2026 年 9 月

勒索软件

流行态势报告



三六零数字安全科技集团 | 安全能力中心反病毒部

勒索软件传播至今，360 反勒索服务已累计接收到数万例勒索软件感染求助。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，勒索金额从数百万到近亿美元的案件不断出现。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监测与防御，为需要帮助的用户提供 360 反勒索服务。

2026 年 9 月，全球新增的双重勒索软件有 BlackLocks、Vexy、NOn、EndZone、RedPipe 等家族，传统勒索软件家族新增 ARK、EniFrost、Calipso 等家族。

本月 Weaxor 家族大量利用 ERP 类软件漏洞，碾压式霸榜勒索攻击第一位。其中某帮的 ERP 类软件漏洞利用在本月最为集中，相关漏洞在开启 360 相关防护的设备上，会自动阻止利用这一漏洞加载恶意代码执行。

本月 Sorry 勒索软件进行了一次变种，修改加密后缀为“.ths”，勒索信文件名为“hello.txt”。本轮攻击依旧沿用之前的某万维漏洞发起攻击。

以下是本月值得关注的部分热点：

① Sorry 勒索软件 ths 变种来袭

② 柏林市政府拒付赎金后，Rhysida 公开近 6TB 行政数据

③ The Gentlemen 攻击医疗巨头 Veradigm，窃取 350 万条患者记录

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。

安全软件占比分析

360 反勒索服务已经存在十年以上，并长期致力于服务来自全网的勒索病毒攻击的响应、分析、处置、攻防、预警、解密工作。自 2026 年 1 月起，新增安全软件占比统计，主要用于评估当前复杂网络攻防态势下愈发严重的基线安全问题，为勒索相关的攻击事件提供接近真实维度的数据。

本月的勒索反馈中未安装安全软件的占比达到 61.09%，而未正常启用 360 安全软件的设备数量则占比 19.19%，安装了其他安全软件的设备则占比 19.72%。

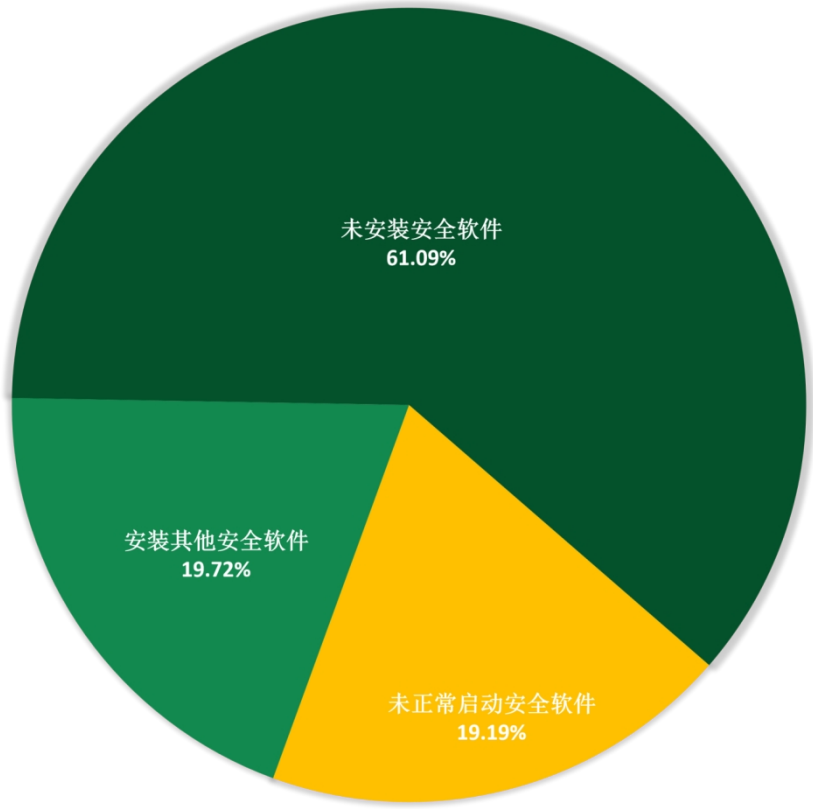


图 1. 2026 年 9 月勒索软件中招设备中安装的安全软件占比

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：Weaxor 家族占比 70.14%居首位，第二的是 BrzCrypt、占比 8.06%；Sorry 家族以 7.58%占比位居第三。

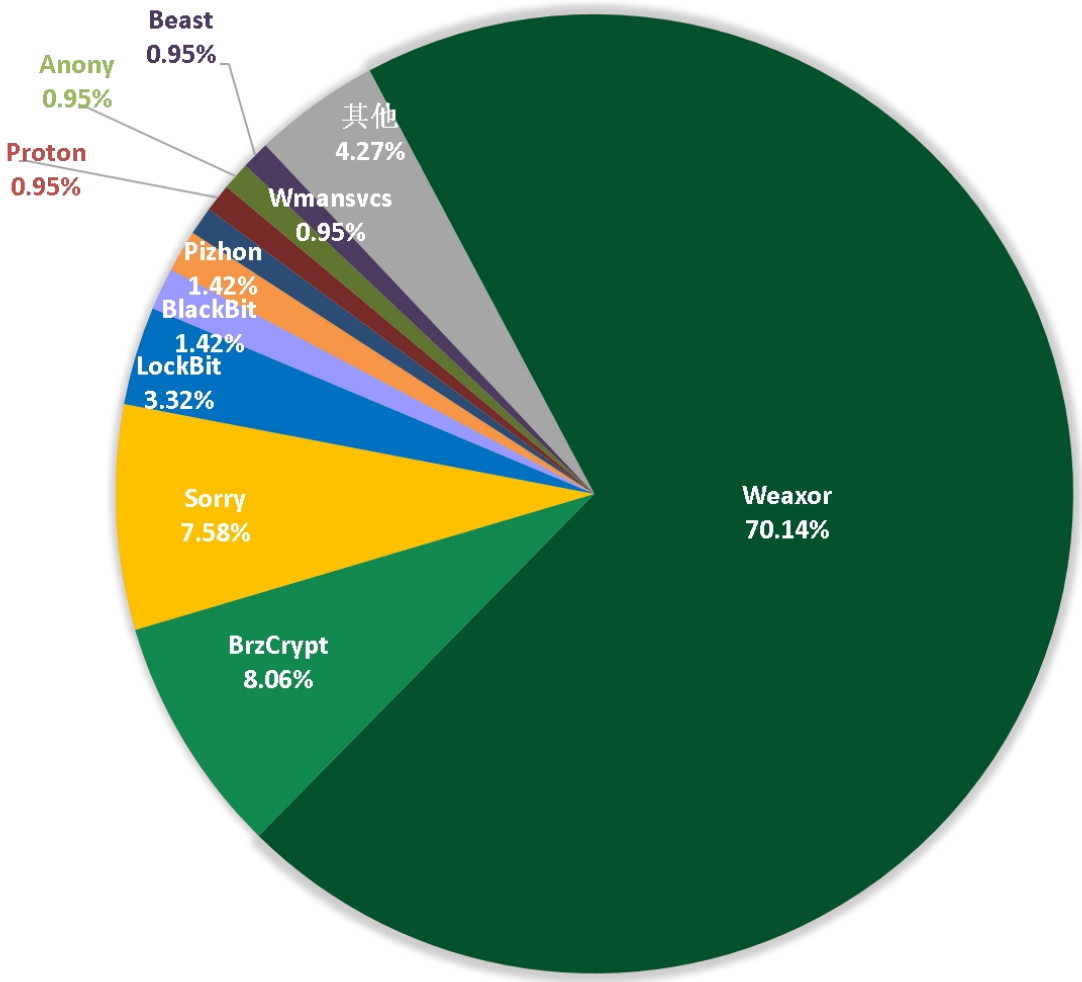


图 2. 2026 年 9 月勒索软件家族占比

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 2016 以及 Windows 11。

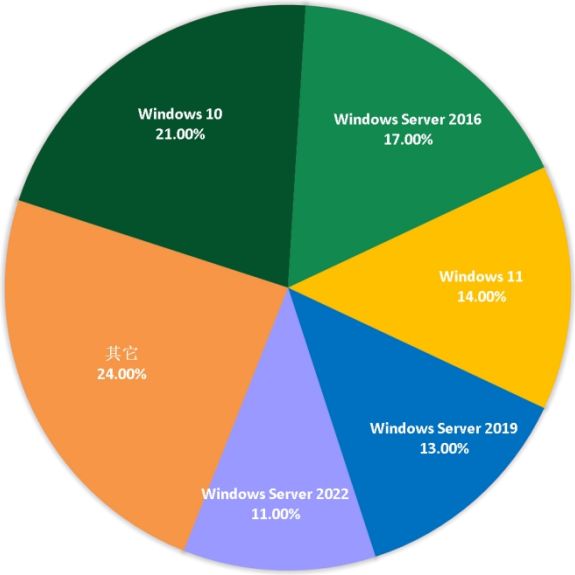


图 3. 2026 年 9 月勒索软件入侵操作系统占比

2026 年 9 月被感染的系统占比显示，受攻击的系统类型中，服务器大幅领先桌面 PC。

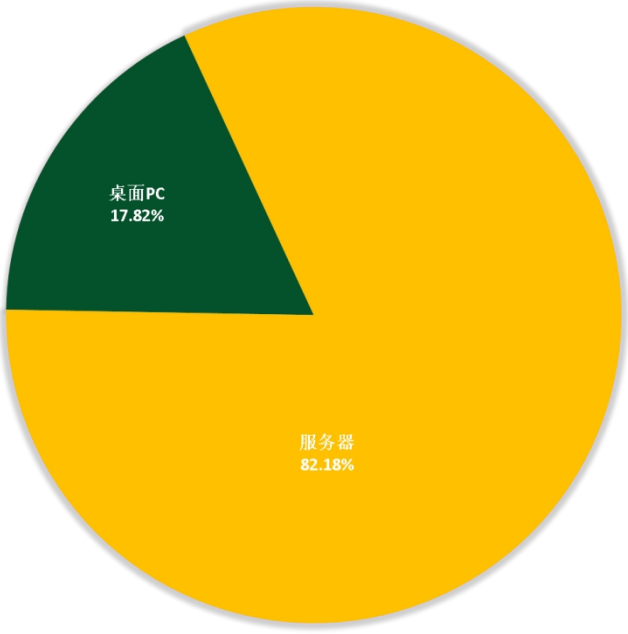


图 4. 2026 年 9 月勒索软件入侵操作系统类型占比

勒索软件热点事件

Sorry 勒索软件 ths 变种来袭

本月 360 反勒索团队连续接到多起 Sorry 勒索家族相关反馈，第一波受害用户数据被加密的时间集中在 9 月 20 日夜间到 21 日，感染规模达数千例，且攻击仍在持续，本轮攻击的加密数据类型覆盖数据库、备份文件、办公文档和源码仓库等。结合对样本的编译时间戳信息、近期集中反馈与告警的事件判断，该家族变种正处于快速活跃期，而非偶发单点事件。

360 反勒索团队结合大量事前未安装 360 防护的用户反馈及云端攻防数据，完成溯源分析，最终确认本轮 Sorry 家族投毒的攻击链源自某企业远控软件的漏洞利用。而本次变种样本的扩展名从此前的.sorry 变为了.ths，勒索信文件名也变为了“hello.txt”。此外，其加密算法实现也从 RSA+AES-GCM，整体调整为 X25519+XChaCha20-Poly1305，其他部分则与之前版本保持一致。

详细分析报告可参见如下链接：

https://www.360.cn/n/13052.html

随着当前 AI 技术的普及与勒索攻击的深度结合，勒索攻击在全球范围内均呈现出高危高发态势。为此，本月 360 在“远控勒索急救”工具中新增了“勒索反馈”入口，首次明确无差别支持全设备平台勒

索事件的反馈与响应。



图 5. 2026 年 9 月 360 勒索急救加入无差别勒索反馈入口

柏林市政府拒付赎金后，Rhysida 公开近 6TB 行政数据

2026 年 9 月 5 日，Rhysida 勒索团伙在暗网公开了近 6TB 从德国柏林市政府窃取的数据，将此前针对柏林政府的泄露威胁付诸行动，标志着这起持续数周的政府网络勒索事件进入最后阶段。事件可回溯至 8 月 14 日，柏林市政府中央网络检测到入侵活动后，所有参议院部门被立即从核心网络断开，城市发展与住房建设、交通运输及环境气候保护等部门的公共服务受到严重影响。攻击者随后声称窃取了 5.79TB 数据，包含约 1.44 万个文件、16389 封邮件、11963 个电话号

码、148 个银行代码，以及数万份合同、司法文档和人事档案，还窃取了以明文形式存储的登录凭据和柏林供水系统的漏洞分析等机密材料。该团伙索要 30 枚比特币（约合 230 万美元），并以拍卖方式声称将出售给单一买家，并设置了公开数据的倒计时。柏林市政府公开表态拒绝任何谈判，这一决定最终触发了数据被整体公开。

此次泄露是双重勒索模式的典型结局：攻击者先窃取数据，再以公开泄露为筹码施压，当受害者拒绝支付时便泄露数据。近 6TB 的政府文件体量表明，其中不仅包括行政公文和内部通讯，还可能包含大量雇员与市民的个人数据。这些材料一经在暗网公开，任何犯罪团伙都可自由获取，可能被用于身份盗用、钓鱼攻击或针对文件所涉人员的定向攻击。对于柏林市民和政府雇员而言，最稳妥的做法是将受影响部门掌握的个人信息视作已经暴露，警惕任何引用政府档案细节的钓鱼邮件和电话，并为关联政府服务的账户更换密码、启用多因素认证。此次事件同时也有警示作用，拒绝支付赎金虽符合执法机构的一贯建议，但机构必须同步做好数据已泄露的最坏打算，将事后身份保护与系统排查纳入应急预案。

The Gentlemen 攻击医疗巨头 Veradigm，窃取 350 万条患者记录

2026 年 9 月 9 日，美国医疗科技巨头 Veradigm 披露了一起数据泄露事件。Veradigm 前身为 Allscripts，总部位于芝加哥，为全美数

以千计的医院、诊所和生物制药企业提供电子健康档案、电子处方、患者随访、诊疗管理和收入周期管理等软件服务。根据该公司向美国证券交易委员会提交的文件，攻击者窃取了某第三方供应商环境中用于客户服务的 Veradigm API 访问凭据，并利用该权限复制患者数据，被窃信息包括部分患者的个人信息和社会安全号码（SSN），临床与医疗记录本身未受影响。该公司称事件未造成运营中断，但影响了部分客户。目前 Veradigm 已启动应急响应、上报执法部门并开展调查，正在通知受影响客户与个人并提供信用监测服务。9 月 5 日，The Gentlemen 勒索团伙在其泄密网站上宣称对此次入侵负责，表示共掌握 350 万条患者记录，包括姓名、住址、SSN、邮箱、电话及担保人身份信息，并威胁如不展开赎金谈判，将于 9 月 11 日（周五）公开全部数据。

The Gentlemen 团伙于 2025 年年中前后浮出水面，采用数据窃取与加密相结合的双重勒索模式，攻击范围覆盖 Windows、Linux、NAS、BSD 和 ESXi 等平台，其泄密网站上挂出的受害者已超过 800 家，遍布 86 个国家的制造、科技、医疗、交通和金融等多个行业。2026 年 4 月，Check Point 曾披露一个超过 1500 台主机、与该团伙附属成员关联的 SystemBC 代理僵尸网络；同年 6 月，ESET 又发现该团伙使用名为 GentleKiller 的新型 EDRKill 工具来终止终端安全软件。此次事件中的第三方 API 凭据失陷再次警示：医疗机构与医疗数据服务商的供应链入口正成为勒索团伙的重点突破口，第三方接口的权限最小化、异常访问监测与凭据轮换治理亟须加强，医疗行业数据泄露的连锁风险持续走高。

黑客信息披露

本月收集到的黑客邮箱信息如下：

aldetron@outlook.com	usenarealnran@onionmail.org	Alex25key@aol.com
this.email.address@gmail.com	restore.uralbti@gmail.com	Alex25key@mailum.com
yasonIDs@outlook.com	vricpe@aol.com	backups2026@2mail.co
yason@mailum.com	vricpe@firemail.eu	BIG@cloudminerapp.com
Bluecrap9@gmail.com	vricpe@2mail.co	bentderstlinpart1987@protonmail.com
usenarealnran@outlook.com	Lollooki@protonmail.com	concbuzzmittcou1982@protonmail.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）。

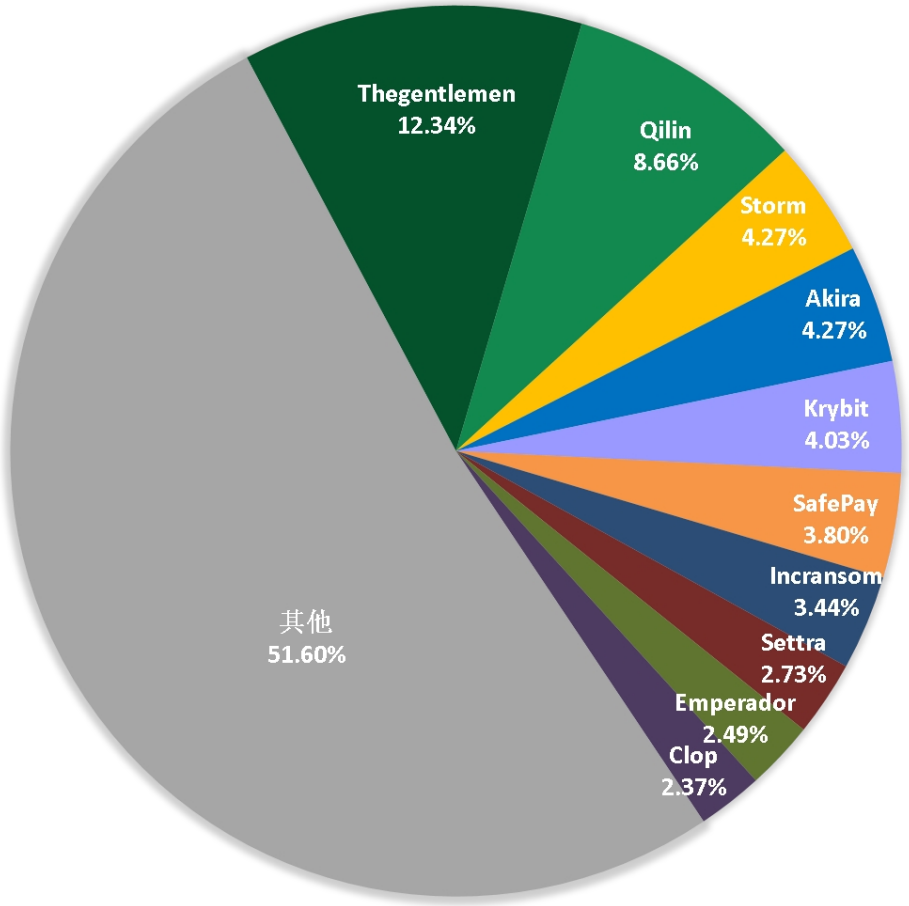


图 6. 2026 年 9 月通过数据泄露获利的勒索软件家族占比

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，做好数据已泄漏准备，采取补救措施。

本月总共有 843 个组织/企业遭遇双重勒索/多重勒索攻击，其中包含中国 12 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。

Houston Thyroid & Endocrine Specialists	quantummarketing-group.com	瑞祥机电 (Ruixiang Jidian)
Software Answers, a Banyan Software Company	moscone.com	Abourametals
The Japan Times	gregjoneslaw.com	Frisby Roofing (Frisby Construction LLC)
Summit Electric Supply	Krapf Group	Praveg Caves Jawai
wolfusofsky.de	The Fifty/50	TOWN OF SUTTON	MASSACHUSETTS
Le Centre National de l'Expertise Hospitalière (CNEH)	Coe Press Equipment	compunnel.com
Titus	TDMI	Imperial Healthcare Solutions
Airtech Mechanical Services	Tulare Western High School	DiamondLease
Orth Automobile	GOTTHELF	Perimetral Oriental de Bogotá S.A.S.
Blaise C. Bender, PC	DI.C.S.EL. S.R.L.	Ozel & Ozel Laws Office
Buford-Thompson Company, LTD	vit.ac.in	Tuboaços da Amazônia Ltda.
dfiretailgroup.com	Columbus Informatica	Port of Tanjung Pelepas
econ-tec.com	Textile City	Foss Inc.
assist2enjoy.be	NAI Earle Furman	Dustin Group
Dr Damiel Pugliese	Sealcon	Konica Minolta Bulgaria
Astidental di Sabbione	FinSoft (Kolibri retail back-office software)	Medical Department Store
Vinco Energy	TruAmerica Multifamily	Agencia Estatal de Meteorología
Becker Logistik	theLender	CO-OP URBAN BANK LTD
Wilhelm Kühne	Metallco	i2k2 Networks
FIDUCIAL	Hurley	M800 and CINNOX
Virtual Ideas	Astemo, Ltd.	Sys-kool
PROJAHN	Hogan Lovells Cadwalader	Grunthal Welding & Supplies
Altmannshofer Sicherheits-Videotechnik	kyyba.com	General Santos Doctors Hospital
MCAP — MortgageHub commercial lending platform	360 Consulenza S.r.l.	Professional Retail Services
GERLON	Summa Gold	California School Employees Association

clicks digital GmbH Information	Allied Supply Co.	alphaomega-eng.com
Law Offices of R. David Williams, P.A.	Kjla	mankatoclinic.com
www.newyjh.com	Telrad Networks	artiflexmfg.com
West County Health Centers	Wiedenbach Brown	NcbChurch
Gardeners' Guild	U.S. Electrical Services and Wiedenbach Brown	On Demand Occupational Medicine
LegalWise	Hudson MD Group, LLC	Goldston Oil Corporation
Samwumed	Bruker Corporation	jms building corporation
Edcon	Flex Ltd	AK Stamping
Defencebit	HyVision System. Inc	Eagle Construction
Datacomm Services	Visual Intelligence, Inc.	George Cameron Nash
Webb Electric Company of Florida	Prestige Management	EASY JOB S.A.S.
Solaria	Grupolider	John Engel Team
Auren	The Money Store	HENRYPRATT.COM
QUALITY SPORT Topsport Italia	TrueCore Behavioral Solutions	HARLEY-DAVIDSON.COM
Europrim	Manroc Developments	Mesan USA
Telrad Networks	Charlottesville Police Department	Air Canada
Groupe APROSEP	IKEGAMI TSUSHINKI COMPANY LIMITED	amorsaude.com.br
Drinks Wines Spirits	Gomomentum.com	Aqualogus
Custom Rx Shoppe	newmantractor.com	Mitsuwa Trading Co., Ltd
Williamson Dacar Associates	siinqeebank.com	cullottalaw.com
Agospap	SECOND HOUSE	gardensalive.com, bitsandpieces.com, iselinursery.local, weeksroses.org, esm.local
DBU Construction	Maryann Kriger	Logar Network Solutions
Northern NJ Eye Institute	arsrenacer.com	https://mediengruppethiel.de/
Tommy Garner Air Conditioning Heating	Alabama Woman's Health Care	RelyComply AML Platform
Auto Holler	TEK SPB	Kyodo USA
North Hills Facility Services	Siddhi Green Excellence Pvt. Ltd	Bosnia and Herzegovina Mine Action Center

VUS - The English Center	acilnet.com	Specchem LLC
Olnick Rentals	Euramex Management Group	Jet Specialty
Josee Bendaaa-Guerrero Asociados	Zorlu Holding	Universal Starch-Chem Allied Ltd
Don Hierro	ShopDunk	BAYMER
Century Management Services	KMLS	Technology Dynamics
Corswarem Group	Touring Club Suisse	Flexmaster
Silvercup Studios	Studio Notarile Associato Salvatore Costantino E Anna Favarato	Lowerys
Pulmonary Services Group	Great Bay Bio	Melitron
UC Components	TOWILL	Gellibrand Support Services
Stockham Construction	Fanatics (global sports commerce platform)	Red Star Oil
Vintners Distributors	HEOLIS	GT Distributors
Agra Industries	FRANCARETRAD	palmettoeyeinstitute.com
Poca Valley Bank	ambpvc	reichenau.at
intense.pl	Schneider’s Computing	cannonpuntana.com
Unique Repair Services	AKAZZO	assiprime.it
advantech.com	voltgames.io	gayafores.es
Tekko Enterprises, Inc	Electrolux	cenmar-manila.com
Gibson Area Hospital & Health Services	Kreishandwerkerschaft Borken	gsngestion.es
Polikem	Young Injury Law	hbpro.pt
AHeadStart Tutoring	tdgroup	recoverycafe.org
Crowder Industries, Inc	Quy Nhon University	mcnishsteel.com
latitudesubro.com	Cassias MG Government	Sales Boomerang
trailerbridge.com	Quest Group	Financi è re d'Uz è s
mccordclaims.com	K3G Solutions Brazil	fdcputman.nl
goriteway.com	Vista Plastic Solutions	contreras.com.ar
northeastrehab.com	Inglewood Golf	copeplastics.com
mulholland.com	Barrett Mahony Consulting Engineers	EMS1R
wildmanbg.com	PITTSRAD	Brent Electric

maxwell-group.com	Inter (Venezuela's largest internet provider)	Brentwood Country Club
bcx.co.za	Premier Lighting & Controls	CreateASoft
Groupe Proxitel	forus.cl	The Zhou Law Group
carolinaasthma.com	kit-e.jp	TTG Asia Media
spg.co.kr	PayPal support operations (Transcom WorldWide)	Alaska Electrical Apprenticeship
oterolaw.com	Ministry of Education — Argentina	Mefa Group
somasolucoes.com	Argentem Creek Partners (investment firm)	SAD'S Interim
noonsugar.com	AstraZeneca Türkiye	Partners Group SK
iccsi.com	STOKR (digital securities platform)	MEI Architects
cpacb.com	Konnatus (usucapião legal services)	Hollard Insurance Group
Precision Facades Ltd	BeLi Teacher / FSC education centers (AWS)	Drogueria Saporiti Sacifia
camorim.com.br	Vietnamese betting operator (GC789 network / Boundless TE)	Mutant
MinMor Industries	United Federation of Teachers	University of San Francisco
Arnold Center	MPA Pharma	Nile Projects Trading
New World Diagnostics	Anderson Industries	Chip7
bakemyday.se	www.roancampingholidays.com	Sharp Office
safescaffolding.net	www.kendallhunt.com	S A Chile
coosalud.com	Ascend Com	Yapı Merkezi
pistonespersan.com.ar	Ceres Tolvas	Soni Dwarkadas Virchand
midwestbit.com	Futuro Forestal	Zanini
apexus.com	Grupo Juste	Domis
bhn-expertise.com	Inland and Offshore Contractors	Metro
stjames.wa.edu.au	American Casting Company	Biotipo Jeans
Goodrich Logistics	Johnson Investment Counsel	Ritz Safety
Chem Process Systems Pvt. Ltd.	First Secure Community Bank	Comin Sac
Starr Whitehouse Landscape Architects	The State Bank	AbacoViaggi
Ever Ready First Aid	First Secure Bank and Trust	El Carriel

PKSF — Palli Karma-Sahayak Foundation	Accela.com	Superstore
Amazon Informatica	AT&T	vsbattorneys.co.za
Geebee Garments	ANYTHINGIT	State of Florida DMV
Netech (Neeser Technik AG)	Giti Corp	NorthShore Health Centers
Juntadeandalucia	Universitt Hamburg	Wellness Partners network(combined revenue)
Premiumfruits	Inovapy	United Group
The Center for Kidney Care	Stim	Master Manufacturing Co., Inc.
Knit	Vigatec	Alurwalls
SKLG	www.harputyapi.com	Precision Vehicle Logistics
ATCO Ltd	www.diakonie-apolda.de	Rug & Home
Nissho Electric Manufacturing Co., Ltd.	Invincible GG	TrainMe
Kellys Home Center	The Gran Hotel Ingles	NFM Lending
manno.ch	Techwise	GGS
auromex.com	expresspros.com	KÖRBER
cromados.com	hoyletanner.com	GENESILICO
lfgholding.com	aecom.com	Lightcast
fedelmundo.com.ph	rottner-tresor.at	Jinny Beauty Supply
bio-strath.com	naturesplus.com	Benshaw, Inc.
sumperk.cz	pacificabs.com	Semper Laser
eagroep.com	fchhotels.com	EllisDon Corporation
Holiday Inn Vilnius	budgetms.com	Jbc
Dediserve Ltd	sym.com.mx	SIFCO Industries INC.
SiteProRentals	xpera.ca	ST Engineering
SMCare	Pertamina	Hologic, Inc.
AHEAD	Silicon Integrated Systems	LIBRERIA SANTA FE A P S SRL
nsbsd.org	Practice Management (maximizedrevenue.com)	MSM Unify: Global Education Platform - CA
Asesor í a FAR	Vetta	Ben Leeds Properties WARNING
Ressources Si	Javep Chevrolet	Medela.com

XICO	Beckman Coulter, Inc	RTAD GOV MM
Island	AECOM	eAssist Dental Solutions
First Secure Bank Group	Promantra, Inc	Sancity
Revenga Smart Solutions	STP Fashion Lab	evergenbio.com
Willatt & Flickinger	hygear.com	KHALED ALFAGIH ENGINEERING CONSULTANCY
Pantaneiro Capas	Westbridge Institute of Technology, Inc.	myLaurel
Car Service Abschlepp	www.appliancefactory.com	Edacentrum
ARCA UNLIMITED Architects	www.diarco.com.ar	Mission Pet Health
cipher.systems	RDA MOTORS S.P.A.	Spirit Cultural Exchange - US
International Chemical Co.	SEVENOAKS s.r.o.	Leo Schachter Diamonds
Apollo 21 - Quality Truck, Bus & Trailer Spare Parts South Africa	Reddrop Group	Zdrowit
Applied Composites	In The Company of Huskies	Veradigm
Guardrisk	palletshop	Lider Aviacao
Metalware Corporation	Wise IT	Mega Velocity
Magna Legal Services	dg.ac.kr	CitizensPay
StMicroelectronics	gownet.net	Philippine Ports Authority
Hell Helmut GmbH	krimax.org	Bauman Law Group
Magnetos y Refacciones	Leisure Coast Kitchens	Jouvet SAS
ANP Health	Thorndale Foundation	G&S Technologies
Progeny	Thema Foundries	Nolan Consulting Group
Grupo MARSAN	Odyssey Charter School, Inc.	Colonial Hyundai
Agrocampo	Roshd Sanat	The Big Table
Markisol	Namibian Defence Force	Metrea LLC/Commuter Air Technology, Inc.
Trifecta Software	Blossomland Accounting	광명산업(주)
PuroClean	Bee Maid Honey	EdgeChem Jamaica Limited
Brancoptica	Manders	Kovo Healthtech Corp
Craisa	ARDA	D-MAX Engineering, Inc
Crystal Glass	Nielsen Design	Judicial Branch of the Province of Jujuy

Pajulahti	Aarsleff	kalahealth.eu
Ligue se Grupo	Community Property Management	huisartsencentrumkleiniterson.nl
Charles Keith	Owen Leigh Optometry	Wolfram Research
FTAPI Software	Hashimoto Jimuki	Stransky Heiz-Mess-Regeltechnik GmbH
Crossett	marlinhvac.com	Sports Endeavors
GE Vernova Inc.	neumerkel-gmbh.de	MBT Telecom
PKF Hadiwinata	triniticaring.org	Palsana Enviro (PEPL)
Platinum Healthcare Staffing	laconcepcion.com.mx	Annapurna Fashion
Electrolux & Ontrac	meterex.com	Sancity Soft Touch
Securitas Group	stoecklin-kuechen.ch	pscindustries.com
Morula IVF	ryomo.co.jp	AP CAPITAL PARTNERS LIMITED
Tobin & Company	ara-lyss.ch	SouthernCarlson
Ar Valve Resources	gob.pe	Worrell
GTFM	Springfield Public Schools	Homewood Sales
Beatus Cartons	Pilot Precision	Norwood Law Firm
Reliance Audit	Wiggins, Childs, Pantazis, Fisher, & Goldfarb LLC	Blanco & Etcheverry
UNIRITA	Taurus Ibérica	Occidental
CENELEC	City of Fort Smith Arkansas	EDIF S.p.A.
ETS	Cumar Marble & Granite	mansurovogroup
Breast Implant Center of Hawaii	Resolve Law Group	PIT.local
Majani Insurance Brokers	Lazyboyz	Hochschule Heilbronn Bildungscampus
Iberia Compositech Manufacturing	Montana Civil Contractors	Schwartz, Giannini, Lantsberger & Adamson (SGLA)
pharma5.ma	Southern California Telephone Company	Studio Oculistico Ciraci
TapClicks (marketing analytics platform)	Incrys	Katten Muchin Rosenman
Armada Credit Bureau	Bravo Group	myglobal.com
Westside GI	ADM	ialegre.com
Martin Lawrence Galleries	SFA Engineering Corporation	Maglin, Miskiv & Associates
Indroj Medical Group Inc.	Nippon Steel Corporation	ligacancerguate.org

efada.sa	Asada Sarapiqu	McDonald's Ecuador
NEAD SRL	McCarthy Tire Service	Complete Packaging Solutions
NEAD Pro	PANTHERx Rare	verveportraits.com.au
bnlawmacau.com www.bn-ip.com	Insight Credit Union	int.diasorin.com
corisricambi.it	ACA Pescara	hansler.com
welgenone.com	Hattiesburg Eye Clinic	hvlawfirm.com
ukbjja.org	Indic	teletekstructures.com
Prater & Ridley Attorneys At Law	Aurora Technologies	medevolve.com
GDM Pipelines	Goteborgsregionens Tekniska Gymnasium	neolife.com
Agora coopérative agricole	Alchin Long Group	buroboot.nl
Catholic University of El Salvador	Gelarti	Dinas Komunikasi dan Informatika
Dao Group	Balkan Polymers	America’s Food Basket
All Tech Machine & Engineering	Cedars Foods	Engefitas
Inversiones Bolívar	Agenzia Vittoria Assicurazioni	Petrocare Construction
Zig Inge Group	Downrite Engineering	Star Aviation, Inc
Wallatec	Neff Drexel	GSAC
Strack Companies	Iveta	Superior Ag
Revolut	Humboldt	Chicago Partners Wealth Advisors
airtanzania.co.tz / airtanzania.com	High Oakham Primary School	Macquarrie
www.jonesthegrocer.com	Tentac	SITES Medical
Grupo Caberj	Dome Gold Mines	Greenberg Traurig
winfashion	Dang Invest Group	Tanner
agiliance.fr	BGR Energy Systems	Cartrack Holdings
www.francare.com	Ardom Eilot	PTT Oil and Retail Business
amb-pvc.com	Technical Asia	Ormond Beach Florida
Arizona Vascular Medical Equipment, Inc	Multipla Contabilidade Empresarial	Uak University
BMGP Groupe	Somit	Asfaltos y Pavimentos S.A. (Asfalpasa)
Elite Industech Co., Ltd	Wada Farms	Westfield Public School District
HEC Group	Aforpa	Trucka

Solucioning S.A.	Apteki Mareshki	Policlinico Triestino
eTeam	Librería Santa Fe	Multiver Ltée
OnTrac	Sarku Japan	Metales Panamericanos
Abtach Ltd.	TMI Tecnicas Mecanicas Ilerdenses	Ville de Libercourt
anery.com.br	MedSkin Solutions Dr. Suwelack AG	PennFab
goldstarfinancial.com	Geieg	ScrubaDub Auto Wash Centers
Tomix / Grupo JOPER	Honda (Peru)	Algra Group
vestfrostsolutions.com	veritiv	part1.simplexengg.in
Legis	HandyTrac (Greystar Litchfield Park, AZ)	Royal Plaza On Scotts
ASYAD GROUP	Better Accounting Solutions	Seasia Infotech
Urban Engineering	Bernath & Rosenberg	Proliance Surgeons
Trump Mobile	Dorfman Abrams Music, P.C	specialtytextile.com
SUUNTO.CN(SUUNTO.COM)	Foremost Mfg	Licindia
HODERO-HOLDINGS-LTD	geekybunch.com	Chip 1 Exchange
KVHELI-WORDPRESS.COM	Winston Contracting, LLC	Grayson Rural Electric Cooperative
CCCM-BC.CA	Minmer Global	Marlborough Partners
BRINKS-CO.NZ	RoadEx America	Quality Resource Pvt
SAUL-ORG.UK	Dublin City Schools GA	Holland & Knight
CCED-COM.OM	Rosello et Fils	Szechenyi Programiroda Nonprofit Kf
INFINIGATE.CH(INFINIGATE.CO.UK)	Vitar Group	rubbermill.com
SWEETLAKE-LAND-AND-OIL-CO-INC	tpi.tw	Oportunidados
KIRKLAND-AND-ELLIS.LLP	comune.robeccosulnaviglio.mi.it	Honeycomb Programs Inc
PALIG.COM	httoy.fi	PT Intraco Penta Tbk
COLUMBIABANK.COM(UMPQUABANK.COM)	Metropolitan Community Health Services	Congressional Iron Works
UNISALLE-EDU.CO	Massey, Stotser & Nichols	Flex1
VALLEY-TRUCK-AND-TRACTOR	glasfloss.com	BYK Construction
KSS-ARCHITECTS-LLP	steelhausinc.com	Transportes Montejo S.A.S.
ELANDRETAIL.COM-KMALL24.COM	Mestechkin Law Group P.C.	SCHMIDT
TRANSPORT-NSW.GOV.AU	Atlas Ocean Voyages	CareerSource Palm Beach County

AMEY-CO.UK	Alicotrans	Nutex Health
Inkript	Cerá micas Kantu	The Sole
Lemon Law	Gilco Scaffolding	iwin
HIT dd	Navitrans	Manchester Airports Group
Apex Litigation Support	www.kashkha.com	REXT Holdings Co., Ltd.
AGROFRUTO SAC	CARIDRO VAL DE LOIRE	Total Education Solutions
COSEF - Consorzio di Sviluppo Economico del Friuli	i2i-systems	seashellhospital.com
The Merrimack County	Kimberly-Clark	uicc.org
Smart Eye Care	INCOR Group	tum.com.mx
Washington County	Strad Solutions	www.alphaplantes.com
RECEITA FEDERAL DO BRASIL	Nexbex Solutions Private Limited	reignwoodpark.com
Aokkef	Axdia International	orex.co.th
Seznam	watchops.com	amptc.net
Abv	www.tiflispalace.ge	dmt-group.com
taspenlife.com	www.tender.mx	jswlaw.bt
Clark Hill	capricornlogistics.com	vedantaainstitute.in
Fresenius Medical Care	www.ibnsinatrust.com	meccahighfeed.blogspot.com
Gaedke & Partner Steuerberatung	lasultanahotels.com	transportesmontejo.com
Grupo Hospifar S.R.L.	eracm.fr	southsign.in
Sherman Chan, DDS, Inc.	pss.ht	hccd-construction.com
Cozen O'Connor	www.metalware.ca	TERRACOM & MONTCAU
PSA - READ THIS NOW [No ransomware: blog post]	intherpro.com	Lawter
AFRICA-TECH (IT services / document processing)	meridian16.hr	Commission de la construction du Quebec
universalautogroup.com	www.eac-airports.com	Rise UP
namtheun2.com	swadeshicipl.com	VIVOTEK
lakebeverage.com	Sutton Public Schools	Italtel Peru

表 2. 受害组织/企业

系统安全防护数据分析

在本月被攻击的系统版本中，排行前三的依次为 Windows 10、Windows Server 2008 以及 Windows 7。

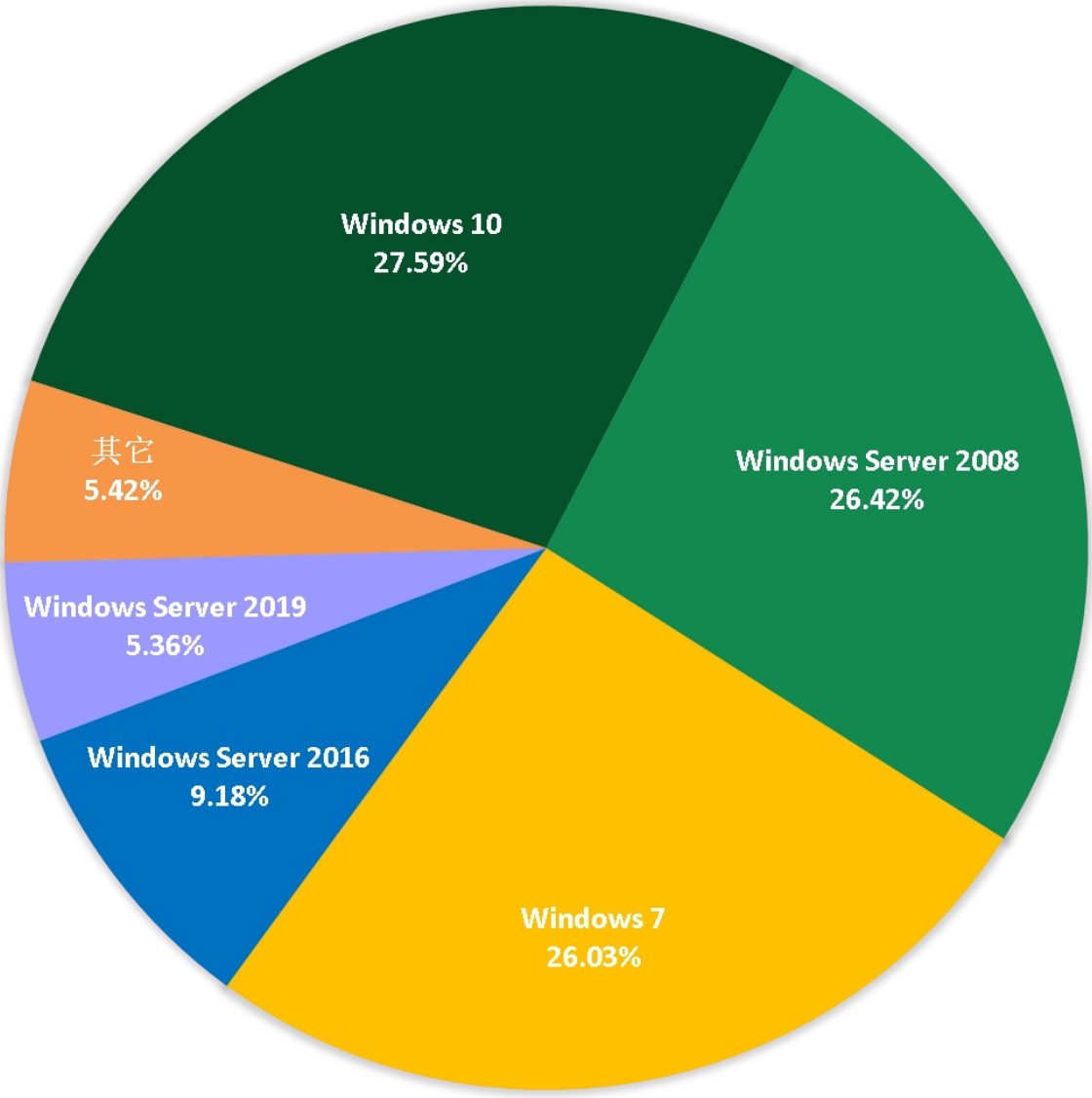


图 7. 2026 年 9 月受攻击系统占比

对 2026 年 9 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。

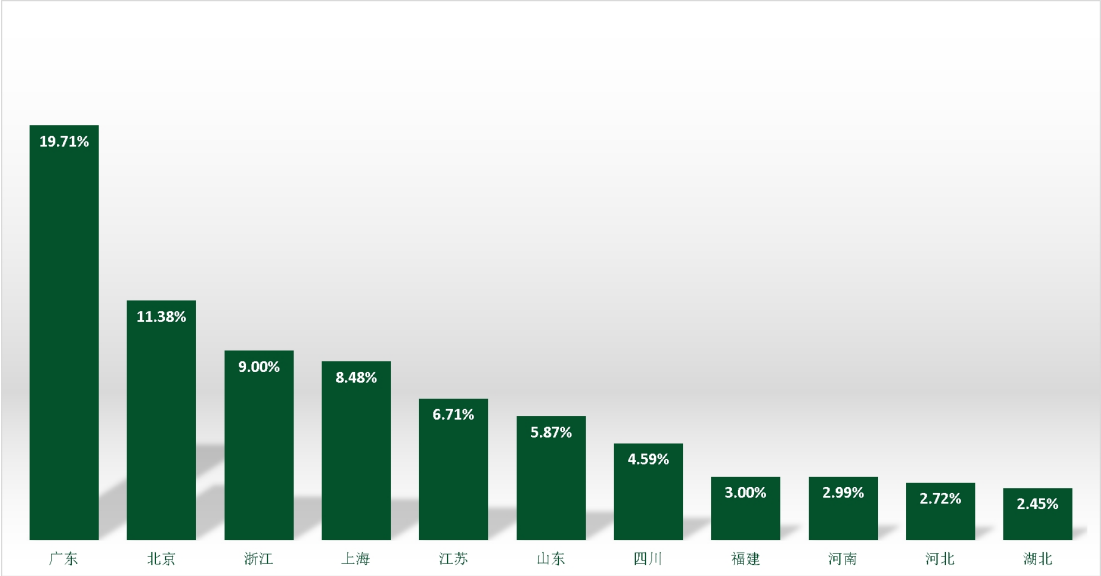


图 8. 2026 年 9 月国内受攻击地区占比排名

通过观察 2026 年 9 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。

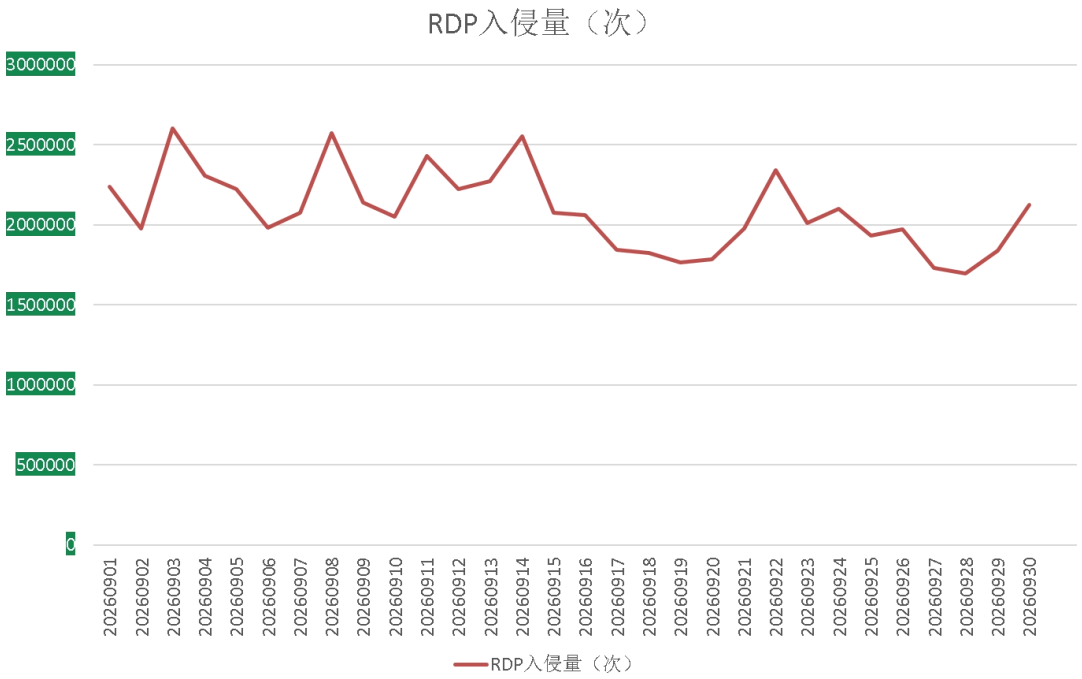


图 9. 2026 年 9 月监控到的 RDP 入侵量

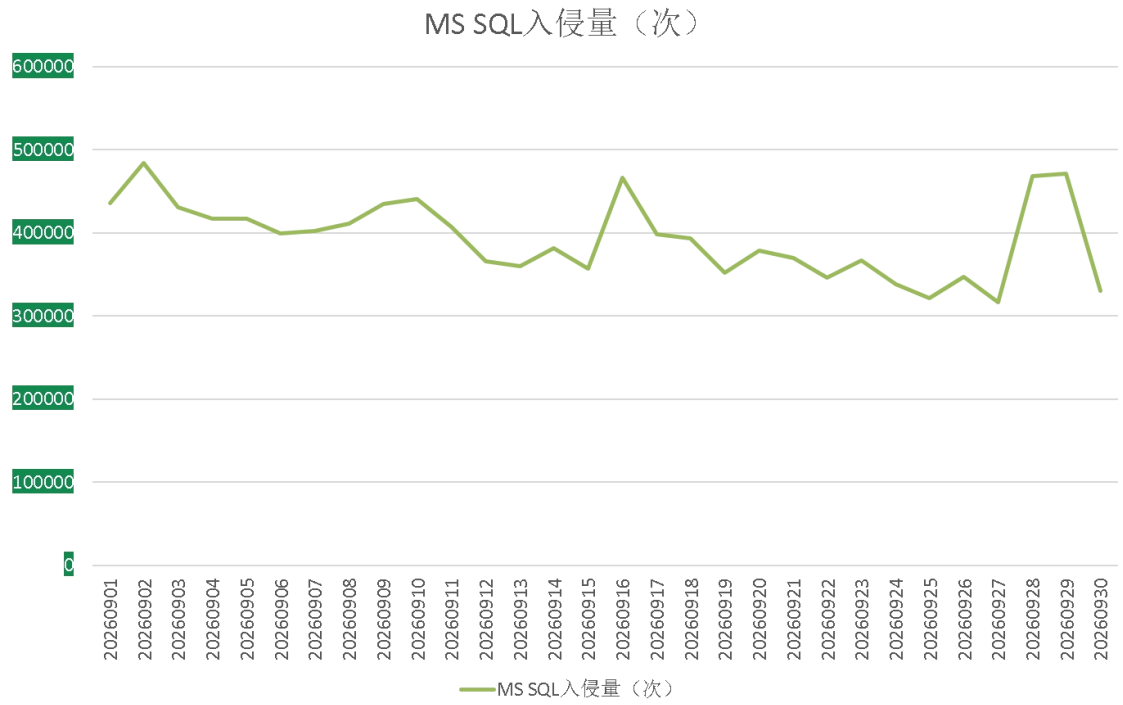


图 10. 2026 年 9 月监控到的 MS SQL 入侵量

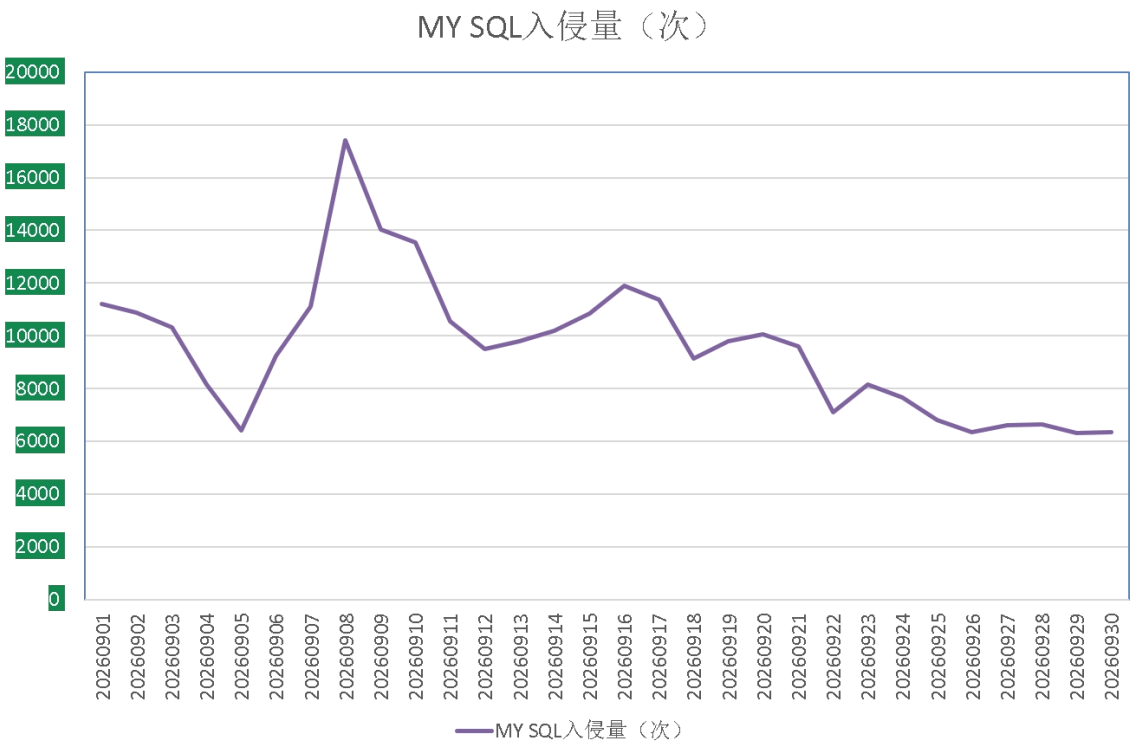


图 11. 2026 年 9 月监控到的 MYSQL 入侵量

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,植入 Anydesk 远控进行手动投毒。

✧ ths

属于 Sorry 勒索软件家族，该家族的主要传播方式为：利用漏洞发起初始攻击，支持跨平台勒索。

✧ bres

未知勒索家族或变种，由于相关受害者均未配合进行溯源分析，故待后续有效反馈再进行研判。

✧ weaxor（同 weax）

✧ cyberfear（同 bres）

✧ 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。

✧ flex

属于 BrzCrypt 家族，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。

✧ test

非勒索软件家族名，属于外部测试关键词。

✧ datahelper@cyberfearcom（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、SQLGlobeImposter 渠道、漏洞利用、僵尸网络进行传播。

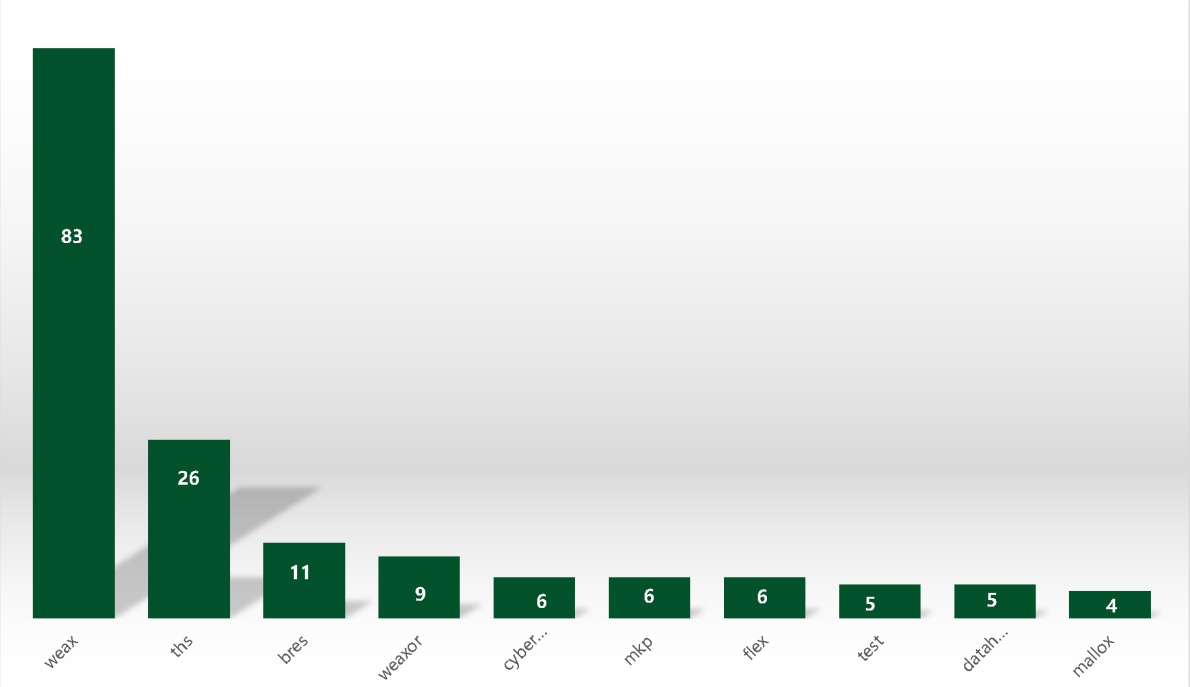


图 12. 2026 年 9 月反病毒搜索引擎关键词搜索排名

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 Phobos。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。

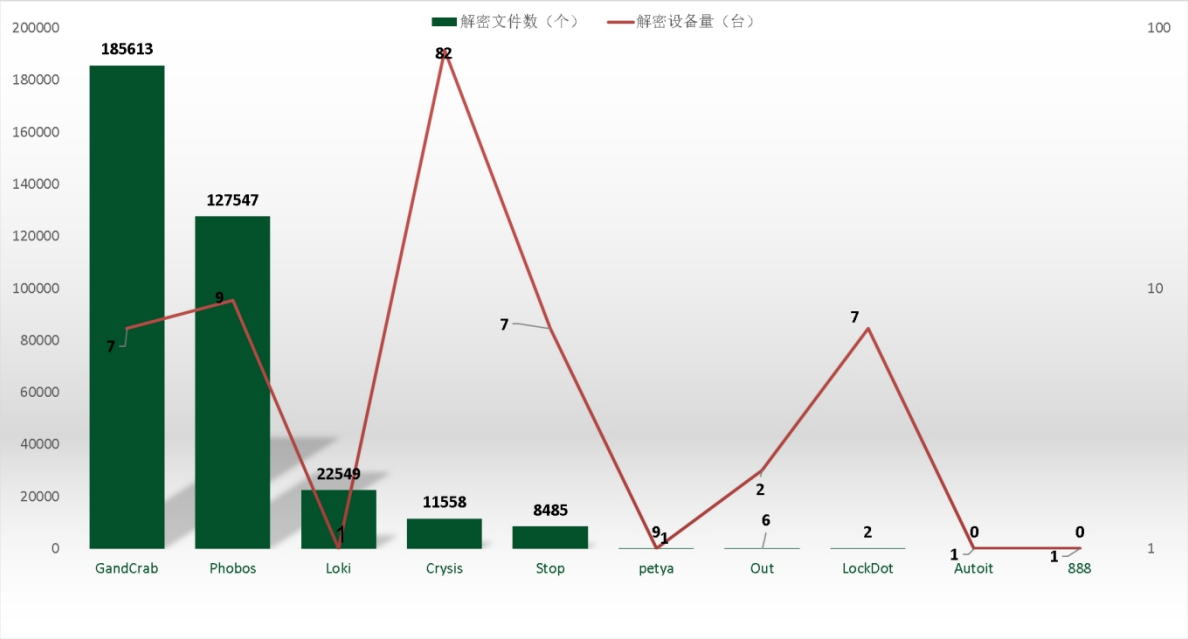


图 13. 2026 年 9 月解密大师解密文件数及设备数排名