360 高级威胁研究院

勒索软件流行态势分析

2025 年 1 月

360数字安全

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。

2025 年 1 月，全球新增的双重勒索软件家族包有 GD Lockersec，该家族目前以攻击 AWS 托管站点并窃取数据进行勒索为主。新增的传统勒索软件家族有 Contacto、Codefinger、DOglun，其中 DOglun 仅发现在国内少数论坛中进行传播。

以下是本月值得关注的部分热点：

1. **Wolf Haldenstein 律师事务所称泄露了 350 万人的数据**
2. **勒索软件利用 Amazon AWS 功能加密 S3 存储容器**
3. **勒索软件团伙冒充 IT 支持在 Microsoft Teams 网络中进行钓鱼攻击**

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:Weaxor 家族占比 40%居首位，第二的是 Makop 占比 14.29%的，RNTC 家族以 10%位居第三。

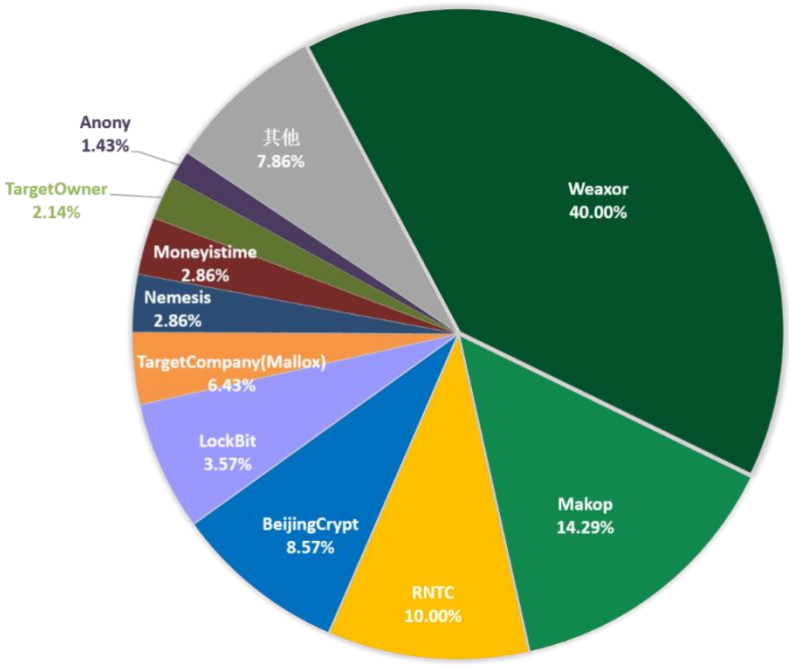

图 1. 2025 年 1 月勒索软件家族占比

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 2008。

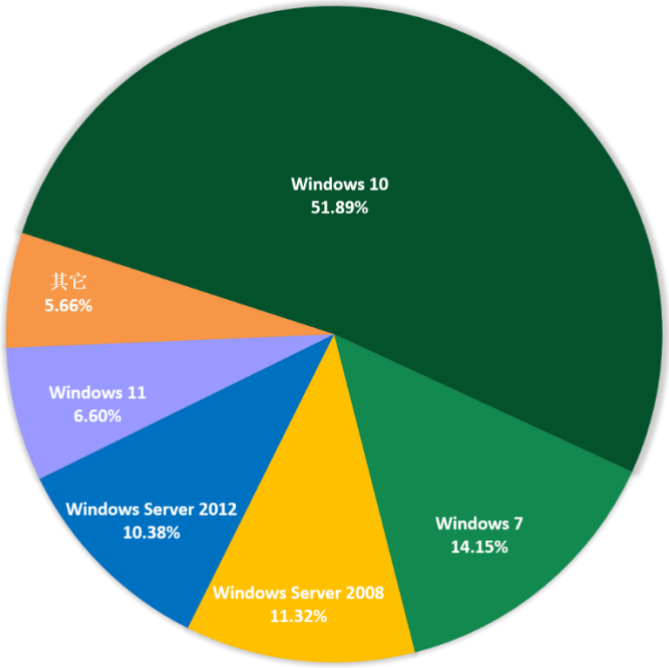

图 2. 2025 年 1 月勒索软件入侵操作系统占比

2025 年 1 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 大幅度高于服务器平台，NAS 平台以内网 SMB 共享加密为主。

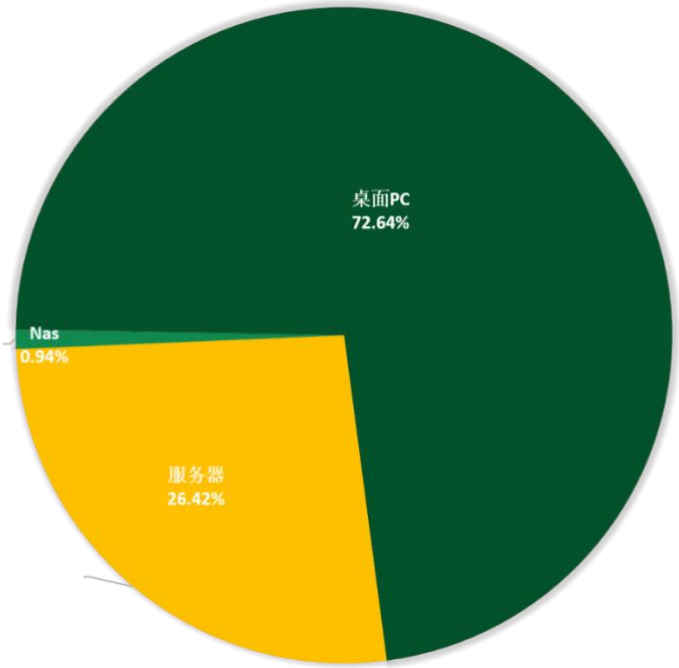

图 3. 2025 年 1 月勒索软件入侵操作系统类型占比

勒索软件热点事件

Wolf Haldenstein 律师事务所称泄露了 350 万人的数据

Wolf Haldenstein 报告称它遭遇了一次数据泄露，使近 350 万人的个人信息暴露给了黑客。此次事件发生在 2023 年 12 月 13 日，但该公司表示数据分析和数字取证并发症严重延迟了调查的完成。

2025 年 1 月 10 日，Wolf Haldenstein 在其网站上发布了一份数据泄露通知，而缅因州 AG 数据泄露门户网站上的一个条目将受其影响的总人数锁定为 3445537 人。虽然这个数字是在 2024 年 12 月 3 日确定的，但该公司一直无法找到许多受影响者的联系信息，因此尚未发送通知。

尽管该律师事务所表示没有证据表明暴露的数据被滥用，但它警告受影响的个人，黑客可能持有有关他们的以下信息：

- ✧ 全名
- ✧ 社会安全号码 （SSN）
- ✧ 员工
- ✧ 身份证号码
- ✧ 医疗诊断
- ✧ 医疗索赔信息

泄露这些数据会急剧增加网络钓鱼、诈骗、社会工程和其他针对受影响个人的针对性攻击的风险。该公司在确定受影响的人方面进展缓慢，以及延迟公开，情况只会变得更糟。尽管无法直接联系受影响的个人，但将向那些认为自己受到影响的人提供补充的信用监控保险。Wolf Haldenstein 还建议个人对其帐户上的未经请求的通信和可疑活动保持警惕，并考虑设置欺诈警报或安全冻结。该公司没有明确说明暴露的数据是否属于客户、员工或将其信息存储在其服务器上的其他个人。如果您与他们有业务往来，谨慎的做法是打电话给他们并询问此事件对您有何影响。

勒索软件利用 Amazon AWS 功能加密 S3 存储容器

一款新的勒索软件使用AWS的服务器端加密和只有攻击者知道的客户密钥(SSE-C)来加密 Amazon S3 buckets ，并索要赎金才能提供解密密钥。

有分析人员发现，一个名为“Codefinger”的攻击者已经加密了至少两名受害者。不过本轮攻击事件可能还会进一步扩大，或是出现更多攻击者开始采用此类策略进行加密和勒索攻击。

Amazon S3 是 AWS 提供的可扩展、安全且高速的对象存储服务，而 S3 buckets 是用于存储文件、数据备份、媒体、日志等的云存储容器。SSE-C 则是其提供的一种加密选项，用于保护静态 S3 数据，允许客户使用自己的加密密钥通过 AES-256 算法加密和解密其数据。AWS 不存储密钥，客户负责生成密钥、管理和保护密钥。

在 Codefinger 的攻击中,攻击者使用泄露的 AWS 凭证来获取 SSE-C 密钥生成权限。此后,攻击者在本地生成加密密钥以加密目标的数据。而由于 AWS 不存储这些加密密钥，因此即使受害者向 Amazon 求助，在没有攻击者密钥的情况下也无法恢复数据。

勒索软件团伙冒充 IT 支持在 Microsoft Teams 网络中进行钓鱼攻击

勒索软件团伙近期越来越多地采用电子邮件轰炸手段发动攻击，并在 Microsoft Teams 通话中冒充技术支持人员，诱骗员工允许远程控制并安装提供公司网络访问权限的恶意软件。攻击者往往会在短时间内发送了数千封垃圾邮件，然后利用已控制的 Office 365 实例呼叫目标，假装提供 IT 支持人员。

自 2024 年年底以来,在不少 Black Basta 勒索软件的攻击中出现了这种攻击策略。但安全研究人员发现与 FIN7 组织有关的其他攻击者可能也开始使用相同的方法。为了联系公司员工，黑客利用目标组织的默认 Microsoft Teams 配置，该配置允许来自外部域的呼叫和聊天。

在发现的案例中，黑客首先通过电子邮件发送了大量消息。不久之后，目标员工收到了来自名为“Help Desk Manager”的帐户的外部 Teams 电话。攻击者说服受害者通过 Microsoft Teams 设置远程屏幕控制会话。攻击者则释放了托管在外部 SharePoint

链接上的恶意载荷，该载荷会为攻击者提供对受感染计算机的远程访问。攻击者还会检查系统详细信息并部署第二阶段的黑客工具与恶意指令。

由于在攻击的最后阶段之前就被阻止了，研究人员认为黑客的目标是窃取数据，然后部署勒索软件。此外，研究人员还观察到 STAC5777 试图在网络上部署 Black Basta 勒索软件，因此攻击者可能与臭名昭著的勒索软件团伙有某种关系。

黑客信息披露

以下是本月收集到的黑客邮箱信息:

rlocked@protonmail.com	helper001@firemail.cc	maxfromhim@gmail.com
behappy123456@cock.li	viton@cock.li	BlackPanther@mailum.com
chinchoppa2299gayspilsss@yopmail.com	fridayboycrazy@dark.net	blackPanther@firemail.eu
mkp_sapport@keemail.me	Helpfile@generalmail.net	CloneDrive@mailum.com
sqlrecover@aol.com	Contacto@mailum.com	CloneDrive@tuta.io
backupsql@aol.com	newqq77@tuta.io	restoremail@mailum.com
wlojul@secmail.pro	newqq77@cock.li	hermesaa@tuta.io
middleeast@cock.li	el_cappuccino@tuta.io	blackbyte1@onionmail.org
onionhelp@memeware.net		

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）。

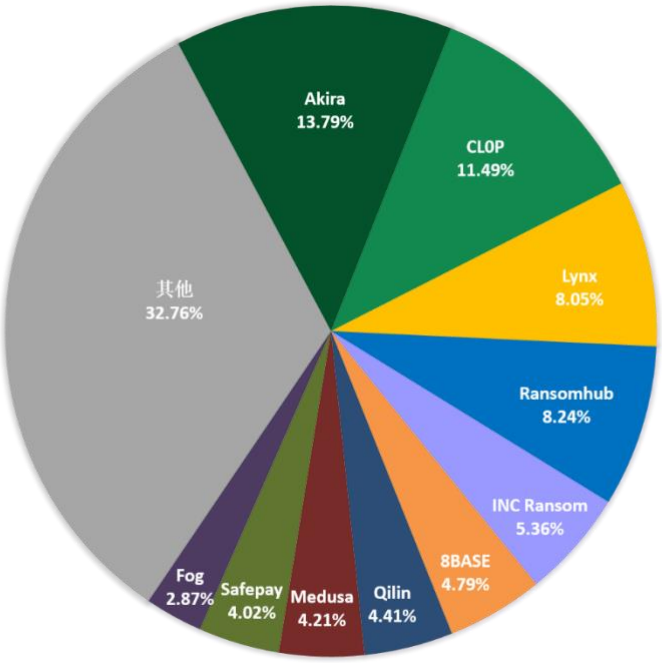

图 4. 2025 年 1 月通过数据泄露获利的勒索软件家族占比

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 522 个组织/企业遭遇勒索攻击，其中包含中国 4 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 7 个组织/企业未被标明，因此不在以下表格中。

Propulsion Academy AG	PrimoTicketing	The Chicano Federation
X-Pans	www.pcm.com.mx	Boart & Wire
Professional Computer Co	RUIA.COM	udb.net
BH Aircraft Company, Inc.	INNOTEKEP.COM	Wynnewood High School
Farrar Corporation	NOWINC.CA	Moraviakov s.r.o.
USGlobeCorp	TERRA.COM	Bring Solution
Kats, Jamison & Associates	POLARISTRANSPORT.COM	Gebäudereinigungsakademie
SCP Building Products	CALEXISCS.COM	QualiTech (qualitech.com)
Engineering Design Initiative	CDRSOFTWARE.COM	Kinseth Hospitality Companies
Angotti & Reilly	UTILISMARTCORP.COM	Douglas County, GA (DDCWSA.COM)
Land and Lakes	SEATTLECHOCOLATES.COM	Beyond79
Fayez Spa	WHITMOR.COM	Moinho Globo Alimentos

Dolmor Salon	BURRISLOGISTICS.COM	PJ's Rebar
Beauty Works Spa	ARTIKA.COM	pittman-construction.com
Trimaco	SPADERFREIGHT.COM	The University of Oklahoma (ou.edu)
Pembina Trails School Division	SULLYTRANSPORT.COM	SciTech Services, Inc.
vanguardpaints.com	BRADLEYCALDWELL.COM	Buttery (butterycompany.com)
adhydraclean.com	MADENGINE.COM	Union Studio
rightofwayequipment.net	ARROW.COM (CLEO)	Thilges & Bernhardt, Attorneys at Law
ibp.com	BUSINESSSYSINTEG.COM	Clnica CES
garcesfruit.com	BMIUSA.COM	Sharm Reef Hotel
andrewlauren.com	NORTHERNONTARIOWIRES.COM	Intelservice.com
centerracoop.com	HILLBROS.COM	Onecare
teligentems.com	Wannemacher Enterprises Inc	Findhelp Information Services
rqsi.com	ORU Mabee Center	Biomedical Caledonia Medical Laboratory (calmedlab.local)
omniflow.com	www.usmba.ac.ma	Imperial Valley Respite (ivrespite.com)
farmatodo.com	www.lnrbda.gov.ng	Riverina Medical
elf.uk.com	www.shihka.com.hk	Spectrum
foxconstructiongroup.co.uk	ELTEK Group (eltekgroup.com)	oyolasvegas.com
irisib.com	De La Salle High School (dlshs.org)	candelasyasociados.es
idrefjall.com	Cabinet JEAN LOUVEL SAOUDI	atpformosa.gob.ar
allbrightcotton.com	CREELED.COM	viacaojacarei.com.br
clarkpower.com	C3GROUP.NL	gelco-s-a.com.br
ad.snadc.com	ALPINEFOODS.COM	nicatel.com.uy
sgbllp.com	SHEERLOGISTICS.COM	lamejor.com.co
isisecurity.com	OFSPORTAL.COM	SERGAS Group
scrantonrealtors.org	SWEETSTREET.COM	Browdy (bl.local)
madisonforms.com	CONSULTANTS.COM	PHG CPAs (bushman.biz)
simcointeriors.com	PREMIERSUPPLIES.COM	Nash Brothers Construction (nashdom.local)
atr.com	BREAKTHROUGHFUEL.COM	Welcomehallmission.com

calfaucets.com	ICERIVERGREENBOTTLECO.COM	Novati Constructions
dkgrar.com	ENCOMPASSTECH.COM	Conad (conad.lan)
yhti.com	STEELBLUE.COM.AU	PT PINS Indonesia
njcar.org	HEARSTPOWER.COM	Delap & Waller
cannara.ca	CPS.EDU	healthcarewithinreach.org
atlanticelectrics.com	CLEO.COM	DURAYDUNCAN.COM
JFGV.ca	WESTERNALLIANCEBANK.COM	telering.de
worldfabricinc.com	ESPRIGAS.COM	mi.edu
HEXPOL COMPOUNDING AMERICAS	PISPL.IN	EKOMERCIO.COM
Southeast Supply	Berman Brothers	Jim Thompson
HIKARI SEIKO	Chappell Schools	Astaphans
johnpaulrichard.com	Safco International Gen Trading	cityofwesthaven.com
akran	Hospital El Cruce	pleasantsconstruction.com
vsstransportationgroup.com	Arrow Motor Auctions	T. Hasegawa USA
ttucorp.com	PINELAND BHDD COMMUNITY SERVICES	Barber Specialties
jayaapparelgroup.com	www.reesndt.com	Costex
sunrise-soya.com	topackt.com	Patriarche Office of Architecture
Kombinat	Bwfg.at	COROB
he2b	CENTRIC.EU	RocSearch
Prasaga	samsill.com	Unisource Information Services
Centromedicoenova	Kooijman Vianen (kooijmanvianen.nl)	schuff.com
malindoair.com | SOLD	archaeologicalresearchservices.com	granbyindustries.com
Night Hawk	WorldNet Telecommunications LLC	plasmatherm.com
Perfect Plastic	Enghouse (ex. Navita)	arunestates.co.uk
nenok.de	starkaerospace.com	brachot.com
Benuta	www.missionbank.bank	avril.ca
Ottawa Family Physicians	FIO	migonline.com
Menway	Black Hills Regional Eye Institute	bnext.nl
alkodistributors.com	Sawley Lock O'Callaghan	Sheyenne Tooling & Manufacturing
Engine Power Source	Omni Fiber LLC - Press Release	Evidn

ome.tv	gaylord.org	Peikko
FENSTERMAKER	sdkgroup.com	www.wisesocon.com
Jalaram Produce	www.manpower.com	Qualinet
KPI Engineering	Architects West	Ichikawa North America Corporation
Scott Engineering	www.grohe.com	Thomas J. Henry Law
Tri-Sen Systems	ilemgroup.com	amerplumb.com
Silverado Contractors	Hayloft Property Management	Capesesp
soitinlaine.fi	www.americanstandard-us.com	Metalmatrix Clamps
payahmedabadechallan.org	Christian Community Aid	xtremmedia.com
Zschimmer and Schwarz	whychoosebw.com	OmniRide (omniride.com)
SCV Med Group	SANTA MARIA LABORATORIO	www.fairhallzhang.com
midwaymetals.com.vn	Mintz Law Firm, LLC	www.leaguecenter.org
Premierautocredit.com	boardman-hamilton.com	www.temotekstil.com.tr
Cahoon Farms	Jacobs & Thompson	www.excelresourcing.co.uk
Marshall & Bruce Printing	icicibank.com	www.mie.com.my
Johnston	semesco.com	www.rotaryeng.co.th
The Wendt Agency	brunetti.com	www.primalwear.com
Rossi Real Estate (ROSSIDG.LOCAL)	solge.es	EVAS Group
Delta Screen & Filtration ()	precisionmechsd.com	depewgillen.com
By design	RETAL Baltic Films	castlehillha.co.uk
Plymouth Foam	miedemaproduce.com	drive-lines.com
Boldon James	JOMARSOFTCORP.COM	pnp.co.za
air europa	FAAB Invest Advisors Private Limited	Rent-2-Own
tnlottery.com	Nimbus Facility Services	alansarioman.com
Strategic Materials	Inaya Clinique	Northern Lights Electric
Commercial & Residential Management Group	supremegroup.co.in	Chain And Rope Suppliers LTD
daVinci	Bethany Hospital	Galfer
TRIVAD	Marukai	Permoda
Wallin & Klarich	PetroVietnam Exploration Production Corporation	hapsch.de

Cimarron Telephone Company	The Urswick School	bendixengineering
biagibros.com	malindoair.com	Fukoku Co. Ltd.
Turning Leaf (TURNINGLEAF.local)	Sentinel Systems	kingpower.com
Heart to Heart Hospice	Angotti & Reilly	Press Color
City Of Beloit	Jacquet Weston Engineering	Huntington Hotel Group
Boutin Jones (boutindentino.com)	compass-underwriting-ltd	fwmep.edu
Mission Locale Montpellier	cana group corp	Surface Combustion
boginmunns.com	Rabwin	Slawson Companies
Versalys.com	Zuk Group Hacked	sahpetrol.com.tr
Miles Industries	D & M Trim	acquafertil.com.br
Addison Saws	Delta Fabrication and Machine, Inc	General Digital
English Braids	Clutch Industries	General Digital CRM
Aden Footwear	Richardson	Muscogee County School District
NG Automatics	TG3 Electronics	BBB Industries, LLC
Philip Laney & Jolly	WELKER | World-Class Manufacturing	astaphans.com
Menominee Tribal Clinic	MERCURYGATE.COM	jimthompson.com
ARDEX Australia	MassDevelopment	Arrotex Pharmaceuticals
BENASSI IMMOBILIARE SAS DI BENASSI ROBERTO E C.	USE Federal Credit Union	Pus Gmbh
Israel Ministry of National Security Hacked	Refreshment Services Pepsi	HECTARE
BBLAWFIRM	Marina Family Medical	Lake Shore Public Schools
delpackaging.com	Kassin & Carrow	SPORT BOUTIQ
lnetwork	gonzalesusd.net	CED Solutions Computer IT Training Centers
Acoustiblok	nightingalehammerson.org	IRO PARIS
metalurgica roma	realtaxcanada.com	Weininger Metall System GmbH
broward.edu	Gossett Motor Cars	Omnitravel
QCN CO., LTD	Divimast	ASCOM S.p.A.
Carthage Police Department	VODOTEHNIKA D.D.	Bergström Wines
sce.org.sg	fol-23.fr	Drivestream
Mercy Supply Collaborative	Vodotechnika	Drywall Partitions

Kaisersbach.de	Chain And Rope SuppliersLTD	AAA Environmental
Neovita.de	LYNXSPA	u0 Excel Transportation
cnnindonesia.com	Regina Coeli Convent	Saint-Bar (saintbar.be)
Mapping Solutions	Kilgore College (kilgore.edu)	D-7 Roofing
Aquasys	Washington Gastroenterology (DHSWA.NET)	Sunflower Medical Group
https://leehartman.com	peponline.org	VELSOL.COM
Alo Center (hq.aloteknik.se)	Taylor Regional Hospital (thcg.local)	WSINC.COM
Grand Fire Protection	platinumcollision.com	Maverick Constructors
lhps.org	The Hoff Brand SL	A Bar A Ranch
Mark Resolve Inc	Woodlake	Los Andes
Prinston Pharmaceutical (huahaius.com)	Volt Infrastructure	Bluegrass Ingredients
RDC Architects	Dona Formosa	Action Imports
International AIDS Vaccine Initiative (iavi.org)	JD Lighting	Gunnar Prefab
Weeks, Brucker & Coleman, Ltd | Legal Services	Delta Dental of Washington	yoniot.cn
AIshu, Eshoo	Netform GmbH	molars.co.ke
www.fgse.cu.edu.eg	Farmacia Cofar	Hunter Taubman Fischer & Li
Let’s Secure Insurance	anupalanonline.com	akantha.fr
Metro Wire & Cable	bsegroup.it	Veccio and Company PLLC
aws.amazon.com | 10 btc	www.solariumrevestimentos.com.br	hasa-arg.com
DataSociete	Access Capital Partners SA	perucontrols.com
bigotti.ro	www.liteputer.com.tw	datascan.com
mcpathology.com	Prestige Maintenance USA	Auxis
nutripack.eu	safecoastseafoods.com	Montreal North
paradiseschools.org	greyform.sg	maxvaluecredits.com
welcomewagon.com	proexequialesresurgir.com	www.smawins.com
cellsciencesystems.com	bellandgraham.co.nz	lscd
Keepz	termopuerto.com	YorkTest Laboratories
envirosep.com	equipo-postal.com	ISOR

Jan Nygaard	ddelta.com.mx	www.alliancemat.com
KEEACTIONSPORTS.COM	combinedpoolandspa.com	Amourgis & Associates
OLAMETER.COM	AKConstructors.com	Nikki-Universal Co Ltd
USLUGGAGE.COM	Lowe Engineers	www.geedingconstruction.com
AMPOL.COM.AU	fplfood.com$675MUSA21GB	Lyons Specialty Co.
SPGUSA.COM	betclic.com	SolGeo AG Baugelogie and Geotechnik
EMKAY.COM	communisis.com & paragon.world	Grupo Buddemeyer
COYOTE.COM	anwsd.org	VOLTAIRE AVOCATS
HERTZ.COM	optiline.com	Jay Enn Corporation
JAKKS.COM	www.eurocert.pl	Tarnaise des Panneaux SAS
Punjab.gov.pk	jgele.com	Carrollton Orthopaedic Clinic
NISSINFOODS.COM	WPD.WOODPORTDOORS.COM	confluxhr.com
COVESTRO.COM	Solaris Pharma	groupegm.com
SDITECHNOLOGIES.COM	Indus Towers	Kitevuc - Equipamentos E Veiculos Utilitá rios E Comerciais
CLAWLOGISTICS.COM	The Metropolitan Borough of Gateshead	lianbeng.sg
LINFOX.COM	AVI Southeast	

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。

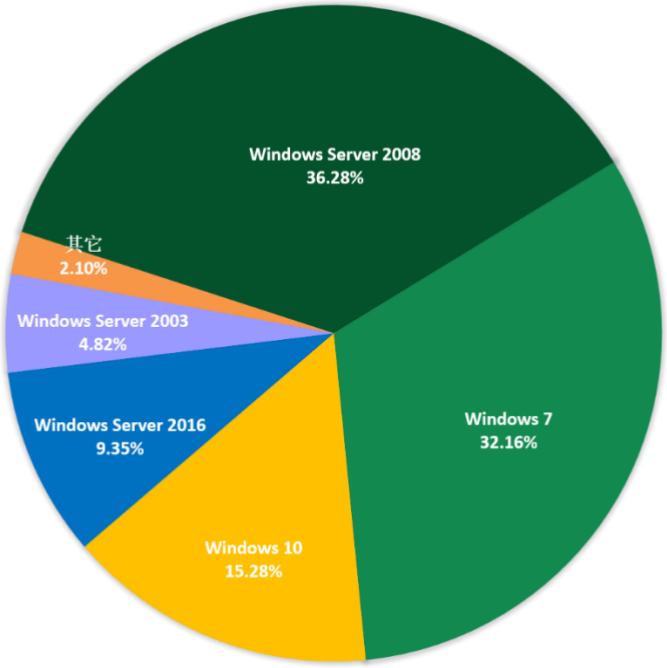

图 5 2025 年 1 月受攻击系统占比

对 2025 年 1 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。

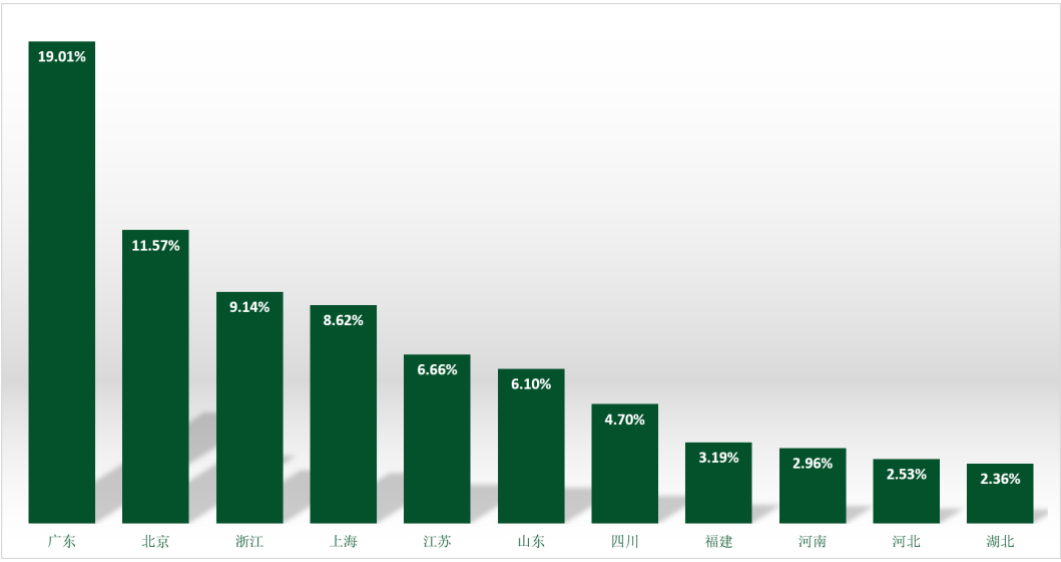

图 6. 2025 年 1 月国内受攻击地区占比排名

通过观察 2025 年 1 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。

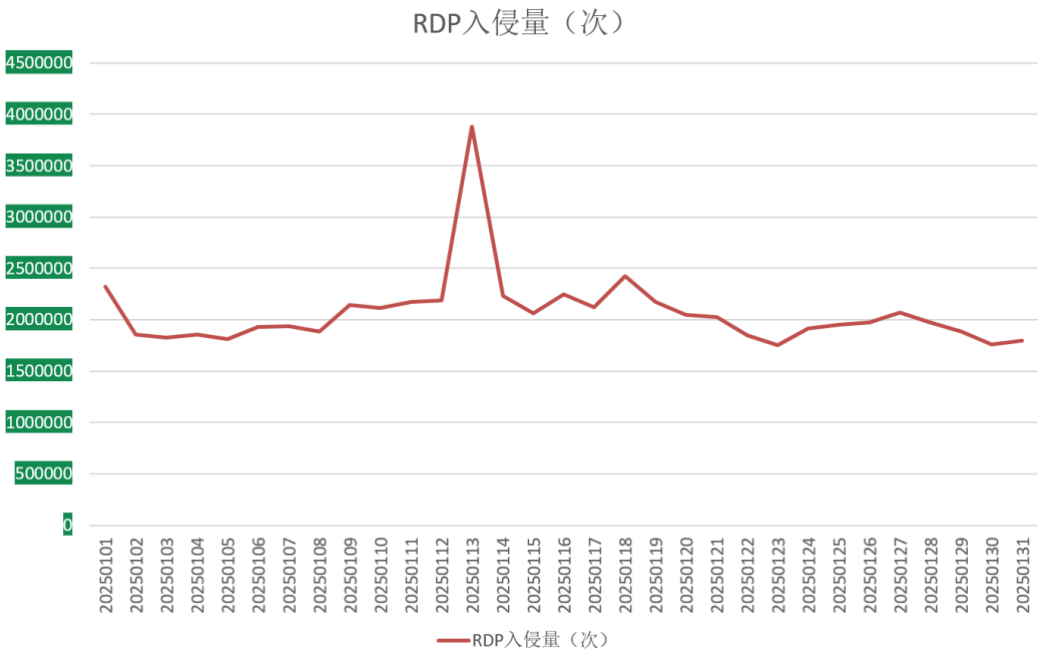

图 7. 2025 年 1 月监控到的 RDP 入侵量

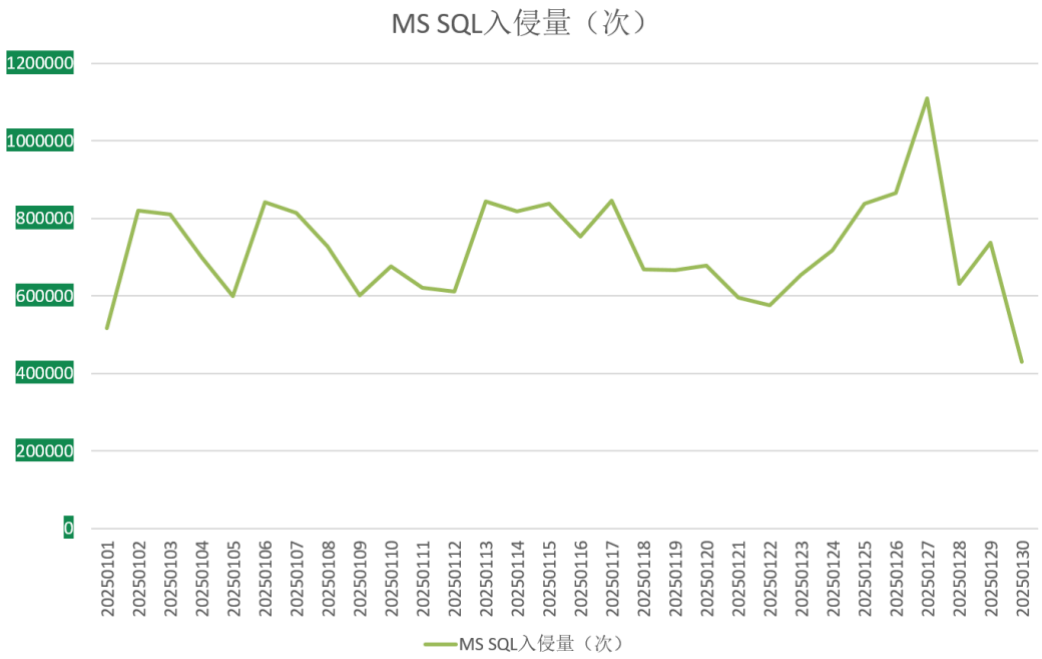

图 8. 2025 年 1 月监控到的 MS SQL 入侵量，12 月 30 日的数据由于一些设备被大量暴破导致数据大幅增高，随后即恢复正常水平。

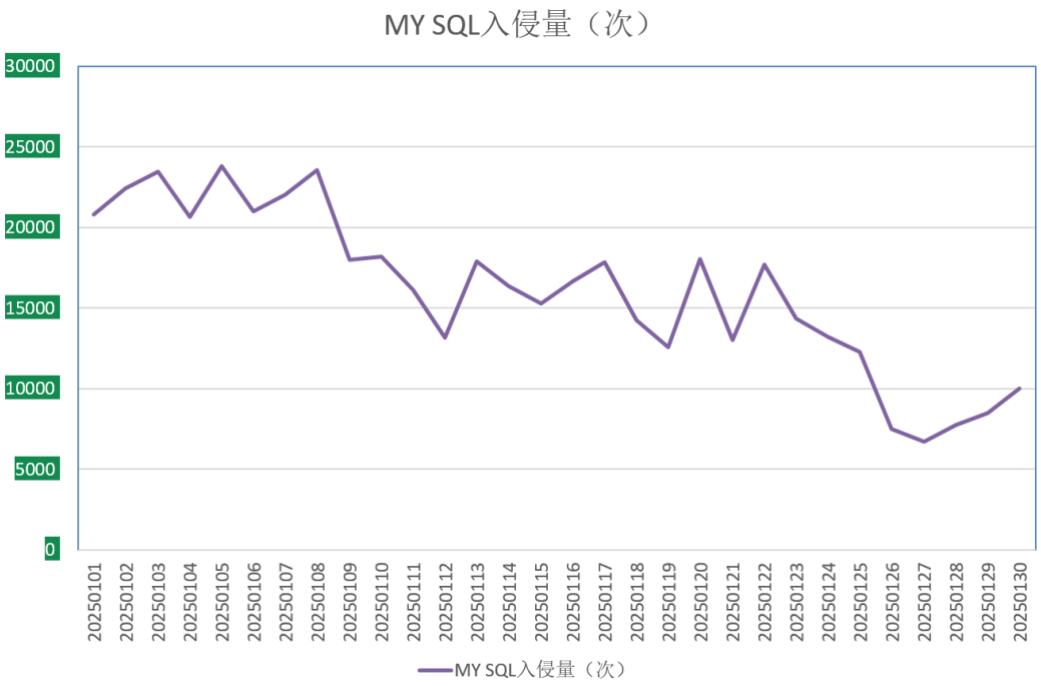

图 9. 2025 年 1 月监控到的 MYSQL 入侵量

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。

- wexor：属于 Weaxor 勒索软件家族，该家族的之前的主要传播方式为：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。自本月起则主要以漏洞利用方式进行投毒。
- wxr：同 wexor。
- 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。
- 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。
- 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。
- bixi：同 baxia。
- src：同 mkp。
- 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。devicdata：同 hmallox。
- sstop：同 wstop。
- devicdata：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本曾通过匿影僵尸网络进行传播。

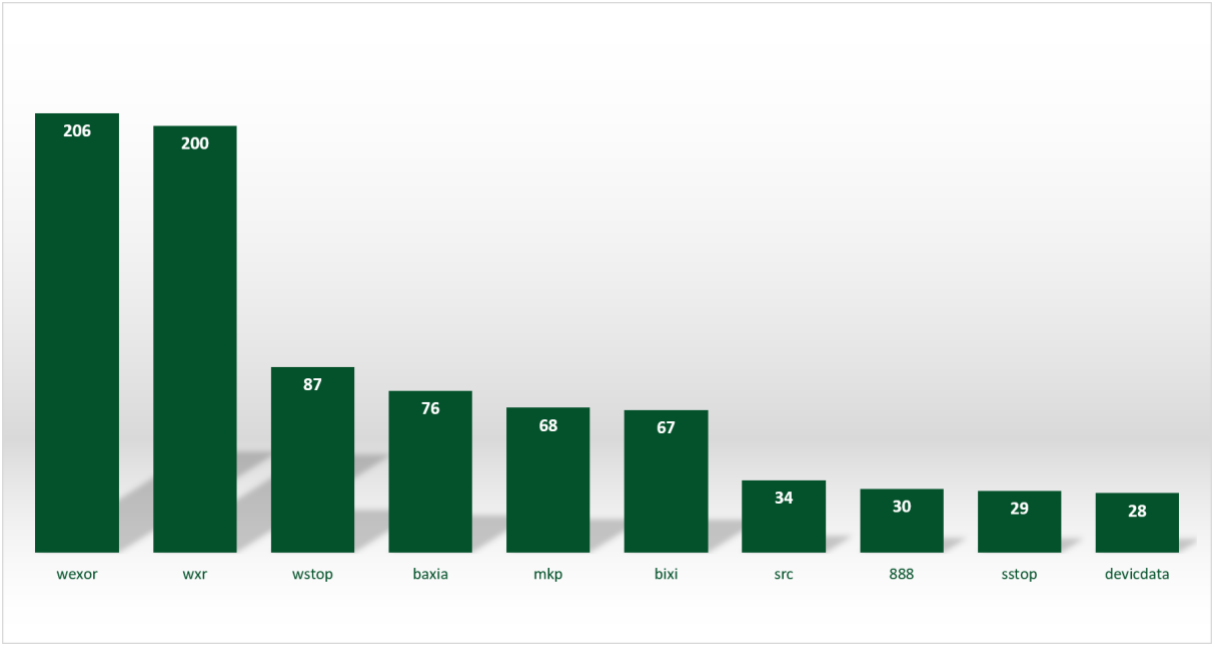

图 10 2025 年 1 月反病毒搜索引擎关键词搜索排名

解密大师

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

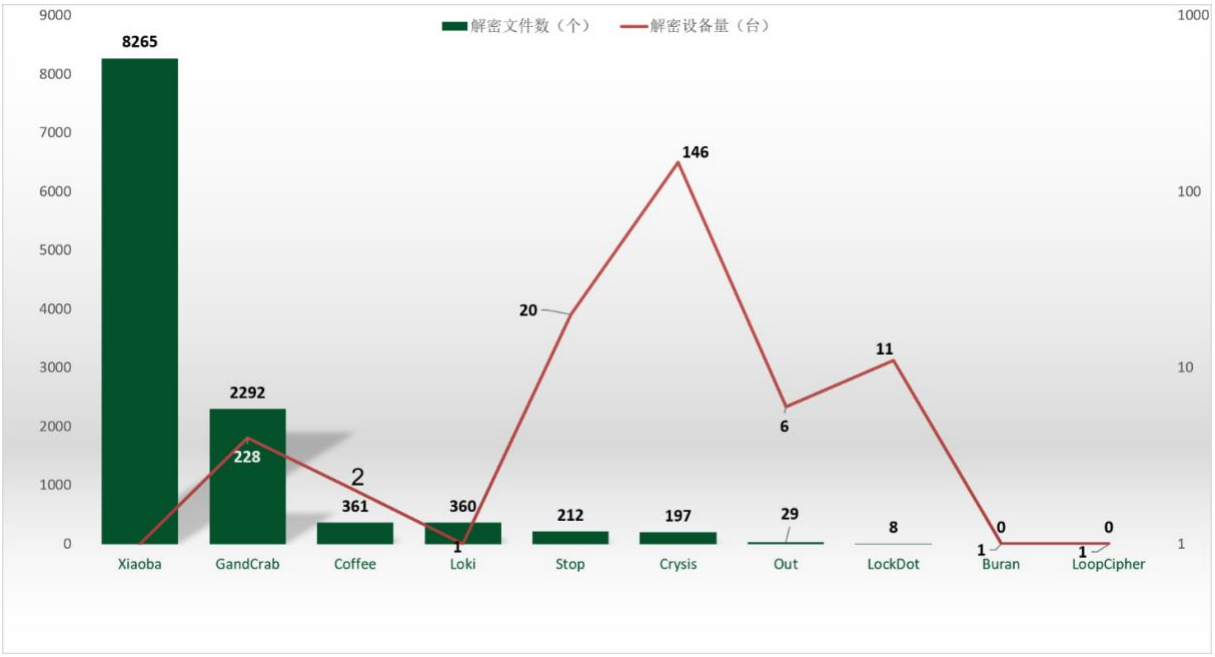

图 11. 2025 年 1 月解密大师解密文件数及设备数排名