶意软件通过恶意网站分发，伪装成合法应用程序，诱使用户安装。安装后，DroidLock 能够完全控制受感染设备，锁定屏幕并要求支付赎金，还能访问设备中的短信、通话记录、联系人、音频记录，甚至删除数据。攻击者通过 VNC 分享系统实现远程控制，并能窃取设备的锁屏图案。

DroidLock 的感染过程始于一个被称为 "dropper"（引导程序）的恶意应用。这个应用伪装成正常软件，诱使用户安装，并加载实际的恶意负载。一旦恶意软件安装成功，它会通过应用更新请求，将主恶意代码传送到设备上。此时，恶意软件会请求设备的管理员权限和辅助服务权限，以便执行各种欺诈性操作。

DroidLock 通过在受感染设备上显示覆盖层，显示勒索信息，要求受害者支付赎金，否则会威胁永久删除文件。与传统的勒索软件不同，DroidLock 不加密文件，而是通过威胁删除文件来达到勒索目的。攻击者还可以通过修改锁屏密码，进一步限制用户访问

设备。此外，DroidLock 还支持多达 15 个恶意命令，包括发送通知、启用相机、恢复出厂设置、安装卸载应用等。

DroidLock 的另一个显著特性是窃取锁屏图案。当用户在恶意覆盖界面上绘制锁屏图案时，图案会直接发送给攻击者，允许其远程控制设备。攻击者可以通过 VNC 远程访问设备，进行进一步的恶意操作。

PornHub 因黑客窃取高级会员活动数据而被勒索

成人视频平台 PornHub 近日披露，其部分 Premium 会员的搜索和观看历史数据被用于勒索，幕后团伙为知名数据勒索组织 ShinyHunters。事件源于第三方数据分析服务商 Mixpanel 在 2025 年 12 月 8 日遭遇一次短信钓鱼攻击，攻击者借此入侵其系统并窃取客户数据。PornHub 表示，受影响的仅为少量 Premium 用户，且并非 PornHub 自身系统被攻破，用户的密码、支付及财务信息并未泄露；相关数据主要是 2021 年或更早的历史分析数据。

ShinyHunters 向 PornHub 发出勒索邮件，声称窃取了 94GB、约 2.01 亿条记录，内容涵盖 Premium 用户的邮箱地址、活动类型、地理位置、视频 URL、视频名称、关键词及具体时间戳，包括观看、下载、频道浏览及搜索历史等高度敏感行为数据。

Mixpanel 则回应称，无法确认这些数据来自 2025 年 12 月的安全事件，并表示相关数据最后一次访问来自 PornHub 母公司的一名合法员工账户（2023 年）。

这是首次公开确认 ShinyHunters 是 Mixpanel 事件背后的攻击者。该团伙 2025 年还涉及多起重大数据泄露，并关联 Oracle E-Business Suite 的 0day 漏洞及多起 Salesforce 相关攻击。同时，ShinyHunters 正在打造新的 RaaS 平台“ShinySpid3r”，进一步扩大其网络犯罪活动。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

defukom@cock.li	crackerfx@cock.li	head666@tutamail.com
LyricSullivan@proton.me	l2ddsqb@protonmail.com	head777@onionmail.org
CaPorter1997@proton.me	coddecryptor@hotmail.com	decrypttools@disroot.org
dageda@tutamail.com	cryptoinvest2019@protonmail.com	xvfxgw3929@protonmail.com
lgqwq8888@onionmail.org	tokaev123@proton.me	xvfxgw213@decoymail.com
mrdecdata@gmail.com	zerobases@atomicmail.io	fastdrop1987@onionmail.org
mrdecdata@hotmail.com	voyager010@aol.com	needheplcry@cock.li
sanert@cyberfear.com	voyager@cock.li	karloskolorado@tutanota.com
yatesnet@cock.li	yilaw37@hotmail.com	bugervongir@outlook.com
hannywochalfol9ar@outlook.com	ano2025@mailum.com	assistkey@outlook.com
emperor_recovery@proton.me	Pent140@tutamail.com	dwhhjzi081@mail2tor.email
unlck4u@tuta.io	files.recovery@mail.ru	chaos88888@protonmail.com
unlck4u@atomicmail.io	rosariley198357@gmail.com	anttnchf@mailfence.com
backtoback@cyberfear.com	aocpocqotox@onionmail.org	restore.bab.yk@rambler.ru
datahelper@mailum.com	360recov@gmail.com	kat6.16st6r@yandex.com

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）。

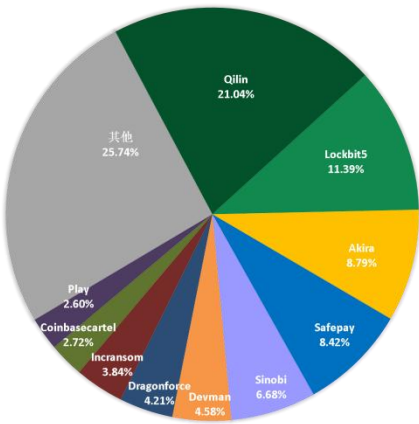


图 6. 2025 年 12 月通过数据泄露获利的勒索软件家族占比

以下是本月被双重勒索软件家族攻击的企业或个人。若未发现数据存在泄漏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 808 个组织/企业遭遇双重勒索/多重勒索攻击，其中包含中国 7 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 21 个组织/企业未被标明，因此不在以下表格中。

Sedgwick Government Solutions	North Star Asset Management	The Center of Association Management
OSI Systems, Inc.	eagrealtyinternational.com	Hardesty & Hanover
Stewart Engenharia	rogitz.com	Chastain & Associates
Auforum AG	reger-zahntechnik.de	Rodenburg Law Firm
Midkiff, Muncie & Ross, P.C	springersjewelers.com	GearGrid
Falk, Waas, Hernandez, Cortina, Solomon & Bonner Overview Metrics	dfcsystems.de	Computing Dynamics
Fitzpatrickhotels.com	kenalex.ca	Municipality of North Perth (Canada)
collinscomputing.com	meyer-lift.de	The Wardlaw-Hartridge School
drogales.com.br	coloradopowerline.com	Empresas Maggi
eroselevators.com	peus-muenzen.de	grupopuma
esopdirect.com	capsum.com	Tele-Fonika Cable Americas
fortishealthcare.com	glasserstv.com	chemstress.com
BioNet-Asia	Publicidad Sarmiento	Serratelli Hat
ManageMyHealth - New Zealand	MAT 4Site Engineers	Cagayan Appliance Center
Firmengruppe Hoffmann	Culinary Jet Concierge	Acu Trans Solutions
setex-textil.de	keystoliteracy.com	Arabian Escapes
davidrosenbakerysupply.com	pdcn.com	Homes 4 Life
knightgroup.co.uk	tuscon-physicans.com	Elysian Real Estate
moorelumber.com	clarindahealth.com	Harbor Real Estate
usdaw.org.uk	maasa.com.ar	Savills Middle East/Cluttons
investigacionesmedicas.com	axxel.biz	Betterhomes
sproutnet.com	firststrateak.com	Hunt & Harris Real Estate
precisionaluminum.ca	jvdbassoc.com	Coldwell Banker UAE
estrumar.es	walters-group.co.uk	One Broker Group
Genoa Lakes	Global Miami JV	Sotheby's International Realty
Esquire Brands	Susquehanna Glass	screenate
JZ Russell Industries	Thunder Bay Counselling	koncept law
MP Filtri	Sampoerna Agro	caryanams
C&r Electric	Shamrock Technologies	playroll
surfishtrade.com	Callipo Group	seajob
klax.de	Melsing	b2be.com
labayenylaborde.com	Colonial Metals	Hazel Mercantile
samkee.com	Flavor Producers	thinkmarkets.com

SEACSUB S. p. a.	SPZC	Sterling Biotech
Burnex	Rconcept	Seipi
NK Technologies	The Genesis Group	Poyntell Limited
Saudi Icon	Maison Law	Redi Carpet
selp	Larry Pitt & Associates	Canno Design
Grupo Hafesa	Club Atlético River Plate	sandiegowarroom.com
Sintac Recycling	Josh Steel	www.goodmanmfg.com
ESSPL	Shah Law Office	www.futureal.hu
Willowdale Steeplechase	MG Chartered Professional Accountant	www.bkcolombia.org
INHA University	Solumek	www.holidaypalace.com
Arkan	Lawsoft	hohmartin.org
pau.at	allenprinting	The Landreau Group
APC Home Health Service	Clarksville ISD	www.eliteflower.com
omrania	Pacific Rim Mechanical	PH Molds
klinge	Heritage Engineering	AGI Group
Goodwin College	RK Centers	Nadel Architects
Questica	Ragland & Jones, LLP.	RUEZ
Seac	L S GRIM	Transimpex Warenhandelsgesellschaft
Neurological Associates	South Shore Tool & Die	TCG
Intonu.com	Lawrence Family Jewish Community Center	SLA.DK
Jennings SD	Optimum Window Manufacturing	Carbon Graphics Group
sharinc.org	The Salarpuria Sattva Group	Nickman, DHK Architects, Profondia, Talbot & Associates, Fishbowl Solutions.
Atalian	NBS Canada	City of La Vergne
JBS	FHIABA	VoiceTeam Call
heatcel.co.uk	Behr Enterprises	https://www.revnomix.com
ryc.org	Associated Thermoforming	Capo Brothers
studioelad.it	L.O. Trading	HESCO
debralmorrison.com	KOEL.CO.IN	Comcast
hmpccpa.com	Farwest Fabrication	Granjas 4 Irmãos SA - Agropecuária, Indústria e Comércio
vanvenrooy.com	Phillips Scales	Ernest Käslin
wadzeck-stiftung.de	Telechaim	Big Lar
inpipeproducts.com	Best Hotels Spain	Caldwell & Company Accounting
larosadelmonte.com	Grandes Vinos	Jeffrey W Krol & Associates
Typhoo Tea	Morningstar Properties	David M. Schwarz Architects
Dom Development	Household & Commercial Products Association	Gopher Industrial
Caramel	beausejourco-op.crs	gotec
Centro Médico Palafox	The Araneta Group	elematec
BMW Guatemala	deerfield.com (singulargenomics.com)	pharmaciedesalize.com.fr

VALLEREDONDO	MedHelp	arko.no
Hometech Window	CVK Hotels & Resorts_Turkey	Galesi Group
Georgia Dermatology & Skin Cancer Center	seguriamericas.com	Quality Companies
Ortho Mattress	smilecenterutah.com	Marta Montserrat Areny Guerrero ABOGADO
Hopital La Rabta	silverlinegroupinc.com	Sanko Air Conditioning Co., Ltd.
drako.com.mx	notar-gerresheim.de	La Costa Dental Excellence
inspired.ee	artcitydental.com	Acoustical Control
zszeleznice.cz	gandlmechanical.com	AMH Philippines
urfishtrade.com	zimeda.eu	Kane's Furniture
towellholding.com	PODOVIA	YAZAKI Corp
tecnicarobertorocca.edu.ar	Adelman & Gettleman	milanoristorazione.it
technicare.com.br	ACME Industrial	kap.co.th
tealca.com	Latitude 33 Planning& Engineering	cadopt.com
soeuae.ae	Netstar Australia PTY Ltd	four-points.marriott.com
savantivibranti.com	Axion50plus	iscot.it
puzio-saunierduval.fr	Amla Commerce	tracsa.com.mx
optral.com	SASP SNCC AUTOMATISME SOLUTIONS PROCESS	chmsbc.org.br
omf.org	Pueblo West Colorado	elundini.gov.za
occgrouptr.com	Eurofret Transports Et Logistique	comune.balmuccia.vc.it
mostykatowice.pl	Hr Björkmans Entr é mator	felixvet.com
prommgroup.com	Capital + Safi	physiciansmedicalbilling.net
q-ads.com	Ciif	incolease.com
smed.at	Ferreteria Scopazzo	Mintzer Sarowitz Zeris Ledva & Meyers
clipan.co.id	Roose Ressler & Green Co	Fish & Richardson Overview Metrics
mc2engineers.com	Smith Hawks	Benchmark Electronics Inc
lfval.net	https://avenira.com/	Ermat Grup
laval-virtual.com	Holiday Tours	www.toc.co.jp
kraslice.cz	ELC Electroconsult SpA	Jack Levine
jefar.be	Lanmark Group	www.mylawcompany.com
gumustasmaden.com.tr	Milhench Supply Company	Iso.com
geselektrik.com.tr	Peaker Services	Precision Compounding
gccservices.eu	Shlansky Law Group	CT Dent Ltd
fresh2you.eu	Bowman Trailer Leasing	platinumone.in
fortrex.hu	Centurion Security & Investigations	Trucash
emresorts.com	Keycodes Inspection Agency	Renasas Electronics
d-klima.cz	A Uzzo	SODISE
csd-drancy.com	TACK Electronics	Towerstream
cmc.com.br	Mercury Wire Products	Khazzan Logistics
casabotas.es	Cinema Concepts	Kasapreko
carseo.de	AIRCOND S. R. L.	Diesel Electric

bwk-berlin.de	aspviewacademy.org	Canvas Church
bonfilet.com.tr	feldmanandlopez.com	UniqueTech Engineering
behranlift.com	hoodriverdentist.com	Camomilla
arabfalcons.com	Leger & Shaw	Trumbull County
anwalt-austria.at	Edward J Kone	bennett.edu
amw-treuhand.ch	seeberger-appel.de	Duhabex
agfri.com	stadtwerke-clausthal.de	mmc.de
acarlar.com.tr	autohaus-paschke.de	juliuskoch.com
rdmetals.nl	ernst-auto.de	untereisesheim.de
ambisig.com	Trine Access Technology	steuerberater-scheerer.de
shwapno.com	Power Curbers	mactavishco.ca
semplastik.com.tr	Florida Orthopaedic Associates	barnet.com.au
proplastics.co.zw	www.ktlgroup.com	Beecher Walker Architects
platinumpws.com	OGI Groupe	King City Lumber
npia.v.com	www.advancedentdenver.com	wachtmann.eu
manuaco.pt	Allure Home Creation	becksgroup.au
itgsolutions.com	Fairgrove Oil	hyperdomemedicalcentre.com.au
grupoconstrutodo.com	Maypay Farms Inc	Shumate Mechanical
Progressive Laboratories	Southern Specialty & Supply	Sieger design
Ruhrpumpen	ILLUMINA	AvtechTyee
CSA Tax & Advisory	Walters Group Inc	Foster & Eldridge
Hintenberger GmbH	McKee-Pownall Equine Services	Advanced Power
VEPLASTIC	LiftPRO	Rosland Capital
THT Bio-Science, France	GPC Industries	3S Software (Secured Smart Systems Overview Metrics)
Bangchak Corporation	Productos Lácteos Flor de Aragua CA	Consolidated Sterilizer Systems
Madera County Superintendent of Schools	Precise Benefits Group LLC	Fargo Park District
kavi.fi	Markham Stouffville Hospital	insightchicago.com
Chrysler	Beyer Law Group	jobberswarehouse.com
CYMA SYSTEMS	YOKOSUKA GAKUIN	rjwalker.com
Lynn Electrical	Grupo Logistics	terracaribbean.com
SEIMITSU THAI COMPANY LIMITED	Merko Ehitus	brumfieldconstructioninc.com
Hermes Medical Solutions	Dacon Networks	intellioan.com
grade results	Fujitsu Systems Global Solutions Sdn Bhd	berjaya-air.com
The Salvation Army	Region of Istria	montaury.com.br
polhun.pl	Denk & Roche Builders	Slimsoft
maxdream.tur.ar	International Standard Valve	National Health Insurance Management Authority
47club.jp	strtn.org	Smith Fire Systems
nhpsa.com.ar	demilac, Inc	Kana Pipeline Inc
vitatrac.com.gt	dgpcommercialisti.it (Italy, Reggio	ABC Home & Commercial Services

	Emilia)	
eiconnect.com	uro.com (USA, Virginia)	Medisend
massfd.org	Print-0-Tape	The Minor Firm
National Credit Regulator (NCR)	Thrings Solicitors and Lawyers	Scientology
cmac-llc.com	Gordon Clifford Properties Inc.	McManes Law
envases-group.com	Angstrom Automotive Group	Institutional & Supermarket Equipment
Agralite Electric Cooperative	DXS SYSTEMS	Peter Meijer Architect
Trubee Wealth Advisors	Diaz Gill Medicina Laboratorial S.A.	Maset
Watertech of America, WorldPoint ECC, Mastermedia, Garrett Leather, Guttenberg Industries.	Hodgins Law Group	Espaço Casa
Rafael Construction	Hopper Developments	sspinnovations.com
Building Trades	STIC	Pioneer Ocean Freight Co., Ltd.
J Grennan & Sons	cityofsignalhill.org	Yellow Cab of Columbus
WSI	steelworksinc.ca	Quasar Inc
ARO	Kier & Wright	Atenção Primária à Saúde Brazil
Happy Telecom	teccart.qc.ca	IES Synergy
Felix Gonzalez Law Firm	sbws.org.sg	CCJM
LogicVein	fest-group.de	Clayco Electric
SV-Büro Ing. Schulz GmbH	lampus.com	Gandía Palace Hotel
Sipl	intrust.gr	Valley Eye Associates
Steel Dynamics	aysa.com.ar	COTTAGE
Tri-State Metal Roofing Supply	VFM Systems & Services (P) Ltd	Providence Academy
Ellison Educational Equipment, Inc	Wavenet	Golden Artist Colors
amsino.com	Smith Roberts Baldischwiler, LLC OKC Engineering Firm	CST Coal
Usina Sao Jose Do Pinheiro	The Youngfor	Quality Engineered Homes
Ever Green Industria e Comercio Ltda	Vlp Hellas	Pan-0-Gold Baking Company
All Rush	dabafinance.com	cpasch.com
Santa Casa de Assis	CANCER	Davis Kitchens, United States
Solus Tecnologia em Sistemas LTDA	Vishnick McGovern Milizio	Custom Engineered Wheels
HSR Specialist Researchers	Jabezco Industrial Group	Building Controls and Services
International Door, Inc	Choates HVAC	Eggelhof
Prime Label	Viga Eatery	SUNNYGO.COM.TW
Autohaus Elstermann	Eastman Cooke	LA Injury Attorneys
Carbis Loadtec	Cinvestav	Brodosplit
pellcityschools.net	Temple Shalom	City of Urbana
Niradia Enterprises	Chema Ballester	NUMALLIANCE
daipa.it	Watermark Beach Resort	Rouse Frets White Goss Gentile Rhodes
SW/WC Service Cooperative	beycelik	Wynn & Wynn
CoreHQ	Keylogistics Chile SA	Fuji Vegetable Oil
Shore Gardens Rehabilitation & Nursing Center	Inter-American Tropical Tuna Commission (IATTC)	Bo Beuckman Ford

The Sonnenschein Groupe	Sponseller Group, Inc.	Armis Group
Jaf Gifts	Cranford, Buckley, Schultze, Tomchin, Allen & Buie, P.A.	Wisconsin Knife Works, The Smith Companies, Envirotech Services, Next Generation Logistics...
Eastern Townships School Board	David M. Schwarz Architects	bisonfamilymedical.com
Notin	ACE Forwarding	Basra Transports
Accela	Startek Engineering Inc.	instyle.com.au
Agr í cola Cerro Prieto	StanleyCo Malaysia	lesker.com
Chatham Asset Management	Unknown	Pathmaker Group
https://www.ckm-montagen.de/en/	United Keetoowah Band of Cherokee Indians in Oklahoma	EDIS
ruskcountywi.us	RJS Logistics	Mr Christmas
https://www.omnibusjp.com	HKR Architects	Moyes
ccedarvalleyservices.org	Warrior Crane Service	Sarmap
www.fecrwy.com	Twinsoft	Petra
loginport	Solarpro Holding	GV Service
Laidley Family Doctors	Maven Solutions	Reading Elevator Service
Sense Eletronica	Arcom Digital	noment
Unified Assessment Platform ExamRoom. AI	ATG	VENZI & PAGANINI AG
Universiti Sains Islam Malaysia	GDEV	GreenBest
Woodglen Medical Group	Anderson Engineering	Saca Industrie SpA
Center for Life Resources ECI	Quezon Power	Oriental Castle Sdn Bhd
Geometrics	Hopital La Rabta	Garrett Taylor, Dds
Total Air Solutions	Personal Injury	Jewell Engineering
Cl í nica D á vila	Jeff D'Ambrosio	Toledo Transducers
Hanlon Electric	Spitzer Auto Group	Prismier
Grupo Amanus	Oxford Rehabilitation Center	Immling Festival DER Festspielort im Chiemgau
Acme Electric	The Parkes Companies	dakkota.com
Scenic Solutions	Greene Metal Products	ASUS
Besco Electrical	Right Power Technology Sdn Bhd	Exegy
National Biscuit Industries	SCIPIONI	Ziglin Signs
Callipo Group	Iroquois Memorial Hospital	www.precipiidx.com
Lasercomb	Northern Air Systems(2)	Thlusty & Kennedy
Swartz Campbell	Dan Technologies Group	ravand.com
cc-estuaire	ABECO Zumtech Drucklufttechnik AG M ü liweg	Mobilelink USA
Lugiano Medical	WJ Professional	Capital Star Oil & Gas Inc.
F ü rth	Nepes	American Pools & Spas
Polaris Parks	Woodard, Emhardt, Henry, Reeves & Wagner, LLP	Cleveland County Sheriff's Office
Ranger Investigation Guard	Leadway Assurance	Cl í nica Villa Zaita

Office of Public Sector Anti-Corruption Commission	A. S. A. P. Restoration	oxfordshop. com. au
Guan Chong Berhad	Bell Lifestyle Products	University Loft
Sanyang Motor	Ada Technologies	PHA Body Systems
Adnan Sundra & Low	Harbour Town Doctors	South Island Public Service District
Assolim	Plonter	San Miguel
GIV SRL	Red Star Studio Ltd	France terre d'asile
GOOD+ Foundation	NSE Insurance Agencies	B dynamic
Hongfa America	Erie Molded Plastics	HASCO Hasenclever
Eanes ISD schools	GROUPE ETMB	Virtualware Solutions
La Papelera	Sunshine Group	Wisconsin Knife Works, The Smith Companies, Envirotech Services, Next GenerationLogistics,
transrocamar. com	Lonich Patton Ehrlich Policastri	Industrial Steam
British Holiday & Home Parks Association Ltd	Kirby Agri	Clark & Sullivan Constructors
Friis & Moltke	LINEMASTER Switch	Hall Aluminum Products
uniplaclages. edu. br	CIDEF Argentina S. A.	Aspen Distribution
Grupo Ol é	Sem Val de Bourgogne	millierwoodtradepub. com
taminsho. com	Urban Remedy	Wisconsin Knife Works, The Smith Companies, Envirotech Services, Next GenerationLogistics,...
Cedar Valley Services	Don Ricardo	Cleveland Construction
Empire Screen Printing	Vestil Manufacturing	Martin
V á hostav	Cdf	Astrofein
Talarico	häussermann stauden gehölze gmbh	www. enea. com
Evercover	dillonyarn. com	Abhe & Svoboda
svlawus. com	Novabio (france laboratories)	Goldenrod
terport. com. py	Cisneros	Innomotive SolutionsGroup
Security ONE Alarm Systems	rainbowtel. net	MD Manouel InsuranceAgency
Kucera International	Teruya Brothers Ltd	TUAN LE Construction Company Limited
Busbusbus	CPS	bpost
Titan Motor Group	James Free Jewelers	Rose Displays
Dolan Construction	Clean Air	Petro Environmental.
Egp Comunicaciones Sac	Tupi	Data Enterprises of the Northwest.
Victoria Benelux	Hexacon Construction	PJSI Consultants SDN BHD.
Unipres Alabama Inc.	West Quay	Curtis Investment Group, Inc.
IAPMO	TopDest	Abdulhadi Hospital
Integrated Technology Group	Leandri & Associes	newhorizonsmedical. org
Homestead Electrical Contracting	Dill Dill Carr Stonbraker & Hutchings.	www. eastersealsnei. org
Insight	Sunair Electronics and Circuitronix.	Soderstrom Architects, LTD
Rio supermarket	Abacus Employment Services.	Hollysys Asia Pacific
Deibel Laboratories	Village Sant é Saint Joseph Hospital	Fun For Less Tours

RM Medics	Inter care	EXPERTISE MOBSIGN
Turnamics		

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，具有黑客入侵防护功能。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。

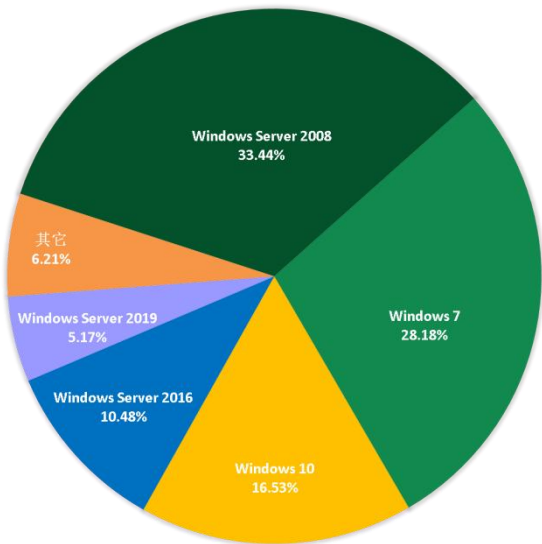


图 7. 2025 年 12 月受攻击系统占比

对 2025 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。

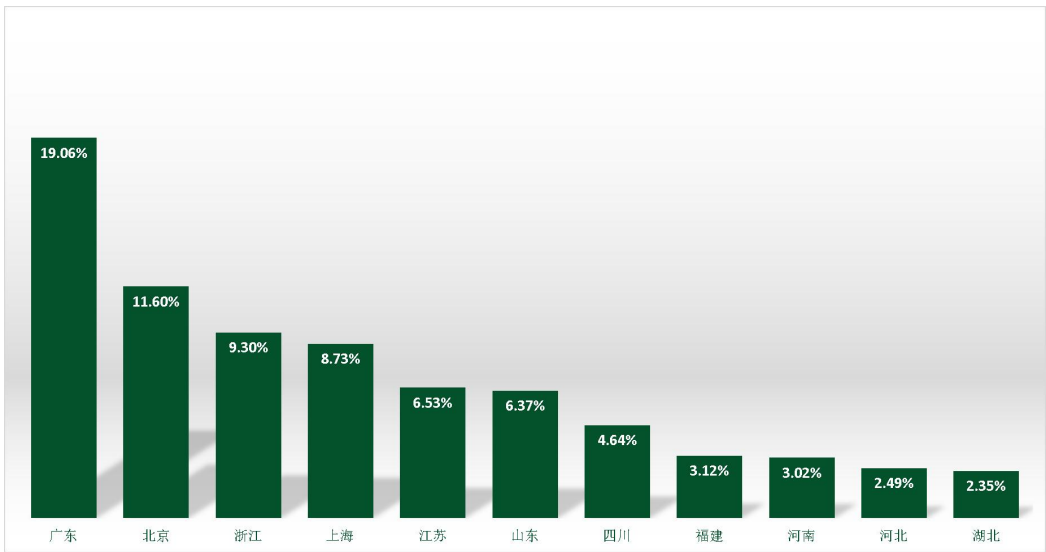


图 8. 2025 年 12 月国内受攻击地区占比排名

通过观察 2025 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。

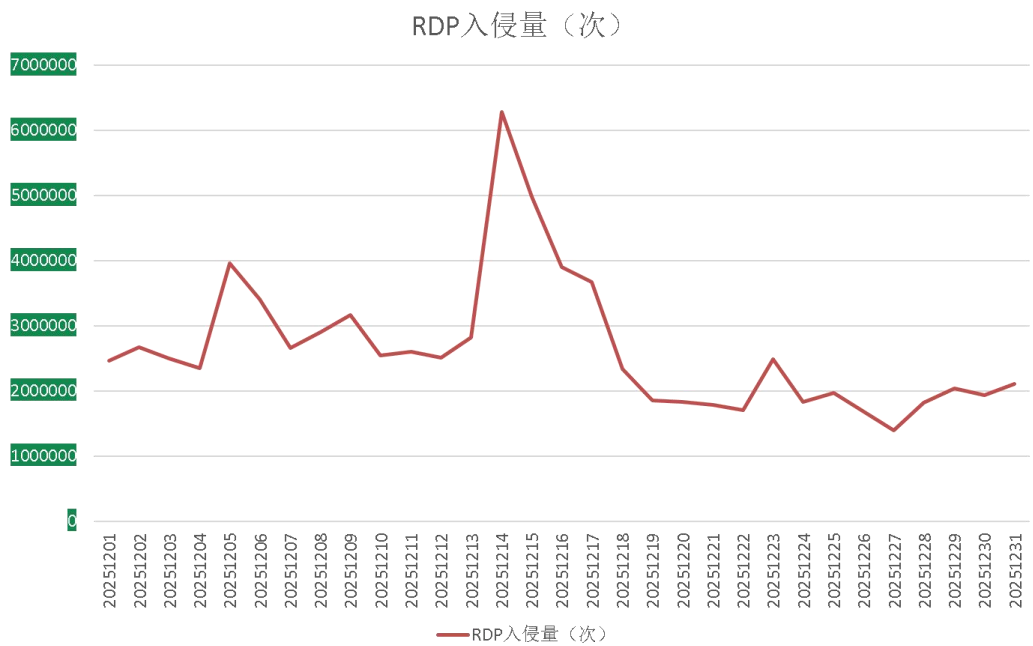


图 9. 2025 年 12 月监控到的 RDP 入侵量

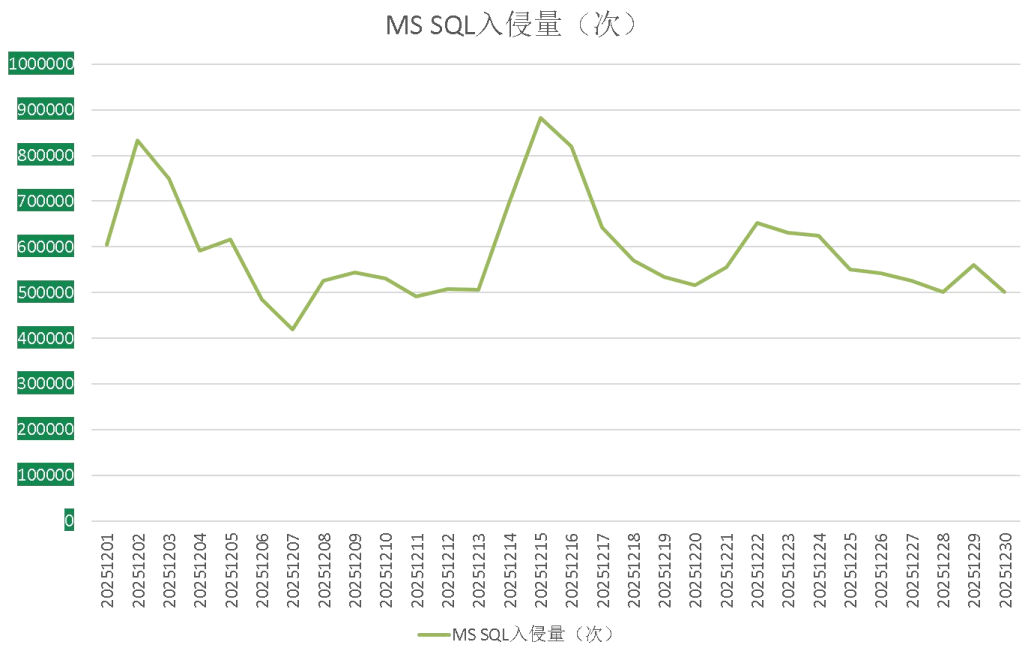


图 10. 2025 年 12 月监控到的 MS SQL 入侵量

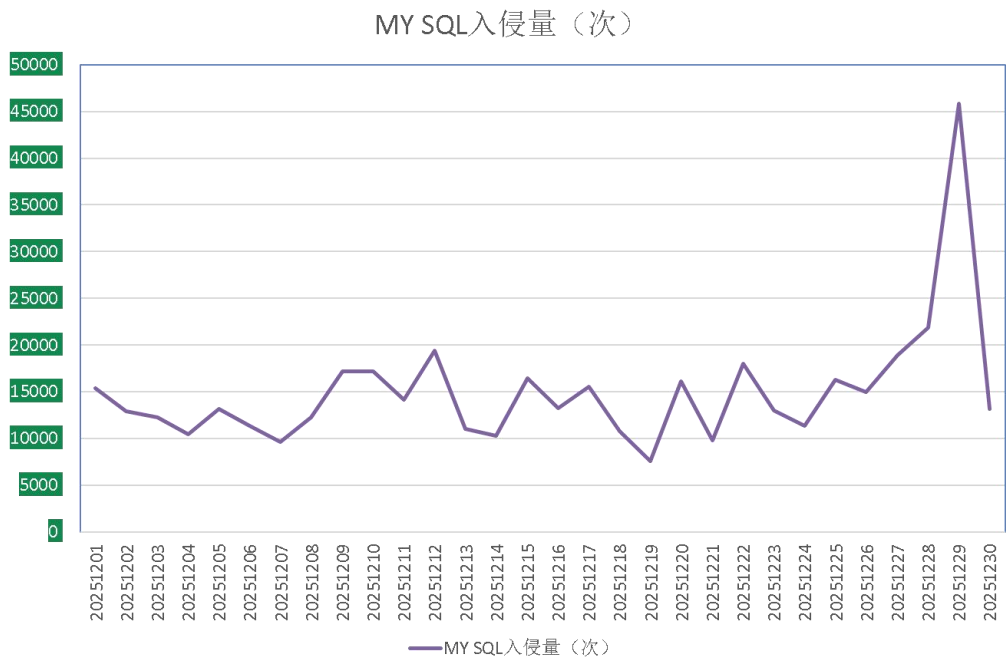


图 11. 2025 年 12 月监控到的 MYSQL 入侵量

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。

- ✧ weax: 属于 Weaxor 勒索软件家族，该家族目前的主要传播方式为：利用各类软件漏洞利用方式进行投毒，通过 powershell 加载攻击载荷并注入系统进程多轮加载不同的漏洞驱动，与安全软件进行内核对抗。部分版本会通过暴力破解登录数据库后，植入 Anydesk 远控进行手动投毒。
- ✧ wman: 属于 Wmansvcs 家族，高度模仿 phobos 家族并使用 Rust 语言编译，目前仅在国内传播。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。
- ✧ wstop: 属于 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。
- ✧ rx: 同 weax。
- ✧ 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，后来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曾通过匿影僵尸网络进行传播。
- ✧ taps: 属于 Paradise 勒索软件家族，该家族目前的主要传播方式为：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。
- ✧ revrac: 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 revrac。
- ✧ datahelper@cyberfear.com: 同 weax。
- ✧ baxia: 属于 BeijingCrypt 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。

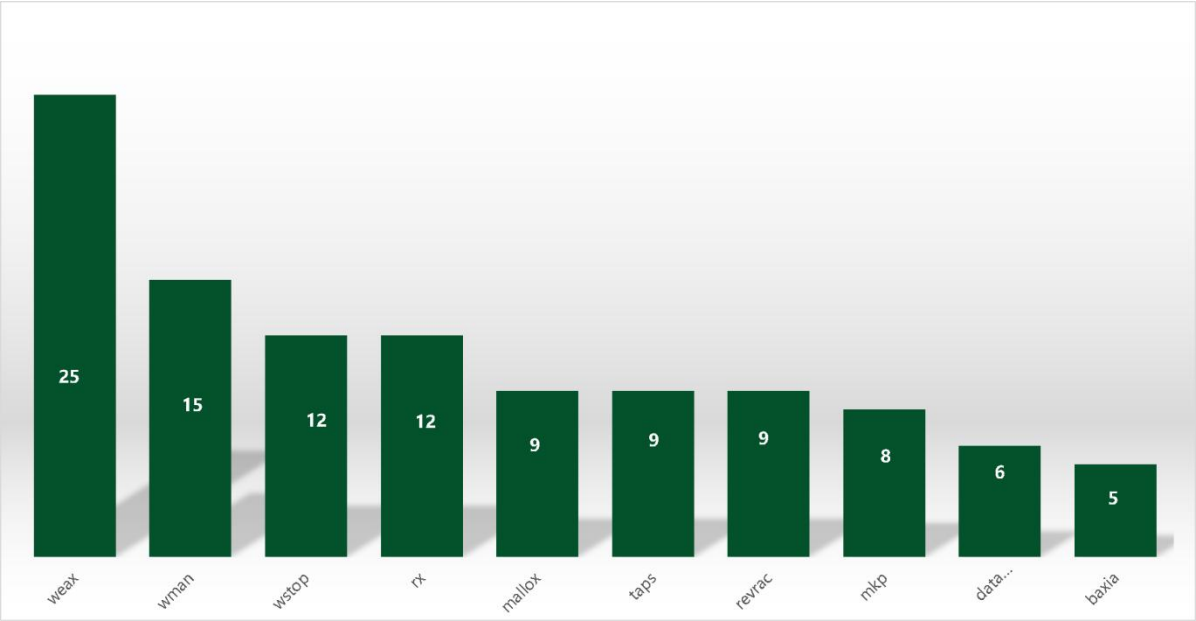


图 12. 2025 年 12 月反病毒搜索引擎关键词搜索排名

解密大师

从解密大师本月解密数据看，解密量最大的是 Phobos 其次是 FreeFix。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。

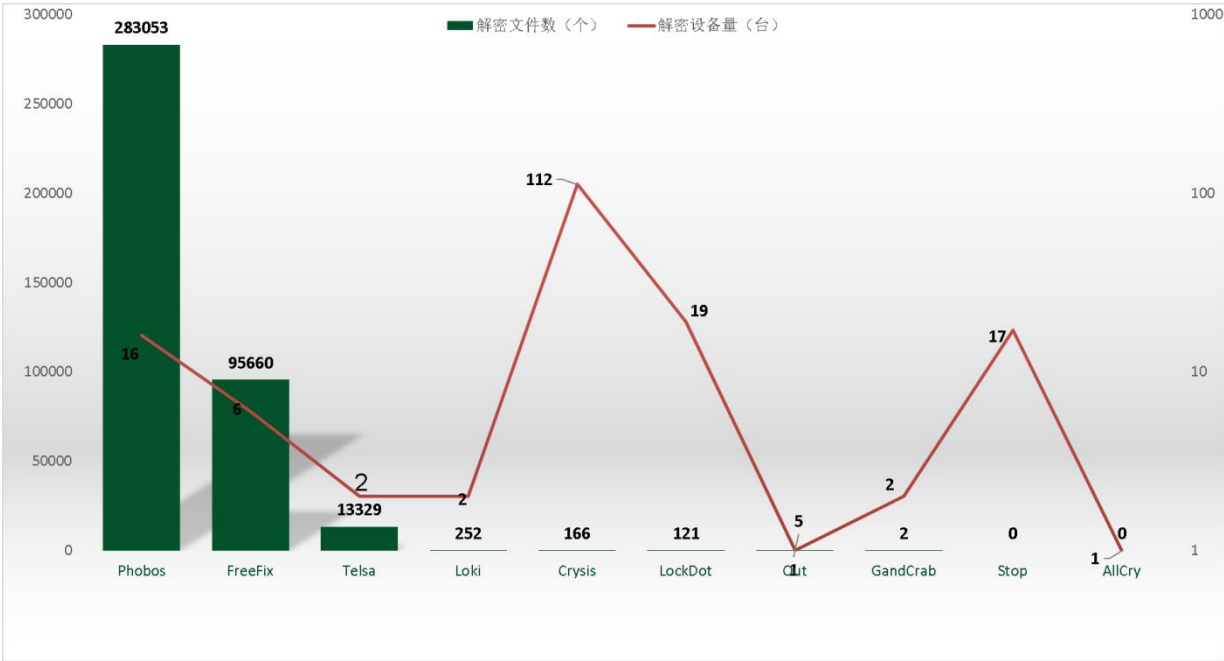


图 13. 2025 年 12 月解密大师解密文件数及设备数排名