

勒索软件流行态势分析

2025 年 10 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，企业数据泄漏风险不断上升，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 10 月，全球新增的双重勒索软件有 Tengu、Kyber、Genesis、Brotherhood、Radiant、Nasirsecurity 等多个家族，传统勒索软件家族新增 Monkey、ThunderKitty、BrawLocker 等多个家族。其中 Monkey 家族有明显的 AI 生成痕迹，在其 Linux 版本的样本中存在删除 Windows 卷影副本的代码。BrawLocker 则使用 Powershell 脚本通过投毒者手动输入密钥加密 Braw 后缀的文件，此类文件是 Blackmagic Design 的 Blackmagic RAW 原始视频格式，用来保存摄像机传感器的原始影像数据和元数据，以便在后期进行高动态范围调色与处理。

加密后缀为 spmodvf 的勒索软件已经在国内持续传播数月，已在本月冲入 TOP 榜单。遗憾的是，该勒索软件受害者数月来无一例配合进行溯源分析，而是第一时间选择重装或重置系统。而从运维人员反馈看，该家族勒索软件的受害者多集中在医疗行业。根据 11 月 1 日起开始实施的《国家网络安全事件报告管理办法》相关规定，对于此类网络安全事件的报告已成为法定义务。在国家对网络安全的日益重视，以及相关法律法规日趋完善的背景下，我们相信今后对此类勒索攻击事件的溯源工作可以开展得更加顺利。

以下是本月值得关注的部分热点：

- 1** 美国航空子公司 Envoy Air 遭 Oracle 数据窃取攻击
- 2** 零售巨头无印良品因供应商遭勒索攻击而停止在线销售
- 3** Qilin 勒索软件在 Windows 中利用 WSL 来运行 Linux 加密器

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 38.06%居首位，第二的是 Wmansvcs 占比 21.64%，LockBit 家族以 8.96%占比位居第三。

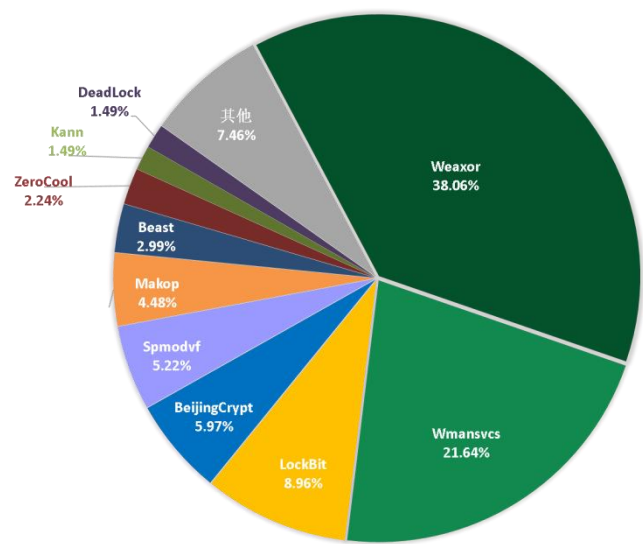


图 1. 2025 年 10 月勒索软件家族占比

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 2008。

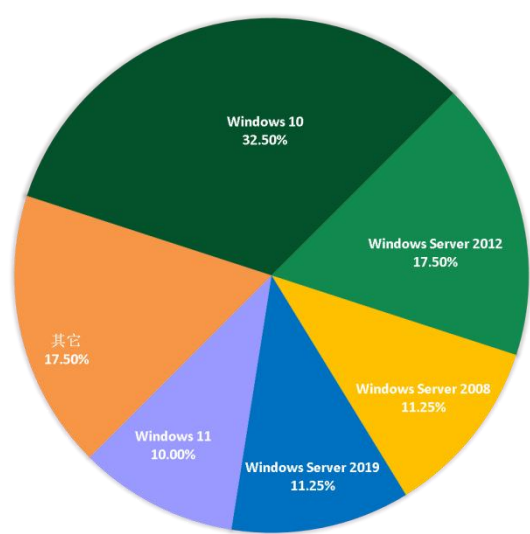


图 2. 2025 年 10 月勒索软件入侵操作系统占比

2025 年 10 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小幅领先桌面 PC。

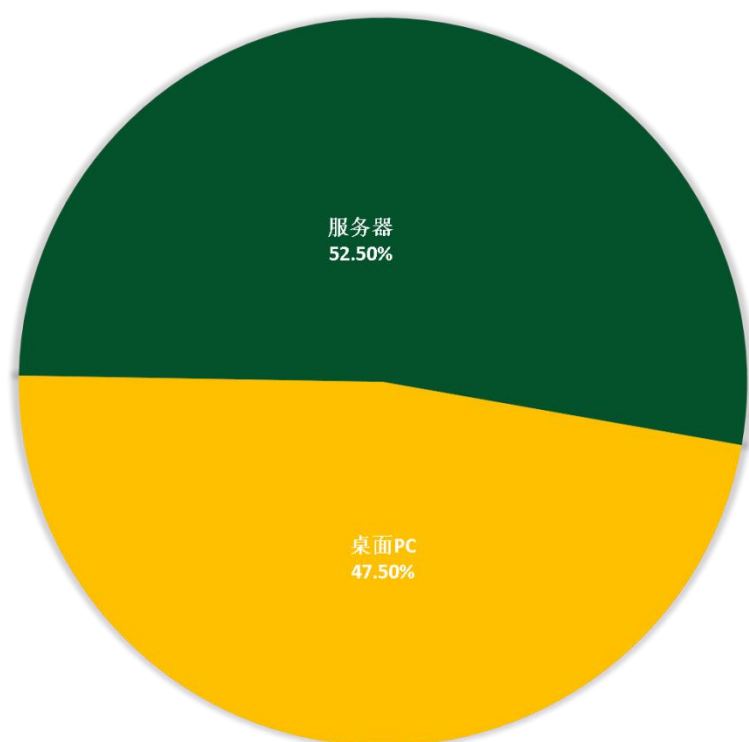


图 3. 2025 年 10 月勒索软件入侵操作系统类型占比

勒索软件热点事件

美国航空子公司 Envoy Air 遭 Oracle 数据窃取攻击

美国航空子公司 Envoy Air 确认遭受 Oracle 数据窃取攻击。根据报道，C10p 勒索软件团伙通过 Oracle E-Business Suite 应用程序，窃取了 Envoy Air 的部分商业信息和联系方式，并将美国航空列入其数据泄露网站。尽管 Envoy Air 表示未发现敏感或客户数据被泄露，但该事件仍然引起了广泛关注。

此次安全事件源自 C10p 团伙对 Oracle E-Business Suite 系统的攻击。早在 2024 年 8 月，C10p 就利用一个零日漏洞（CVE-2025-61882）侵入多个组织，部署恶意软件并窃取数据。尽管 Oracle 曾表示攻击者利用的漏洞已在 7 月修复，但后续情况表明，攻击者利用了这一未修补的零日漏洞。C10p 团伙并未披露受影响的具体公司数量，但据了解，至少有数十家组织遭到数据窃取。

此外，C10p 团伙还在同一波攻击中向哈佛大学施压，即便只有少数与该校某小型行政单元相关的人员受到影响。C10p 此前已在 2023 年通过多个漏洞攻击多个平台，如 MOVEit Transfer 和 GoAnywhere MFT，导致全球上千家公司的数据遭窃。

C10p 自 2019 年起开始活跃，最初以加密勒索为主，之后转向利用零日漏洞窃取数据，已成为全球最知名的勒索软件团伙之一。美国国务院目前提供 1000 万美元奖励，寻求与该团伙活动相关的外国政府信息。

零售巨头无印良品因供应商遭勒索攻击而停止在线销售

近日，日本零售公司无印良品因其配送合作伙伴 Askul 遭遇勒索软件攻击，导致无印良品的在线商店服务暂停。此次事件影响了包括在线购物、订单历史查看和网页内容显示等多个服务功能。无印良品在日本时间周日晚间宣布暂停相关服务，并在周一下午的更新内容中表示，除在线购买和申请月度服务外，其他功能已恢复。公司目前正在调

查哪些订单受到影响，并计划通过邮件通知受影响的客户。

Askul，作为一个主要处理办公用品及物流业务的电商平台，确认遭遇勒索病毒攻击，导致其网站和订单处理系统瘫痪。这次攻击造成了多个业务中断，包括退货申请、收据邮寄、目录邮寄等服务暂停。同时，通过电话或网站也无法联系 Askul 客服。Askul 正在调查是否有个人信息泄露，截至目前，尚未有勒索软件团伙宣布对此次攻击负责。

因 Askul 专门处理无印良品在日本地区的订单，此次攻击事件仅影响无印良品在日本的业务，无印良品在其他国家的门店运营正常，没有受到此次攻击影响。

Qilin 勒索软件在 Windows 中利用 WSL 来运行 Linux 加密器

Qilin 勒索软件利用 Windows Subsystem for Linux (WSL) 技术，绕过传统的安全防护，成功在 Windows 系统上运行 Linux 加密程序，成为当前最活跃的勒索软件之一。Qilin 最初以“Agenda”之名于 2022 年 8 月出现，随后于 9 月改名为 Qilin。到 2025 年下半年，该勒索软件每月攻击超过 40 个新受害者，覆盖 62 个国家，影响极广。

Qilin 的攻击手段主要包括使用远程访问工具（如 AnyDesk、ScreenConnect 和 Splashtop）入侵目标网络，窃取凭证和数据。同时，攻击者还利用 Windows 自带工具（如 Microsoft Paint 和 Notepad）来扫描文档中的敏感信息。此外，Qilin 勒索软件还采用了“BYOVD”（自带漏洞驱动）攻击技术，通过安装漏洞驱动程序（如 eskle.sys）禁用安全软件，并使用“dark-kill”和“HRSword”工具清除其恶意活动痕迹。

最具创新性的是，Qilin 攻击者通过 WSL 在 Windows 系统上执行 Linux 加密程序。由于 Qilin 的加密程序是 ELF 格式的 Linux 可执行文件，无法直接在 Windows 系统上运行，因此攻击者利用 WSL 功能，在 Windows 境中运行这些程序，成功规避了许多传统 Windows 安全工具的检测。这种方法显示了勒索软件家族如何适应混合 Windows 和 Linux 环境，进一步增强其攻击能力。

通过这种方法，Qilin 勒索软件能够最大化提升其攻击范围，并绕过许多依赖于 Windows 操作系统行为的防御机制，使得检测和防范变得更加困难。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

stolenrans@hotmail.com	unlock@cl-leaks.com	decryptionwhy@india.com
support2@norviscon.com	support@help-center.com	Austinlecca@proton.me
support1@bancerc.com	support@pubstorm.com	Ioniaa@tutamail.com
decryption@protonmail.com	support@pubstorm.net	Nilson@firemail.de
findourtxt@tuta.io	r@n50mw@re	nilson@msg.ws
findourtxt@mailum.com	fastsupport@protonmail.com	stevensfalls@outlook.com
onlinechat@cryptolab.net	mvarsonic@atomicmail.io	richardfeuell@outlook.com
n0b0dyh4@onionmail.org	WayneEvenson@protonmail.com	247help@cryptolab.net
Faster@mailum.com	WayneEvenson@tutanota.com	monkeyransomware@onionmail.org
allosfix@hotmail.com	juanjoorodriguez@protonmail.com	lockaaaabbbbit@proton.me
MastersRecovery@protonmail.com	juanjo. rodriguez@tutanota.com	horox@cock.li
MastersRecovery@cock.li	addressesupcr@protonmail.com	BM-2cUm1HG5NFf9fYMHpZLhjoBdXqde26iBm 2@bitmessage.ch
unlock@help-me.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）。

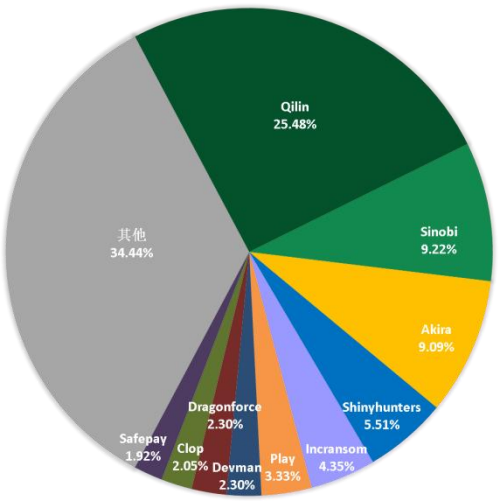


图 4. 2025 年 10 月通过数据泄露获利的勒索软件家族占比

以下是本月被双重勒索软件家族攻击的企业或个人。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 781 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 14 个组织/企业未被标明，因此不在以下表格中。

TMF Logistics	dekalbcountyga.gov	Downes
aa-llp.com (aa.law)	BRDSoft	ms-security-ltd.com/Cyprus/1.48TB
holtzofficesupport.com	ccls.org	forestry.gov.jm
Fouad Alghanim & Sons Group of Companies Holding W.L.L.	McDonald Building	Complete Milling Lab
Hometown Credit Union	Greater Mental Health of New York	Paleontological Research Institution
Gun Accessory Supply	Tryon Distributing	empirico-mr.com
CCI Tax Pros, Inc	Grupo JSA	tango-hotel.com.ar
VZW Avalon	MSC-Wireless	bridgenetcommunicationsrgv.com
verdugohillsdental.com	Integra SAP	krne.com
The Matlusky Firm LLC	South Atlanta Medical Clinic	glatten.de
CyPark Resources Berhad	Harmony Brands	portofuneralhomes.net
TENAX Law Group PC	Phoenix Village Dental	ggw.net
Thompson Dorfman Sweatman	ocbar.org/USA/114GB	cmlmachinery.com
FA Servers	oxfordcounty.ca	Bellingham Vet Center
Center for Neuropsychology Learning and Development	cdom.org	Central Jersey Medical Center
Disseny Dental	Cape Dara Resort Pattaya	Sunbulah Group
Post Ranch Inn	saacke.com	Brevard Skin
Architectural Systems	Computer World W.L.L	Artan Holding
Saxun by Giménez Ganga	Selig Enterprises; AAA Parking	grupocaparros.com
C.M.G, entreprise de serrurerie et métallerie à Saint Calais	Cabinets 2000, LLC	Den Hartogh Logistics
Anderson-Moore Construction	Al Ahly Leasing & Factoring Company	Confie
LATCOM	Egaraset	americanhome
Huber , Erickson & Bowman	Peppermint Properties	Five Star MechanicalInc.
Boilersource	Corneilhan	Carlson Building Maintenance
Sullivan Interests	B. G. Schneider Treuhand AG Information	Friendly Gus
Buffalo Games, Edaron, Ceaco	Gruppe Lehen	Momentum Logistics
Silverlake Axis	Imagicle	Sternthal Montigny Greenberg St-Germain
ANSELL.COM	Linxx Global Solutions	Kevmor
The Gerson	DALCANS	Woodmen Valley Chapel

RPI Roofing	Accord Carton	UVJ Technologies
Econo-Pak	Khatami Law	Motility Software
Apache OpenOffice	SANgel	Orion Communications and Public Relations
Suarez & Menendez	Kudela & Weinheimer	Coal Industry Social Welfare Organisation
bagnoles.nl	Distribuciones Camba	Israel Fuel System
halifax.k12.va.us	Klima-Therm	Falco Electronics
ASKUL	healthandvitalitycenter.com	ucisd.net
Spindletop Center	BARCO Rent-A-Truck	georgetown-brewing-co
Evolve Mortgage Services	Octomeca OY	NextGen Mold Technologies
ApleNet Co., Ltd	Gas Generator Solutions	Benedict Industries
nationalcoatingsinc.com	Cellini Design Center	tongapower.to
DILOSA FOOD COMPANIES	Stowaway Storage	Accelerated
fsbgroup.ca	JA Jennings	Elmer W. Davis
semag.fr	BIOPHARMEX, SA de CV	Midsun Group
axxia.fr	Stephenson's Rental Services	Northern Air Systems
Time Equities	London Women's Clinic	Sdii Global
TBM Service Group	Scales Sales & Service	msssolutions.com
PF / PS	Laloma	MBS Secure
OpenEyes Technologies Inc.	My Florida Case Management Services, LLC	SG Ceresco
Phillips Printing Company	The Blood and Marrow Transplant Group of Georgia	Legal & Contingency
Bell Engineering	Platinum Wines & Spirits	Heritage Communities
Ritz Clark & Ben-Asher	Sports Medicine and Orthopaedics	ROXU
Price & Ramey Insurance	Winholt Equipment Group	Personal Collection
bassetti-group.com	All Weather Architectural Aluminum	cameronhodes.com
We R Family Foundation	Wassa, SRO	St Peter Law Offices
Wright-Gardner Insurance	SIGN Fracture Care International	Hoyer Law Group
Clarion Safety Systems	Indian Spring Country Club	VIM Technologies
reesegroupinc.com	Grande Prairie Public Library	Chek Tan and Company, LLP
southernspecialtysupply.com	Long Island Weight Loss Institute	Shape Corp
tanyacreations.com	summitgolfbrands.com	The Catered Affair
Super Value	MC INVERSIONES INMOBILIARIAS Construction company in Peru	Public Relations Society of America
Simon Property Group	TK HOLDINGS GROUP	Sun Fiber
Truro Cannabis	Marmotech	MTI America
renrns.com	EMERSON.COM - (EBS)	D. Wilson Construction
upea.com	AA.COM - (EBS)	IFPC Worldwide
chirhochiropractic.com	WITS.AC.ZA	Right at Home Care
alissco.com	Collins Aerospace / RTX.com	Industrial Chemicals
echolakefoods.com	D Magazine Partners	Niess Agriculture

Sadler Gibb & Associates	HOEHNER RESEARCH & CONSULTING GROUP	Tibbetts Lumber
Altimedia	Madagascar Airlines	Dakota Boys and Girls Ranch
Enessance Holdings Co., Ltd	Hematology Oncology Consultants	Lashbrook
Malibu Boats Australia	Cottage	Bohlsen Restaurant Group
G & H Distributing	Shadrix & Parmer, P.C.	Desert Plastering
Bridgehead I.T	Manko Window Systems	Telstra
Yateem Group	Tenryu America	Osland Financial Group
Bestlog Logistic Solutions	Dental Society of La Plata	St Catherine of Siena
Pritchard Brown & Chillicothe Metal	GFF&F - Galine, Frye, Fitting & Frangos, LLP	Termotasajero
Federal Auto Holdings Berhad	pharmaciedesalizes.fr	JB Brown & Sons
Spijkermat	Sold Real Estate, Sold RE PTY LTD	Tecnomarket
Florida-Spectrum Environmental Services	UrbanX PTY LTD	DataStream Content Solutions
WarmBlue	One Agency Eastlakes	Chapter 13 Texas
Heimbrock	Consolidated Restaurant Operations, Inc.	Cerenade
Eligibility Tracking Calculators	Plastics Extrusion Machinery	Linxx Global Solutions
Alios Finance Group	Alitech	Lux Actuaries & Consultants
MASTEC.COM	Curtis Steel Co	Grupo Serex
Lorber, Greenfield & Polito, LLP	WEBER	Cofix Asesoría de Empresas, S.L
Gemini Group	gardeners solicitors	Acuna Fomona (AFOM)
Henry Raymond & Thompson	GEIGER	Charter Industrial Supply
Evogence	SK shieldus	LC Informatique Sàrl
Super Quik	Aussie Fluid Power	Allgäu Stern Hotel
Fast Freight	M3 Group Sp. z oo	Seguros la Cmara
Aphase II	ShareP	ebaengineering.com
Kitchen Design Concepts	Jos é Guma S.A.	rocketstores.com
Furniture Plus	BMP Worldwide	indiesemi.com
Ouranos	Coilplus	Kronospan
Sylvester Roofing	Regency Specialist Hospital	BCR Recouvrement
BK Technologies	bmcinnovation.com	California Golf Club of San Francisco
Boyer	gslong.com	JASCO Applied Sciences
fhw.org	coppage.net	auto-bernhard.at
Microbix Biosystems	arizonafireplaces.com	Massachusetts Bay Community College
NSC PLUS CO, LTD	arpis.com	J Lorber
Sangeetha Mobiles	pcdpackaging.com	Harbor Diesel & Equipment
KONCISE COMPANY LIMITED	pandarose.ca	One law firm in Canada
romar industrial company limited	montship.ca	Asahi Group Holdings, Ltd.
Bergman Dacey Goldsmith	dalton.com	archway.com
CESO	Sibbalds	Lautrec
Productive Tool Products	ronvil.com	AutohausMalin
Bellflower Unified School District	Beta Dyne	T. Choithram And Sons, LLC

Axelsson WilliamowskyBender & Fishman	Gulf Warranties LLC	Clifford Paper Inc
Riddell Law Group	Middlesex Appraisal Associates	CHRIST Juweliere
Jimfor, S.A.	Sprague & Jackson	Centers Laboratory
Advantage CDC	Docurail	kanzlei-schramm.com
Kipp & Christian	Dutch ???	AES Clean Technology
DeCeTe	Bengal Industries	Dataforth
Cohen's Fashion Optical	Rasi Laboratories	Development Services Group, Inc.
usbmemorydirect.com	Tex-Tube	landmarkmgtinc.com
sincroslab.com	Agencia Tributaria	Rogue Valley Door
visioninksltd.in	Richmond Behavioral Health Authority	Law Offices of James Scott Farrin
americanadecolchones.com	Cellucap Manufacturing	nurturercare.com/USA/192GB
francetravail.fr	Global Shop Solutions	Milliman Financial Risk Management LLC (Milliman, Inc. subsidiary)
MedImpact Healthcare	Legacy Manufacturing	Daily Printing
Navigator Business Solutions	Koch & White Heating & Cooling	Orion Engineering
Trojan Construction & Holding Group	Royal Thai	Mecklenburg County Public Schools
glawitsch-sutter	EMBASY OF BOLIVIA DC	mcgeorgeai.com
SanDiego Automotive Museum	regionalurology.com	ville-saintclaud.fr
Luis Garrat ó n	Core Resources Inc (CRI)	kecymetals.com
Double Oak Construction	Newmark Healthcare Services	Lipapromet
Engineered Profiles	East Jefferson General Hospital	Ludlow Construction
SK group, Za Za Bazaar, TH UK & Ireland Ltd and a few more.	Zierick Manufacturing Corporation	Natoli Engineering
Delтта + Unique data center	Commune De Saint Claude	naturmaelk.dk
Cavalry Consulting	LEYHAUSEN Research	Saskarc
Mainetti UK - Data breach	Centurion Family Office Services LLC	Perennial
Micke Stridh Maskin	Turnkey Africa	libertydentaltown.com
Henrietta Ezeoke Law Firm	Superior Linen Service	WELLSLANDSCAPING.COM
Izaki Group Investments	Buanderie Blanchelle	The Methodist Church of Southern Africa
Maki Building Centers	Victory Christian Center	Dnc
Domy	Bay West	SD Soluciones Digitales
MotorsportMarkt.de	Florida Marking Products	Red Hat, Inc.
ANIA KRUK	TF LE TOIT FOREZIEN	Cobra Rolamentos e Autopeças
Abilene Family Medical Associates	Wheale Law Firm	terex
Malgor	ville-elne	S&P Global (spglobal.com)
Flegenheimer International	cbsaust.org.au	CIC Vietnam
Miami Management	ChampionX	2GO Group
GeBePro	Kearney Public Schools	hillside library.org
Bolt Electricity, Oil & Gas	Navigator Business Solutions	stalkerradar.com
Meinhardt Group	Unimed do Brasil	ocmaine.com
Bayu Buana Travel	Executive Cabinetry	Rihatec.de
dwgra.com	Alu Perpignan	uhlcompany.com

partitio.com	Roger RENARD Entreprise	AIP Asset Management
Limocar by Transdev.ca	Hunter Construction Group	Standard Fiber
LaBonne	Urban Linker	Medstar Health
Metal Pros	Alqueria	Garro Fabril
Donacoop (VinaCapital)	SICE	AUSA Soluciones Logísticas
InfraCom Group	SFG Technology Sdn Bhd	Corban OneSource
South Alabama Regional Planning Commission	WebCut Converting	IONODES
Dublin Airport	Kecy Metal Technologies	Western Orthopaedics
auge.com	Volkswagen Group France	teeuwissen.com
Latona Trucking	Pro-Fab	Astra Otoparts / PT. Inti Ganda Perdana
Saturn Machine	New Jersey Property-Liability Insurance Guaranty Association	Waterborne Environmental
West Welch Reed Engineers	All Truck Transportation Co., Inc.	hameshakem.co.il
Papsud	Charles River Properties	DSA
Precision Machined Products	ICET Studios	Leprohon
Essential Cabinetry Group	Ganther Construction	LGB
Air Arabia	Canapé s Mobilier Dé coration	IKEA
Adore Children and Family Services	Prim Saveurs Import Export	Chanel
ATIRG	UT Health Austin	TransUnion
Cooperativa Esercenti Farmacia Srl	Radiant Beauty Supplies	Pandora.net
Alissa Group	Tong Yang Group	Cisco
City of Sugar Land	Club Lleuresport	Google Adsense
Zacho-Lind	Repeated Signal Solutions	Air France & KLM
Kaufman & Stigger	Catawba County Government	1-800Accountant
Omrin	HMP Global	Saks Fifth
Svenska Kraftnät	Morris-Sockle	CarMax
DAVIDYURMAN.COM	Capitol Construction Services	Qantas Airways
PANAMERICANSILVER.COM	Polar-studio	TripleA (aaa.com)
COXENTERPRISES.COM	H. Gascon	Adidas
HRSD.COM	Sistema Odontológico Privado	Cartier
MetroWest Community FCU	American Journal of Managed Care	Puma
constructiondprovost.com	EURORDIS	Petco
xortec.de	PQCNC Hospitals	Instacart
mino-in.co.jp	Paris Ré tina Vision	HBO Max
bannenbergandrowell.com	Buldi	Kering (Gucci, Balenciaga, Brioni, AlexMcQ)
greenhouseapt.com	City of Riviera Beach, Florida	Engie Resources (Plymouth)
hanson-inc.com	Gittens Healthcare	Albertsons (Jewel Osco, etc)
Hall Estill	Trans-World Shipping Service	Instructure.com – Canvas
Le MULTI LABORATOIRE LC2A	Addis	Fujifilm
Doha British School	Ditransa	HMH (hmhco.com)
Summit Hotel Properties	LaRosa's	GAP, INC.

Essilor of America	Typology	ASICS
Peruvian Connection	Ostrolenk Faber	KFC
simmerscrane.com	Art Guild	McDonalds
Danthi Comunicacao Integrada	baronespecialtysteel.com	Stellantis
ClearCare Periodontal & Implant Centre	DV Hardwoods	Walgreens
Adichunchanagiri Institute Of Technology	The Law Offices of Michael C George	Vietnam Airlines
Gericke AG	Atarfil	Marriott
IREM companies	Greenstar Social Marketing	Home Depot
OCI International Holdings	DuVal & Associates	Aeroméxico
Kurogane Kasei Co.	Pratt Homes	UPS
UniCursos, Brazil	Force Marketing	Republic Services
S Food Co., Ltd.	Plast-O-Matic Valves	Disney/Hulu
ozsoft.com.au	Blood Bank Computer Systems	FedEx
iCare Software	Autorotor	Toyota Motor Corporations
Vanan Online Services	M&E Global Group	Capital Reinforcing LTD
FOOD & MUSIC MANAGEMENT SL	Speed Inter Transport	Saint Mary's Home
Al Rimal Group	Miguel Veiga, Neiva Santos e Associados.	Sobotec
STAR LÉGUMES	Schedler-translog	Milburn
Qatargas and Tar Company, Iran	Business Integra	Field and Goldberg
Goodfellow & Schuettlaw	Karnes Electric Cooperative	Banco Hipotecario del Uruguay
Paterson & Dowding Family Lawyers	Bank3	Supercash (Alimentos Y Bebidas Premium)
SE.COM (EBS)	mercantetubos.com.br	stockmeier-urethanes.com
CSCGLOBAL.COM	San Bernard Electric Cooperative	GWP Engineering
AUSENCO.COM	BHI Co., Ltd.	TriMed Inc. (Henry Schein)
LKQCORP.COM	SourceOne Corporation	sagchip.org
The Laxmi Niwas Palace	Fountains Condominium Operations	Mitchell Industries
Real Estate Specialists	Indaco Warna Dunia	suratisweetmart.com
Samera Health	hautsdefrance.fr	Xebec Building
CHDFS	Furuno Electric	Shamir Medical Center
NurseSpring	Undefasa	wilsenergy.com/USA/77.1GB
Integral Networks	LA VOIE EXPRESS	Weber Flavors
Signet Armorlite, Inc.	Design To Print	Dual Temp
Grupo Promasa	EcoPetróleo	Displayit
KHL Printing	Cemtrex	Apricorn
ACTi.com	North Stonington Elementary School	Gesimde Asociados / Ausil Systems / Esnova
Magna Hospitality Group	espectral.pt	Spectrum Painting
More Than Gourmet	michigancityin.gov	Prince William Ice Center
United Lube Oil	PLC-Transportation	American Association on Health and

		Disability
KIS Asset Evaluation	dsv.com	Judson Center
AT&T Careers	Kuehne + Nagel	Karat by Lollicup
Applied Technology Resources	Altas Temizlik	Immaculate Heart of Mary
Northern Light Technologies	Borrowell.com	Johnson Regional Medical Center
MILGARD.COM	Legal Boutique	AT Solution
COPELAND.COM	Canias ERP	Lugand Aciers
PT Pupuk Iskandar Muda	Carewell	Integrity Wealth Consulting
Kumwell	Dynamic Precision Sverige	LASER AUTOMOTIVE VALENCIA SL
Tri City Foods	Frisquet	suntreeinternalmedicine.com
SANHUA INTERNATIONAL	IDB Clinicas	Watsonville Community Hospital
Nelligan White Architects	CMF	Mitrani Rynor Adamsky & Toland
National Coatings	Sunbelt Design & Development	The Green Labs
Prime Dental	Valtorta	Calsoft Systems
Crave Management	HARVARD.EDU	White Birch Paper
Peraso	Ministerio de Salud de la Nación argentina	profimetrics.com
Pacific West SystemsSupply	Team Schierl Companies	Barr and Barr
Microdevice	Balfour Beatty	The Plainview Volunteer FD
marquscompanies.com	Kido Schools	Dimensional Control Systems (3dcs.com)
Southern Specialty and Supply	Magna Foodservice	adhunikpower.com
Roth & Scholl	Minnesota Hospital	Keystone Solutions Group
River City Eye	Retail Texas	Climatron
Austin Capital Trust	UK Rail Services	miraense.com
Healthy Living Market and Café	Taldor	DRL Group
Claimlinx	Streebo	callhci.com
Ronemus & Vilensky	Integlia	icc-nw.net
Dependable Plastic	Citizens' Committee for Children of New York	Cholakyan Chiropractic
I-Tek Medical Technologies	Adore UAE	LAMMCO.NET
U.S. Vanadium Holding Company LLC	EPS FUJ Private School UAE	Smiles By Steedman
Mailing.com	Mandom Corporation	idealbathrooms.ie
Nvno	Maine Oxy	Nacsworld.com
trailridgeenergy	Express Logistics and Distribution Ltd	

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。

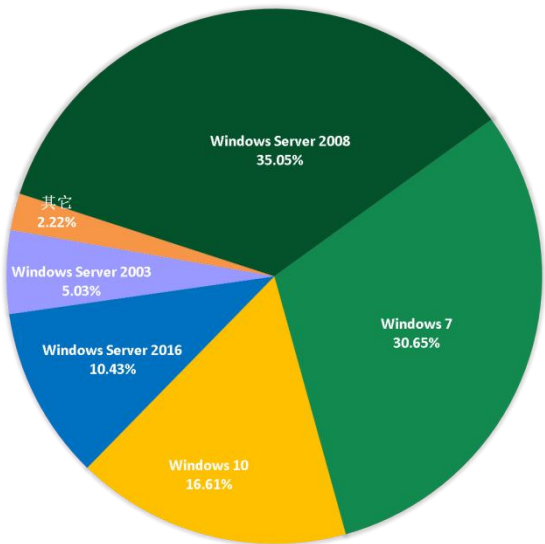


图 5 2025 年 10 月受攻击系统占比

对 2025 年 10 月被攻击系统所属地域统计发现，与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受攻击的主要对象。

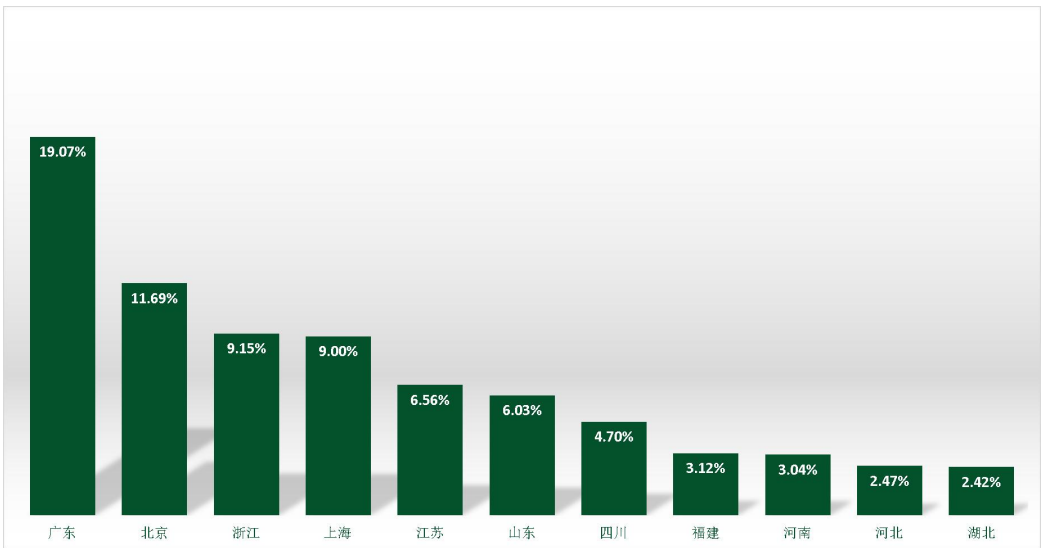


图 6. 2025 年 10 月国内受攻击地区占比排名

通过观察 2025 年 10 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。

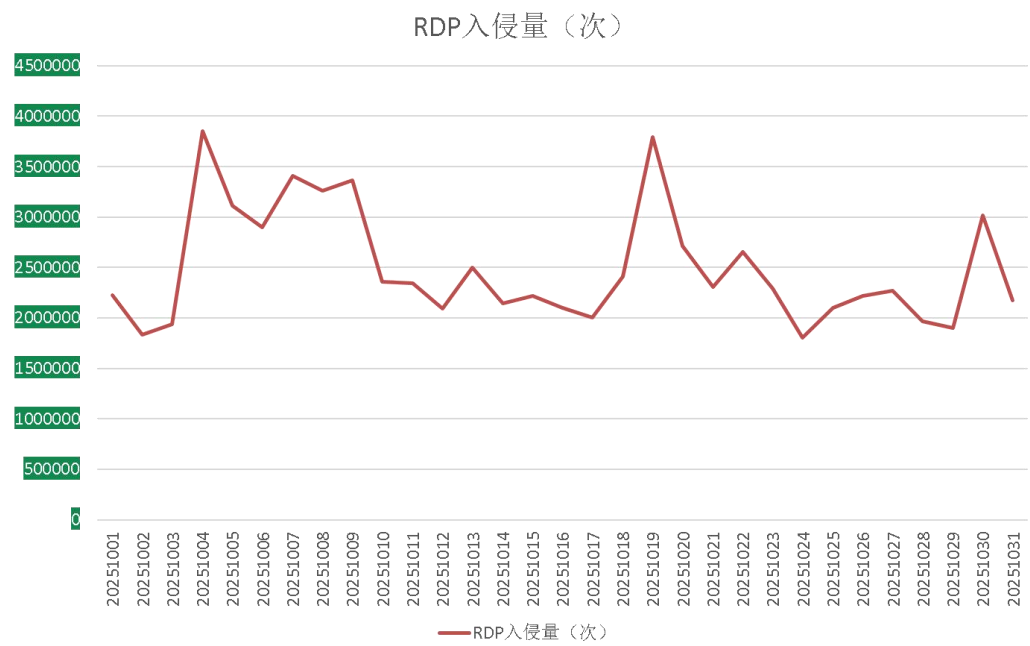


图 7. 2025 年 10 月监控到的 RDP 入侵量

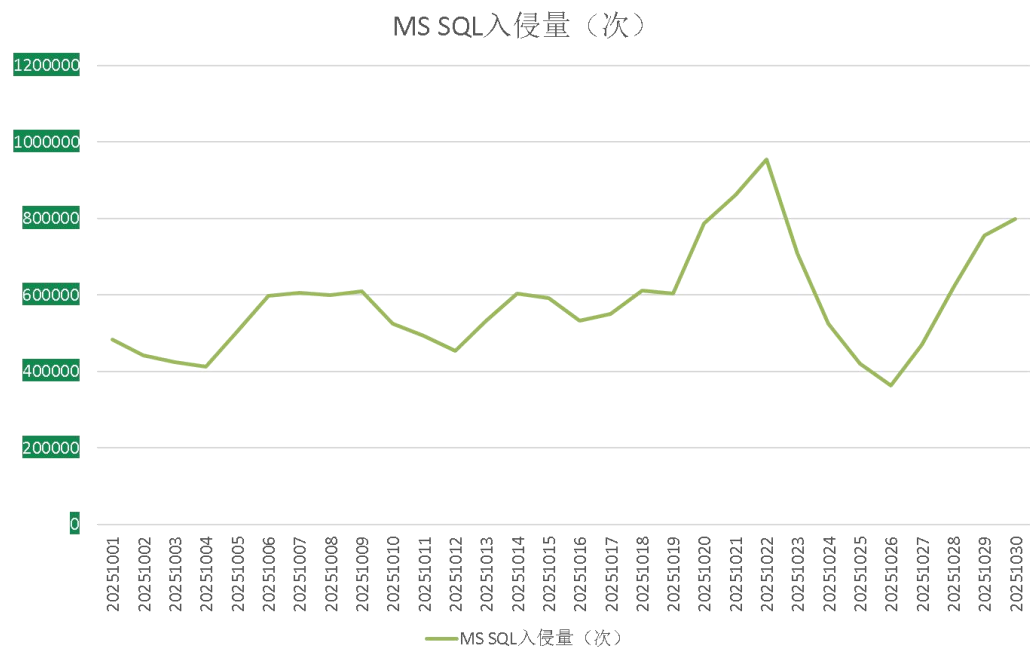


图 8. 2025 年 10 月监控到的 MS SQL 入侵量

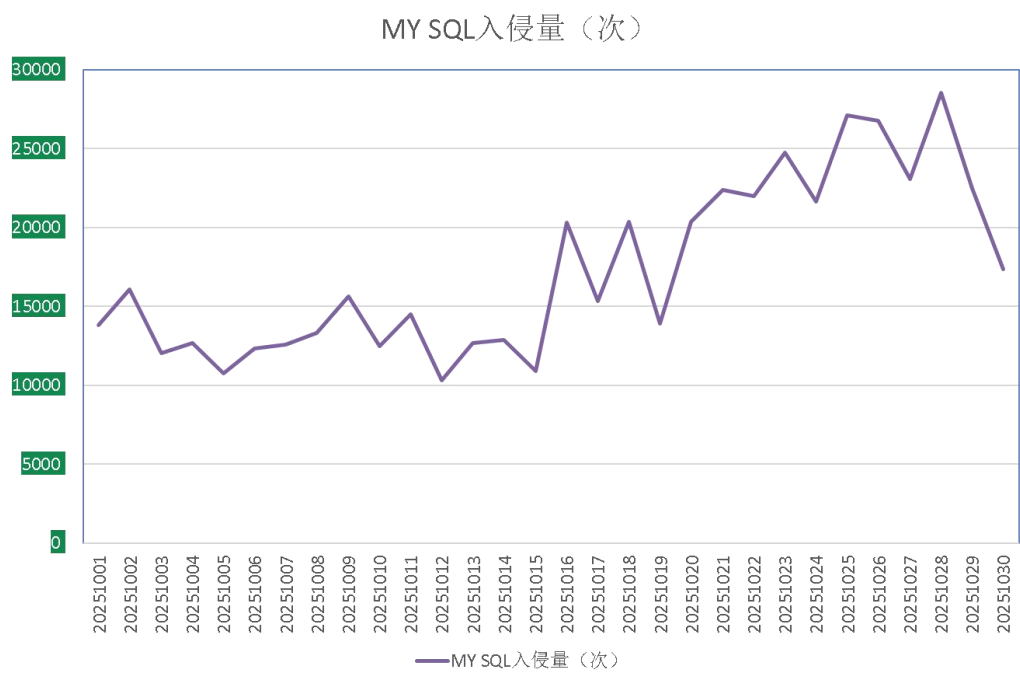


图 9. 2025 年 10 月监控到的 MYSQL 入侵量

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。

- ✧ wax: 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。
- ✧ weax: 同 wax。
- ✧ roxaew: 同 wax。
- ✧ 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与数据库口令，成功后手动投毒。
- ✧ peng: 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。
- ✧ bixi: 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。
- ✧ spmodvf: 目前此扩展名反馈的用户均未提供溯源信息，暂未研判家族归属与攻击方式。
- ✧ 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。

- ✧ **beast**: 属于 Beast 勒索软件家族, 该家族的传播方式多样, 具备暴力破解、漏洞利用、共享加密等多种攻击方式, 同时具备跨平台加密能力。
- ✧ **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。

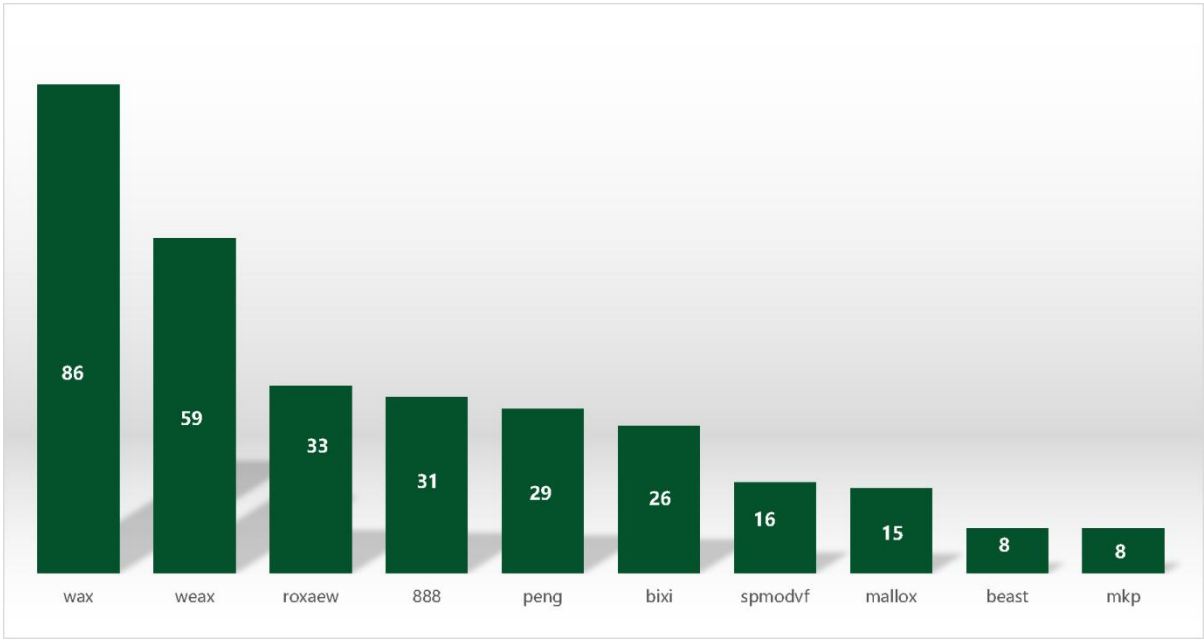


图 10 2025 年 10 月反病毒搜索引擎关键词搜索排名

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 Crysis。使用解密大师解密文件的用户数量最多的是被 Crysis 家族加密的设备。

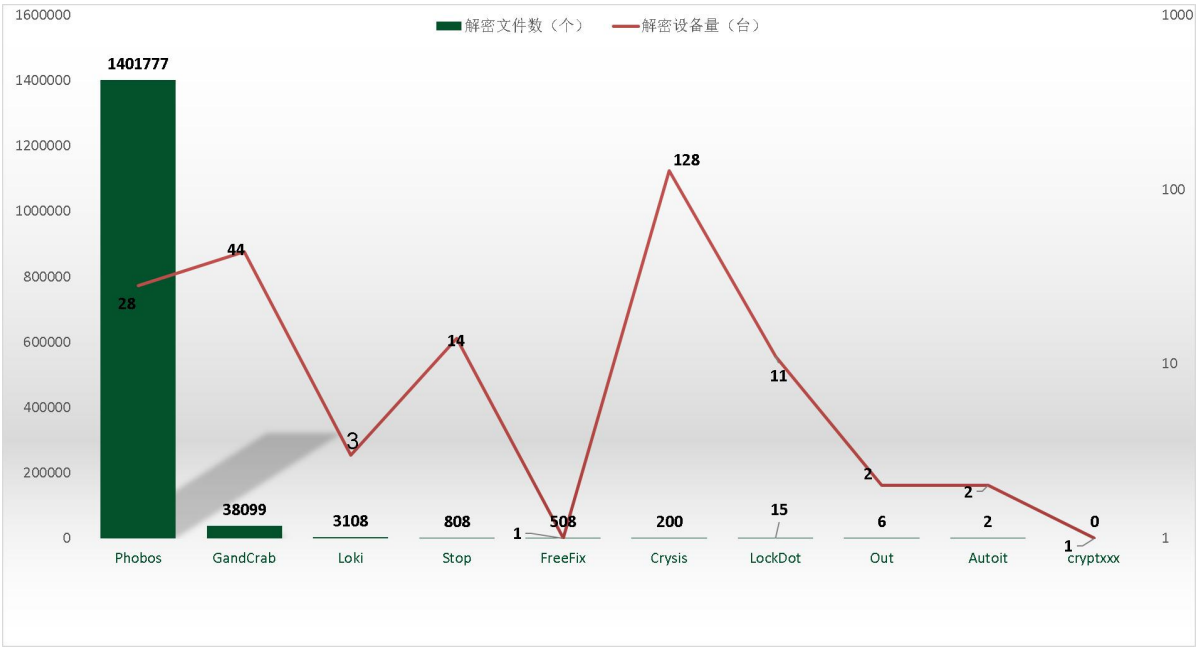


图 11. 2025 年 10 月解密大师解密文件数及设备数排名