2026 年 10 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，数百万到近亿美元的勒索案件持续出现。勒索软件对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。

2026 年 10 月，全球新增的双重勒索软件有 UmBra、BYOD、0x00、Mimori、Whitearmor 等家族，传统勒索软件家族新增 Hexsomeware、Prizrak、OneCryptor、CoffinLocker 等家族。

本月 Weaxor 家族继续凭借大量 erp 类软件漏洞利用霸榜勒索软件第一位。其中某普 erp 软件的 SQL 注入漏洞利用在 10 月 23 日集中攻击了一波 Windows 服务器，而 AJ-REPORT 大屏系统的“命令执行漏洞”被用于 Weaxor 家族 Linux 的.weax 变种的传播。

本月 Redpipe 家族集中攻击 24 家中国企业，连同 9 月被袭的韩国企业，共 4 家支付赎金。360 掌握的一例反馈显示，攻击平台为勒索攻击常见靶点 ESXi，存在多个流行漏洞可利用。

以下是本月值得关注的部分热点：

① 双群晖 NAS 勒索软件来袭

② 勒索恢复公司 MonsterCloud 因赎金中介行为被起诉

③ 美国哥伦比亚市遭勒索攻击致多项政务服务瘫痪近一周

基于对 360 反勒索服务数据的分析研判，360 数字安全科技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设备数量占比达到 63.25%，安装 360 安全软件但未正常启用的占比 18.61%，安装了其他安全软件的则占比 18.14%。

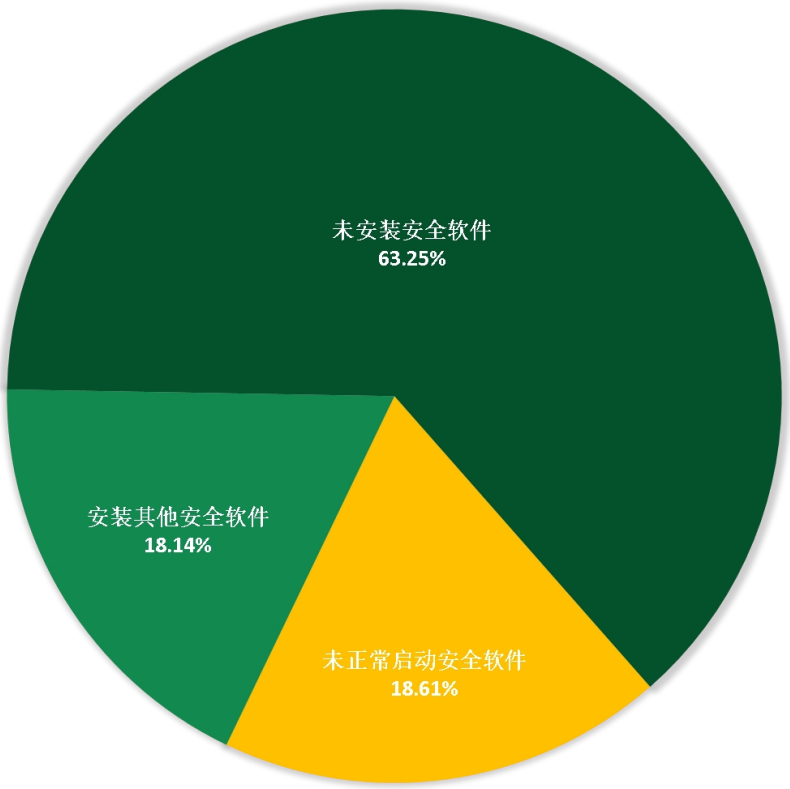


图 1. 2026 年 10 月勒索软件中招设备中安装的安全软件占比

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 57.26%居首位，第二的是 Cerber，占比 13.68%；BrzCrypt 家族以 11.97%占比位居第三。

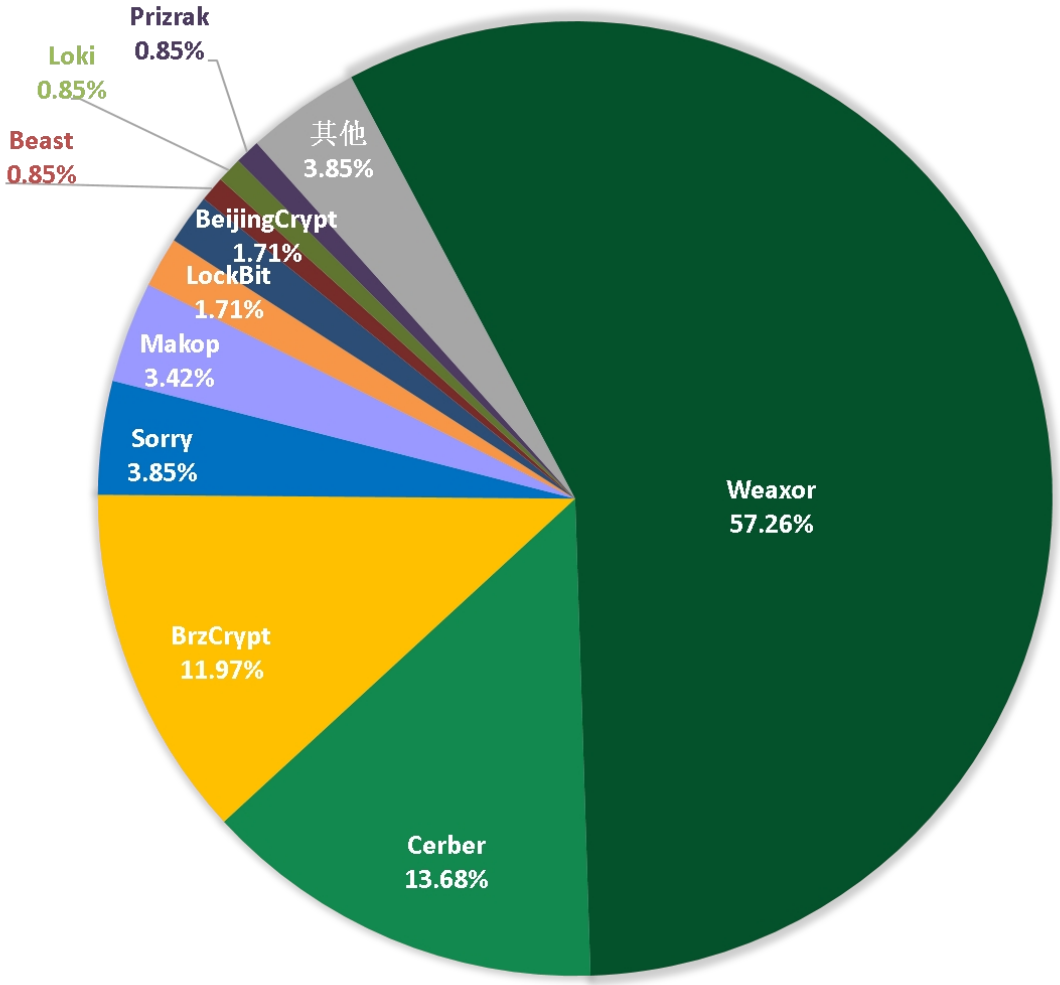


图 2. 2026 年 10 月勒索软件家族占比

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 2016、Windows Server 2012。

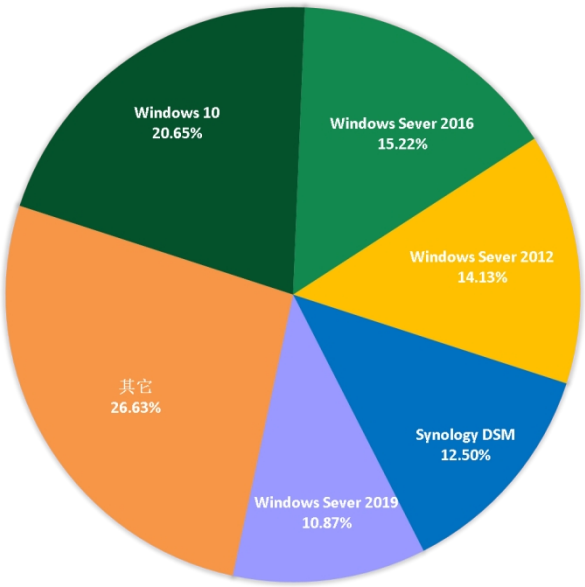


图 3. 2026 年 10 月勒索软件入侵操作系统占比

2026 年 10 月被感染的系统占比显示，受攻击的系统类型服务器大幅领先桌面 PC。

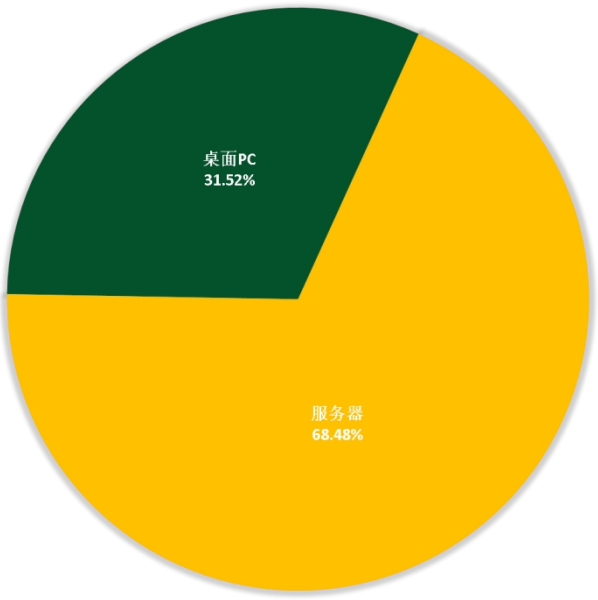


图 4. 2026 年 10 月勒索软件入侵操作系统类型占比

勒索软件热点事件

双群晖 NAS 勒索软件来袭

本月两个针对 NAS 的勒索家族同时活跃，其中 Cerber 家族对群晖 NAS 的勒索案例最早出现在 10 月 24 日，并在 10 月 28 日集中爆发。

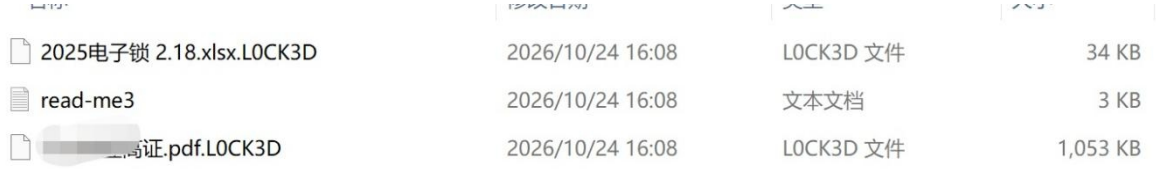


图 5. 2026 年 10 月 24 日 Cerber 家族群晖 NAS 的受害案例

另外一个老牌 NAS 勒索家族 eCh0raix 也在 10 月 28 日起针对群晖 NAS 发起攻击，但被 Cerber 的大面积漏洞利用攻击抢了风头。eCh0raix 勒索家族最早出现在 360 的 2019 年度勒索态势报告中，攻击覆盖多个 NAS 厂商的硬件产品，且在随后每年都有传播案例。

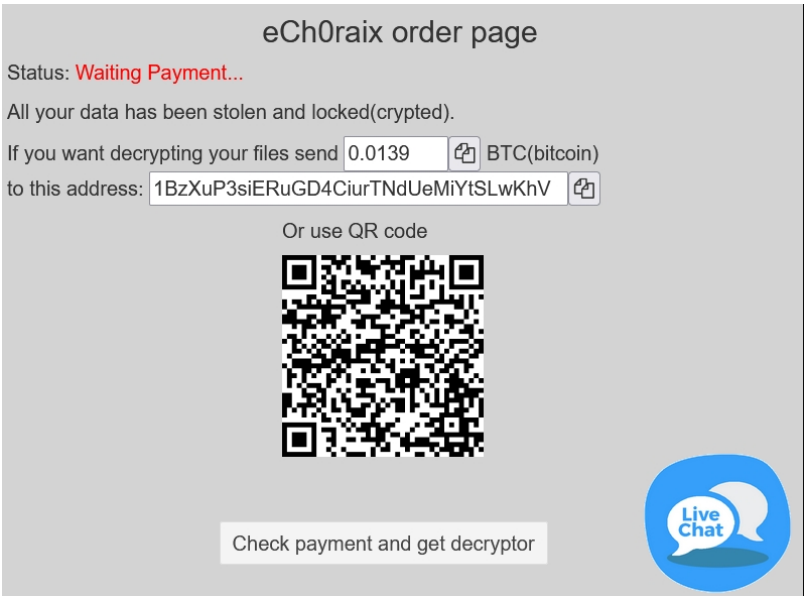


图 6. eCh0raix 家族本轮攻击的联系页面与钱包地址

其中，本轮 Cerber 家族 NAS 版的加密器样本分析报告参见如下链接：

https://360.cn/n/13055.html

两个勒索家族在本月同时流行，再次暴露了 NAS 平台的维护不当的问题：管理端口常暴露公网、用户缺乏安全知识使用弱口令、数据缺乏有效备份等问题凸显。因为 NAS 设备全天在线且存放有个人重要数据，建议一般用户收窄攻击面、不要直接将设备暴露在公网上，多数 NAS 厂商都提供转发代理服务，使用这类服务，可极大降低 NAS 被攻击风险。另外，在日常维护中，关注官方发布的安全补丁，尽快将系统升级到最新版本。一旦发现勒索加密行为，可联系 360 反勒索团队进行溯源分析与加密器算法层面的解密可行性评估。

勒索恢复公司 MonsterCloud 因赎金中介行为被起诉

2026 年 10 月 8 日，美国司法部纽约东区联邦检察官办公室通报：佛罗里达州勒索软件应急恢复公司 MonsterCloud 老板佐哈尔·平哈西（Zohar Pinhasi，50 岁，美以双国籍，化名“Zack Silver”“Zack Green”）因电信诈骗及合谋实施电信诈骗罪被起诉，已在纽约布鲁克林联邦法院首次出庭。

起诉书指控：该公司长期宣称，凭“专有工具”和“先进解密技

术”即可恢复被加密数据，无需向攻击者妥协，并警示客户自行支付赎金的风险。实际上，平哈西毫无解密能力，而是背着客户联系勒索团伙、付费换取密钥，再以远高于赎金的“恢复服务费”向客户收款。截至 2023 年的五年间，他向客户收费超 1900 万美元，暗付赎金超 800 万美元；为掩盖真相，他要求员工只称“恢复工具”、不说“解密器”，严禁透露已付赎金。

赎金中介们的骗局如何运作？

通过广告投流与其他技术手段进行互联网引流获客，并先以 2500 美元的“分析”服务设饵：取走两个被锁样本，交回解开版本充作“恢复证明”——多数时候样本被直接发给黑客破解（勒索团伙本有免费解一两个文件以证明持钥的惯例）。客户见数据确实能解开，便签下数万至十几万美元的“完整恢复”合同。合同另埋伏笔：写明“所有直接解密手段用尽后”才会联系攻击者，而检方指出，这正是他的第一步。对外背书来自 FBI 前副局长约翰·皮斯托尔（John Pistole），此人曾是该公司的网络安全顾问委员会成员，连宣传视频台词都出自他手，而后来他则承认早知该公司多数时候其实就是在付赎金。

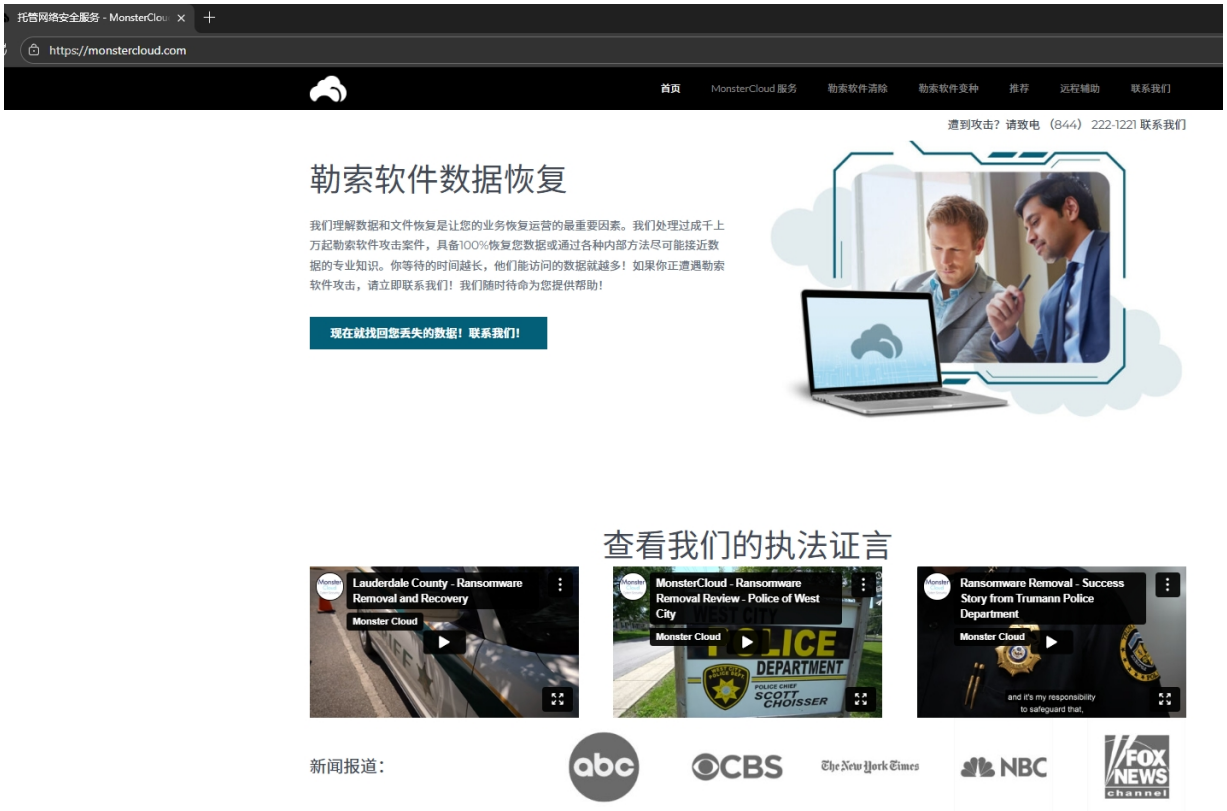


图 7. MonsterCloud 官网的部分用于引流的电诈套路化描述

早在 2019 年，ProPublica 记者勒内·达德利（Renee Dudley）就在《商业秘密》中介绍过该公司的行为：阿肯色州杜鲁曼镇警局的案卷、笔录、工资记录被整体锁死，警长哈德·汉森（Had Henson）看中其“对执法友好、不付赎金”的特点，结果 72 小时恢复完毕，还以免收 7.5 万美元服务费换得一封推荐信。但两位安全研究员当时即指出：该款勒索软件彼时无任何已知解法，公司只能付钱。报道之后，这门生意又做了四年，才等来起诉书。

本案暴露出勒索事件响应市场的信任黑洞：受害企业在慌乱中求助第三方“恢复专家”，反遭二次伤害。检方用“再受害化”一词点明危害——既虚增受害企业成本，又喂养勒索犯罪经济、推高整体赎金

水平。防御方应得两点启示：其一，选择事件响应与谈判服务商时须核验资质与服务措施透明度，对“百分百恢复、绝不付赎金”类承诺保持警惕，要求书面说明恢复手段并接受审计；其二，建立事前能力——离线备份、恢复演练、法务与保险联动预案——减少对不可控第三方的依赖。此外，支付赎金可能涉及制裁合规（向受制裁主体付款可能违法），应将网络安全律师纳入决策链条，避免“病急乱投医”引发合规与财务双重风险。

美国哥伦比亚市遭勒索攻击致多项政务服务瘫痪近一周

2026 年 10 月 20 日，美国南卡罗来纳州首府哥伦比亚市的 IT 部门在网络中发现可疑活动，随即请求州执法部门（SLED）介入调查。10 月 23 日，市经理 Teresa Wilson 通过视频声明正式确认该市为勒索软件攻击受害者，攻击影响了多项面向公众的服务，并涉及市政网络内的敏感数据。为了应对攻击，市政部门主动下线了部分应用系统，导致 MyColaSC 在线举报平台、商业许可、公园与娱乐、规划与发展服务、地理信息系统（GIS）、动物服务等非紧急在线服务持续不可用，居民需改用电话热线办理相关业务。截至 10 月 26 日，部分服务仍未恢复，GIS 地图等系统显示“暂时不可用”。市政府强调警察、消防、911 应急通信、自来水系统与缴费中心等关键公共服务始终在线运行，各部门已启动替代流程保障服务供给，并与第三方网络安全专业人士制定处置方案。SLED 表示调查仍在进行，后续可能联合 FBI 及其他州和联

邦合作伙伴确定攻击来源、范围及影响严重程度。目前暂无勒索组织宣称对攻击负责，数据是否被实际窃取仍在评估中。

首府城市整体网络遭勒索加密，是勒索威胁向地方政府治理中枢渗透的又一实证。事件处置呈现两点典型特征：一是“主动下线+替代流程”的应急范式——通过电话热线等传统渠道兜底非紧急服务，同时确保应急与市政核心系统不受波及，为同类城市提供了可参照的降级运行样本；二是敏感数据面临泄露的不确定性将长期存在，攻击涉及“网络内敏感数据”的官方表述，意味着后续可能触发大规模个人信息泄露通知义务。建议地方政府机构：一是对政务服务系统按业务关键性分级，明确勒索事件中“必须在线、可降级、可下线”的系统清单，并为每类服务预置离线办理预案；二是建立与上级执法部门和联邦机构的快速协同通道，缩短取证与溯源周期；三是定期开展全员安全意识培训与钓鱼演练，重点防范针对市政员工的初始入侵；四是对身份体系与远程访问入口强制启用多因素认证，限制攻击者获取初始立足点后的横向移动空间；五是提前制定数据泄露通知与公众沟通预案，避免事件发酵期的信息真空引发信任危机。

黑客信息披露

本月收集到的黑客邮箱信息如下

supportx@privatemail.com	FunhouseRaaS@proton.Me	diskstation@atomicmail.io
MainpartVI@tutamail.com	Funhouse8764@tutamail.Com	hashhead@tuta.io
MainpartVI@mail2tor.cc	bytebane@lockbit.io	hashhead@mailum.com
WeAreZynex@tutamail.com	shadow533night@outlook.com	coffin.locker@onionmail.org
Getyourdata@onionmail.org	universejohn@tutamail.com	onecryptor@onionmail.org
DOKADOKA@ONIONMAIL.COM	witold@tutanota.de	UseNarealNran@firemail.de
kittentor@proton.me		

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）。

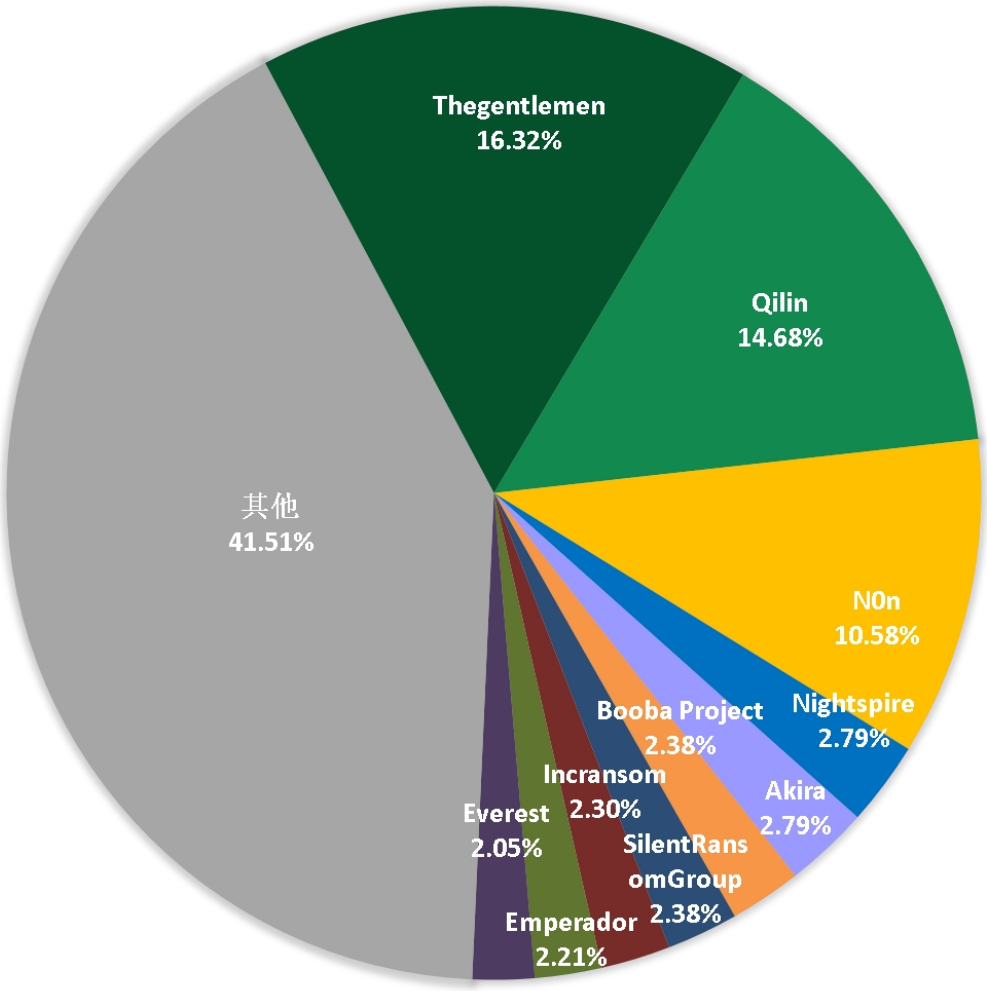


图 8. 2026 年 10 月通过数据泄露获利的勒索软件家族占比

以下是本月被双重勒索软件家族攻击的企业或个人。未发现数据泄漏的企业或个人也请第一时间自查，做好数据已被泄漏准备，采取防范措施。

本月总共有 1187 个组织/企业遭遇双重勒索/多重勒索攻击，其中

包含中国 50 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 109 个组织/企业未被标明，因此不在以下表格中。

System Soft	ADL Lift Services Limited	MGNP
JHAMF Group	Zena Office	Portonave
Punta Shopping	Bi-silque	Polaris Shipping
Community Medical Center, Falls City Nebraska	Line2Line Coatings	ZPMC
Straze Garden Center	Fresh Farms	Tsuneishi / Kambara Kisen
Kraft Lernen	EMARKETER	Yusen Logistics Hong Kong
SALEG	Coop Italia	Premier Alliance
Phoenix Charter Academy	Horn of Africa Regional Environment Centre and Network	CULines
Cabka	Prism Medical Products	BNCT Busan New Container Terminal
Ivan Smith Furniture	PROTEX Confection	T.S. Lines
Holcim	SunTechnics Fabrisolar AG	HPC Hamburg Port Consulting
quevedo-ponce.com	B2Chat	Apical Group
mars-semi.com.tw	SEPIVER	Superterminais
Rood Trucking	United Restaurant Supply	NEOM Ports
grifosespinoza.com	Airtificial	GCS Kuwait
jumonji-u.ac.jp	AMSAM	GNCNet / DGT Busan
everon.com.ar	Barrow & Grimm	Samudera
goldencrops.com.tw	Kirkland & Ellis LLP	Dongkuk Steel
layam.com	Bethany Press International	NCT Kandla
uaa.mx	Medienwerkstatt	TTI Algeciras
Digital Triumph	Annapath	Saehan Marine
atljamaica.com	DR.SCHNELL GmbH & Co. KGaA	April Asia
flynn-construction.com	Bathurst RSL	Dong-A Tanker
smithandcasady.com	Creative Universe	EUSU Logistics
nelsenarchitects.com	istanbultrading.com	BMT IQ
spencers.com	PWC	BKH ICD

chicagolawyer.com	Performance Ford Inc	Korea Ferry
ArentFox Schiff	SGLA	T2S
Studio Stelitano e Associati	Hecker Holzsystembau	Samjoo Maritime
Acclaim Companies / JCJ Investment	Linebarger Goggan Blair & Sampson	Camellia Line
Gilliam & Associates, P.C	bereskinparr.com smartbiggar.ca	Eurogate Tanger
Facts N Figures	Gräfliches Hofbrauhaus Freising	ILCS Pelindo
Illinois Work Injury Resource Center	VERGI Muenster	Pusan Newport Company
Psychometrics Canada	Heritage Senior Living	Nam Dinh Vu Port
Louisiana Crane & Construction	FuG-Gruppe	Cognosis Limited
Aliqout Association	MECA-PRECIS	Canadian Mennonite University
EAS Engineering	WEPOS Chemie	Placer AI
Fred H Beck & Associates	novagroupgbc.com	BigID
KTU Shipyard	oflaherty-law.com	Confluent
Moritt Hock & Hamroff LLP	clinicaromero.com	MoneyGram
TRAUCO AG	sodali.com	KFC
Honghwa International	srsnodgrass.com	Eversource Energy
Suburban Orthopaedics	prosomnus.com	MGT Lojistik AŞ
Cipsa Industrias Sa De Cv	olyortho.com	KP Industries
Richland Resources Corporation	mvjllp.com	Spelman Logistics
Sistemas Visuales 360	Allmand-Smith Limited	huntcompanies.com
Societe Ivoirienne De Telediffusion	Hanjin Information Systems & Telecommunication Co., Ltd.	Reed & Giordano PA
Palletline	Coastal Alabama Community College	CNESTEN
FrenchCreek Production	Porter Hedges LLP	Friendship Christian School
Rapid Manufacturing	Westrock Coffee	Charles E. Tabor AAL LLC
Phillips Nizer	Flextron Circuit Assembly	Confipetrol
Farmacia I	Cascade Flooring America	TQC S.A.
Grupo Ciosa, SAPI de CV	Hypertherm	hsc.mb.ca
Innoe Asesores	PLD Group	HYSYTECH S.r.l.
iFink	Lindauer Dornier	TEXMA International Co., Ltd

Light Rail Manila	Lanham Associates	Royal Thai Air Force
Hudson & Hudson Sign Products	Adobe Insurance Brokers, LLC	Helwan University
Service One Transportation	gabonmeca.com leak incident	DexCom
CP Manufacturing, Inc.	dangvuongcac	poolegroup.com.au
NOVADATA	LEGAL-RECORDS.US	saintpierredescorps.fr
CommTank	TheHomeMag NorCal	ACI Proyectos SAS
Ined	police.rajasthan.gov.in	Secretaría de Modernización e Innovación del Municipio
Five Star Jewelers	genesys.com	KOIKE Sanso Kogoyo Co. Ltd.
lyserp.com	nbcuniversal.com	Gress Clark Young & Schoepper
INTI International University & Colleges	Xylanpicks	Glenhardie Country Club
Minutes Quick Services	GSE-M Technology Sdn. Bhd.	LD Constructora
Susman Godfrey LLP	Bruin Group LLC	Saber1
TDS Telecommunications LLC.	Graves Fireplaces, Inc.	idi pharma
IT Foods Industries	centralrogers.com	hoteldelfinolugano.ch
Friendly Senior Living	Beach Eye Medical Group	dwi-bau.de
Morgan White Group	Asensus Surgical	astranahealth.com
Antwerp House Dentistry	The Excalibur Group	Supreme Energy
corp-smart.com	Duarte Nursery, Inc.	solutend
rolly.io	51Ridge	northshoresun.timesreview.com
LA PROFUMERIA SRL	Research Foundation of The City University of New York	Vadeto Group
sunnybrook.ca	Chicago Vein Institute	Anne Arundel County
au.bank.in	Pearland Pediatrics	fleetworksinc.com
Udima	City of Mt. Angel, Oregon	DW McMillan Memorial Hospital
W Interactive	City Hall - Everett, MA	Saskatoon Tribal Council
Proterial	OpenText	Aquatech
City of Columbia, SC	Aveva	AnyTech365
INTAX, Inc.	COASTAL CAROLINA NEUROPSYCHIATRIC CENTER, PA	Greenbrook Engineering
www.viehhauser-kfz.at	Fisher59	TGN

LifeFone	BW Office World	Galil Engineering
National Association of Credit Management	Brüninghoff Group	Smart Value
California School Boards Association	Toyota Canarias	Kooltronic
South Weber City	GardaWorld	Skyplan Services
Programs for Parents, Inc.	Rosenberg & Pittinsky	Refako Autodele
Circleville Police Department	chooseultimate.com	SAS H2O MICHEL
Terrebonne Parish Government	Baker Donelson	Husky Ltee
MAA Group Consulting Engineers	Vormittag Associates Inc	Asessippi Ski Resort
ClaimTek Systems	Seminole Schools	PIR Sales
Santiam Hospital & Clinics	Froggys Fog	Jentech Precision Industrial
Lowenstein Sandler LLP	Seetelhotels.de	Santee School District Foundation
susannecerda.com	Walbro	University of Buraimi
xspringcapital.com	WalkingTree Technologies	Ansonia Public Schools
Cyrious Software	SkyWorld Air Cargo	All Souls St Gabriels School
Fortrex	Johnson & Pace	Rag Electric
Morrison Foerster	Dental Team FL	Maverick Desk
A&B Lab	Grupo Cronica	Polishing Proz
The Anglican International School	Salauno	Northwestern Polytechnic
PQE Group	CREDIN	Machine sro
Noelker and Hull	PingCAP / TiDB Cloud	Ability Enterprise
Hauhinco	Latham & Watkins	Alcoholics Anonymous
Marbre Design	Hotel DuPont	Tepcomp
Insurance Services	Kingwood Endoscopy	Mabris
Trulife	The Akeeli Group	Potomac Animal Hospital
Roberts Consulting Services	GTL Concreto e Logística LTDA	The Law Office of James R Walsh
EWM Group	POWERsonic Industries Inc.	All Smiles Dental of Falls Church
Femern Link Contractors	Baltimore Tank Lines	Majestic Holidays India Private Limited
GIO Dental	Merit Financial Group	Habbas Associates
Broadstreet HEOR	Patriot Maritime	Palma

Meleghy Automotive & Cie. GmbH	American Campus	MercyMed of Columbus
SK Capital Partners	Finzly Corp	North Philadelphia Health System
Cherry Bekaert	Amagi Media Labs	Deloitte
Angeles Contractor	Belcorp	Merrill Iron & Steel
Svedala Kommun	Telecom Egypt	Watermark Retirement Communities
First Dental	All Business Technologies	bayer
Echo.com	SMIC US Company	enTouch
Ryder	International Corpo	lopay
Machelen	Llano Independent School District	Shalom Christian Academy
Bi Link	mckenneys	Mynd
TWICE SRL	BRUTRA Logistek	Imperial Diamond Jewellery
Tailormade Logistics	Pengurusan Aset Air Berhad	Melchioni Spa
Coast 2 Coast	Pergande	Yarema
VPC Builders	Mastelli S.r.l.	AETHOS
Hygiena	Southwire	mblllp
Money Concepts Capital	www.marvinpac.com	Ladrillera Mecanizada
MicroSearch	passavant-ee.com	iDentalSoft
QLC	acclaimcompanies.com	Dudley Land Company
wagyu.xyz	binsky.com	Design Electric
GRUPO PETROIL	konsis.no	TigerPress
Kerckstede vzw	monroeroadways.com	RealManage
BASS Medical Group	adapt-global.com	Anaergia | World-Leading Anaerobic Digestion Solutions
Hudson River Museum	exo.inc	Hagiva Yh
Horizon Eye Specialists & LASIK Center	Luzco Ilumination	Fondy Food Pantry
Aesthetic Specialty Centre	Quikrete	The Bernard Osher Foundation
City of Big Spring	Solid Trading B.V.	PMG Project Management Group
KING FAMILY MEDICAL	ECO USA	Ministarstvo poljoprivrede, šumarstva i ribarstva
Charter Township of Commerce	SQA Services Inc	Mäntelhaus Kaiser GmbH & Co. KG
Regent Christian Online Academy	Personify Health	INAPI

GreenbergFarrow	Bay Alarm	Medcom Tech Information
Bristol City Council	Smith Douglas Homes	WAGA Enterprises Architects LLC
Hawaii Law Enforcement Fedral Credit Union	PART2 Global AirFreight International	Heidi's Events & Catering, Inc.
NuVista Federal Credit Union	oakgrovetech	Sangre de Cristo Arts and Conference Center
FPT Software	First Brothers Co., Ltd	Vietnam SuperPort
Eichstatt	polisee Inc	Valvorobica Industirale S.p.A
OR Technology	Rheem Global	KC Pharmaceuticals, Inc
Burris & MacOmber	Asia Market Ltd	MCM Telecom
Energy Storage Terminal in Singapore	Wellington College International School Bangkok	O'Hagan Meyer
Point Robotics	Gio Dental Med Spa	Mid Atlantic Gynecologic Oncology and Pelvic Surgery Associates
Natuzzi	First Dental Health	SOCOCO
TECNA ICE	AirQ	dipecarr.com.br
MediSolution	Kissei Shoji	Baker McKenzie
SleepEx LabRetriever	Chugoku Bend	Manipal Academy of Higher Edu
Antah HealthCare Group	Taekwang Network	IIT Roorkee
DATEM, Inc.	Brenner Base Tunnel	FSE, Cairo University
Verification	Prafesta Ind. e Com. de Embalagens Ltda	Boullard Musique
probe-011637cabbf94076-	WSBI-ESBG	simplexengg.in
Zhito Technology	New Tec Tool Limited	sanjoseattorneys.com
Regency Park Oak Knoll	MicroSearch Corporation	DIPECARR
Morrison Cohen	Pure Options	Global AirFreight International
Afflelou	ock.com.my	Morton LTC Pharmacy
University of New Mexico	ONEOK, Inc.	Cooperative Des Techniciens Ambulanciers De La Monte
MISC Group	Data-Core Systems	TheraCare
Ingelectus Innovative Electrical Solutions S.L.	Girl Scouts of Eastern Massachusetts	yalebooks.yale.edu
ImmoVia Hausverwaltung	Parker-Hannifin Corporation	Asociación de Escribanos del Uruguay

Gamdom	Xinos Construction Corp and its accounting group	Sociedad Portuaria Mardique S.A.
Beasley Allen Law Firm	BladeTech Inc	Sinae Phuket Luxury Hotel
Mercantile Investment Corporation Bolivia S A	EnVision Eye Care	INI Fiocruz
SuperScale	Macfarlan Capital Partners	Lumabuilt
Rexville Radiology	Solar Communications International	Royal EGT
Grundbaulabor Trier	Caretaker Landscape and Tree Management	Deese and Locklear Chiropractic Center
Mann Group	Minkon	KSL Dirtworks
Groupe AC Environnement	Adams Warehouse & Delivery, Inc.	Nantou Shiuhkuang Senior High School.
SAP	Martin LLP	Petrosul Distribuidora, Transportadora e Com é rcio de Combust í veis Ltda.
Trade Union Co	MAP SA	TMobile
Trade Union Co [tuc-dxb.com]	Suhai Segurana Pessoal	Gate | Crypto Exchange
SOME	SBI Audiovisual Medinbox	RÉSO
WABAG	Saga University	The New Community School
Lydenburg Toyota	Netcore Unbxd	Qatar National Import & Export
Unisa Shoes	REGiO Nord	Matadero Frigor í fico Aviny ó
Zinkan Enterprises	Museum Siam	University of Rostock
Betopia Group	Skin Center	Riviera Healthcare Center
Malmsten	Thai Ha PCL KASET	Leadec
Acodafe	Inovar Packaging Group	Wavecrest HFA
Atlas Stamping Manufacturing	Engineers Ireland	Tec Imports
EPMMOP	North Bridge Venture Partners	UAE Pro League
Pure Perfection	SONGWOOI	City of Cloverdale
Belmont Resorts	Petroleum Telcom Communications	SANAtech Global Solutions
SoftwareOne	Axle Logistics	Raqib
Farmacias 911	Cradlewise Inc.	Tharisa
StarImage	CAS Paper Mill	Chibitek
Grupo Sanirent	Globeia Inc.	acmestamping.com

WIKA Beton	St Peters Anglican Primary School	harborpacific.com
Incomelec	Pantanal Agricola	architekt-vondanwitz.de
Epic Health	Canva	grunenwald.com
Surexport	Sladek Partners	avsa.com.ar
ASL İnsaat	JJS Justice	Aon
Vietnam Airlines	Hospital S í rio-Liban ê s	EPTISA
Northwest Micro Systems	ServiceMaster of Ottawa	Andersen Group
RaceTrakka	Verano Holdings	EDFelectronics
Smith Feddeler & Smith	Entry Systems Garage Doors Gates	Beni Suef Technological University - BTU
Serit CC	Europ Assistance South Africa	BNYH
Montship	Harness Inc.	Ciftay Insaat Taahhut Ve Ticaret Anonim Sirketi
Zehren and Associates	Taiwan Otsuka Pharmaceutical	KOOKABARRA JUICE
Pac Production	CLIMEDI	SweetRush
United Rolls	iHeartJane	magnals.com
Marie Kruses Skole	Universidade de Passo Fundo	Greggio Argento
Dataprobe	Campbell Rhea	Agri Industrial
Spontini	Newport Beach Dentistry	B-accountants
Florida Retina Center	Tulsat	Morcon Developments
KV Final	Shared Medical Technology	Kennametal
Animart Pet Stores	Santa Barbara Endodontics	Flydubai
Reynolds Logistics	Ecuadors National Police	Four Hands LLC
Aceros Ocotl á n Group	R. A. Wood Associates	Michael K Shelby, CPA
Tape Ruvicha	Tech Electronics	Hygrade
Lawrence Paper	Via Credit Union	CORBY ROCK MILL
Lodi Police Department	Evolution Spine / All Labs	Delta Marine
CS Repair Services	CureMetrix, Inc.	J&D Financial
Studebaker Submetering	Keio Corporation	Philander Smith University
JTEKT	Kemlows Diecasting Products Limited	Global Security Concepts
Capital Trade	fairfeelegalservices.com	Medical Data Rx

Imperial Glazing Concepts	verveba.com \ www.att.com	Agio International
Airbus SLC México	www.coopecaja.fi.cr	Sims Vibration Laboratory
schmitzmix.com	nowaszkola.com	Circulating Air
slyfoxbeer.com	Telcoe Federal Credit Union	Gen3
steeplechasetool.com	TGM Manufacturing, Inc	JPS Health Network
mpark.net	Segres Systec	Champaign Unit 4 School District
bicicletasmilan.com	Shield Wall Systems of Florida	Praxis EMR
Southeastern Food Supplies	karix.com	Standpointe / Trinite Solutions
Lingkaran Trans Kota Holdings Berhad	kidzrkooldental.com	dd-automation.ch
Thomas M Hughes	torcivialaw.com	stuecheli.ch
carypeds.com [carypediatriccenter.com]	lcww.com.eg	bwi-bau.de
Vienneau Insurance	neweramachines.com	halservice.it
Auto Bernhard	grupoabg.com	grundens.com
pratthomes.com	hilmar-cheese	t-systems.com
Corporate Services	KD Corp	Nelson Mullins Riley & Scarborough
Saginaw Chippewa Indian Tribe	Svd	Sheppard, Mullin, Richter & Hampton
Cooptech.hu	Videk	Turn5
www.skv.com	Boyle, Pecharich, Cline, Whittington and Stallings	anwo.cl
windowmaster.com	bienestarempresarial	duhaas.sk
infiniteservices.org	middleby	ikhasas.com
connexcu.org	sunshine-mills	sterrer.net
springbrooksoftware.com	Hocon Gas	Asia Era One
Hartshorne Plunkard Architecture	HyperGen	H&L Manufacturing
KONTEK Systems	Chattanooga Shooting Supplies	Onsemi
Omesti Berhad	Commune Du Tampon	part02.simplexengg.in
Lucky Union Foods	Brame Telecom	02 Dental Group
Michelle Accesorios	hensley	windor.com
Warrnambool Bus Lines	Enchanted Fine Jewellery	ENKA Schools
Fairfield City Council	buckle	Cam Group LLC

Ndi Engineering	camden-living	Franklin Empire
Southern Specialty & Supply	MPI LTDA	Infomedia A/S
Safe Data Storage	Amity University Dubai	Millensys
Delta Electric Power Association	Alma Center Servizi Medicali S.r.l.	Rueegseggerag
Bangor Wholesale Laminates	Holistic Health Group, Inc.	PANCARIBBEAN LOGISTICS GROUP
TeleTronic	alera	METROCOLOR S.A.
FIRMENGRUPPE APPL Holding GmbH	Interior Technologies	Thomas Y. Pickett & Co., Inc.
Premier Medical Group	japantimes.co.jp	Trump Mobile Wireless
Zachary Confections	MOA Architecture	Eteam
THOMAS JORDAN, P.A	Joliet Public Schools District 86	Royal Selangor
Five Star Sheets	Shediac Lobster Shop	Fluge Audiovisuales
Power Funding	FOODMatch	Bender Tribunenbau
Hochschule Worms	Torns Enterprises	TRANS LOGROÑO SOCIEDAD ANONIMA
Mountain Rheumatology	Oceania Digital Communications	Grupo Industrial Tauro
Taubensee Steel & Wire	FINANCIAMENTO LTDA	capitalbankhaiti.biz
Natural Energy Laboratory of Hawaii Authority	Trieschmann Dumala Architectural Group	Bold Spring Nursery
Burnaby Schools - School District 41	E-Z Pack Trucks	Silicon Valley Glass
Miller Stratvert	Green Clinic	Unident Group
Seufert Construction	kordhotels.gr	Chadwick Switchboards
Nissho Electric Manufacturing Co., Ltd	MyM ODONTOCLINICA S.A	Emser
BCSA GEAR	Estrategias BigMat S.L.U.	Cotesma
TRANSPORTES JIMENEZ and REYES JIM REY S.A.	Colorado Texas	OMUR HIRDAVAT LTD
Referans Lab Ref-Lab	Lane Equipment	Mutsumi Group
Ernesto Malvestiti S.p.A.	The Golden Legacy Financing	MorseLife Health System, Inc.
Inside Passage Electric Cooperative, Inc	Scheduled post	Nipigon District Memorial Hospital
mahsing.com.my	Iliff, Meredith, Wildberger & Brennan, P.C	Softruck
LoveSac	skycc.co.th	Center State Engineering

Glückauf-Vermessung GmbH	YYC Advisors	euroditel.com
Miletic GmbH	Cooper Tec Solutions	superpack.com.co
Edelstahl-Mechanik GmbH	nodhom.com	daralteb.com
J.B Hunt	IGPL	Genesis Credit Management
Yodingenierie	ocean beverages	Precon Marine Inc
White & Case	tdotnet	Skaff Group
Hossner-Textil GmbH	Ecuador police headquarters	St. Francis Healthcare Systems of Hawaii
Partido Liberal	merkezilac_archives	World Cup 2034
Ooredoo Myanmar	Ahlqvist & Almqvist Arkitekter AB	States Industries
Weitz & Luxenberg	Englunds Konsultbyrå AB	Aware
Astrana Health	Spectrum Arkitekter AB	Allied Machine & Engineering
A-RMS	Vendus Sweden AB	WOOSHIN SAFETY SYSTEMS CO LTD
Aesthetic Dental Designs, P.A	Fab Support AB	Step By Step
ECOM	Byrån för Arkitektur och Urbanism	Zelham
Jons Civil Engineering Company Ltd.	Briab Group AB	Hospital de la Santa Creu i Sant Pau
AyT COMPUTERS SRL	Danvikshem	Rotamac
ETO	Brunnberg & Forshed Arkitektkontor	Mandurah State Emergency Service
TOPLIVO AD	Mantum Holding AB	Westrop Primary & Nursery School
Technoleads Services Inc.	Lambertinum Seniorenwohnanlage	Gerrity Stone
Pure Grow Diamonds Inc.	KVH	Forma Therapeutics Holdings, Inc.
Mach Law APC	Laerdal	seven seas group
Keidel Supply Company Incorporated	Topcon Healthcare	Thai Lion Air
Andrews Advisory Group LLC	Milstein Siegel, LLC	Mat Bao Corporation
AB InBev	Comisión Municipal de Agua Potable y Alcantarillado de Victoria	Paessolucoes
Hisense	Great Lakes	Electro Heat Sweden AB
Newcomer Cremations, Funerals & Receptions	Durga Bearings	Sports Events365
mediporta.ch	Codar Ltd	The Official College of Architects of León
Castle Howard Estate	Alfameli Group	Jampac Alimentos

Vins Viallet	Hunter Neurology	hollypoultry.com
Heber City, UT	Interseguro	www.windor.com
Phoenix S&S GmbH	Excess Baggage	translarity.com
Frommann Energie GmbH	Wolf & Sofsky GmbH	Pacific Tank Lines
SLTN Inter Access	Guarufilme	Inova Semiconductors GmbH
www.choicegoodwill.com	Admirals Trading	PT Indo Tambangraya Megah
mainplace.com.my	Valode & Pistre	Raleigh Family Medicine
MODON Developments S.A.E	Zenidoc	EdgeEndo® USA
www.zhservices.com	MarieBelle New York	Soni Medical Centre
grupoeuro.com.mx	PG Group	University of Illinois Chicago
www.optika.ca	CMC AUDITORES SRL	Tronex A/S
Texcar Inc.	Decorolala	www.kres.cz
GPIC Projectos Con Instalacoes Lda	The Buckner Company, Inc.	www.raajratna.com
Asisken Asistencia Médica S.A.	The Innovation Group	www.pierrefeu.fr
Adirondack Networks, Inc.	DFK Group	sai.org.in
Arthritis Center of Riverside	Saddlers Court MFG	baltimorefreightliner.com
Morrow Meadows Corporation	Culinary Specialties	goldenpearfunding.com
Merical LLC	Advanced Imaging Solutions	mcpolymers.com
Weld Re 8 School District	The Park Lane Hong Kong	UNION FA
Red Oak Technologies	Libre Wireless Technologies	Far West Contractors
Penco Products	Amantya Technologies	Automovil Club del Ecuador ANETA
Conax Technologies	Gatetech Technology	Sangre de Cristo Electric Association
Commonwealth Community Bank	AAA Architectural Hardware	Main Place Mall
Trinity Custom Homes	hiqbio.com	EURODITEL/RESOTELECOM
Family Planning Association of Pakistan	RingSide Creative	Hospital Hermilio Valdizán
Hensel Elektrik	Aeroklas Duys / Duys Engineering Group	Slate Valley Unified School District
von Schaewen	Rechtsanwaltskanzlei Dr. Bien	steelco
Tamponnt	Franklin Miller Inc.	ProMind IT

Sanders Law Group	PennEastern Architects LCC	DISK PRECISION GROUP - diskprecision.com
Miljaus Producciones S.L	Claire's Inc.	FUNAP - Fundação "Prof. Dr. Manoel Pedro Pimentel"
mickeybody.com	Albertin Alcide e Figli S.n.c.	ASSOCIATED GASTROENTEROLOGISTS OF CENTRAL NEW YORK, P.C
ARX Group SA	SA BAUFER V.F	Terca
Aryza	Tema Energy S.r.l.	Superior Plating Technology CO
Aerotop	CFG SERRAMENTI S.r.l.	Wesmar
CDG Chartered Accounting	i2r Packaging Solutions Limited	DPL Group
mlh.com.lb	Robert Hitchins Limited	Krycler, Ervin, Taubman & Kaminsky
dorsiacademy.it	Pedigo Products, Inc.	Graybar Electric Company, Inc.
lidoway.com	Valenti Management	Rimrock Foundation
zelsior.es	Concord Eye Center	parkdental.com
JS Constructor, INC	Greentech Environmental	VPNE
Whirlpool	Engineers Contractors Fabricators Inc.	TLC Perinatal
JB Hunt	Nu-Quest Distribution Inc	Vera Science
Labaid Cancer Hospital And Super Speciality Center	brookslawfirm.com	Owens Distributors
Kale Balata A	Louis Fusco	Dynamic Office Solutions
MaxiSeguridad	PIC GROUP, INC	Guardian Pharmacy LLC
Revi Group	ConAuto	Den Hartog Industries
Bankruptcy Software Specialists	Prodiel	Northern Counties Health Care
Bravilor Bonamat	MyMichigan Health	Post Metal Recycling
SCHWAB-SYSTEM	VIATechnik	LA PONDEROSA
Wah Chan Consolidated Sdn Bhd	GlobalNet LCL	Laboratorios Roemmers SAICF
Trevi Technology	Santos Brasil	consilio.com
Don Pickett & Associates	Asyaport	Ocean Network Express
vinsolutions.com		

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 Server 2008、Windows 10 以及 Windows 7。

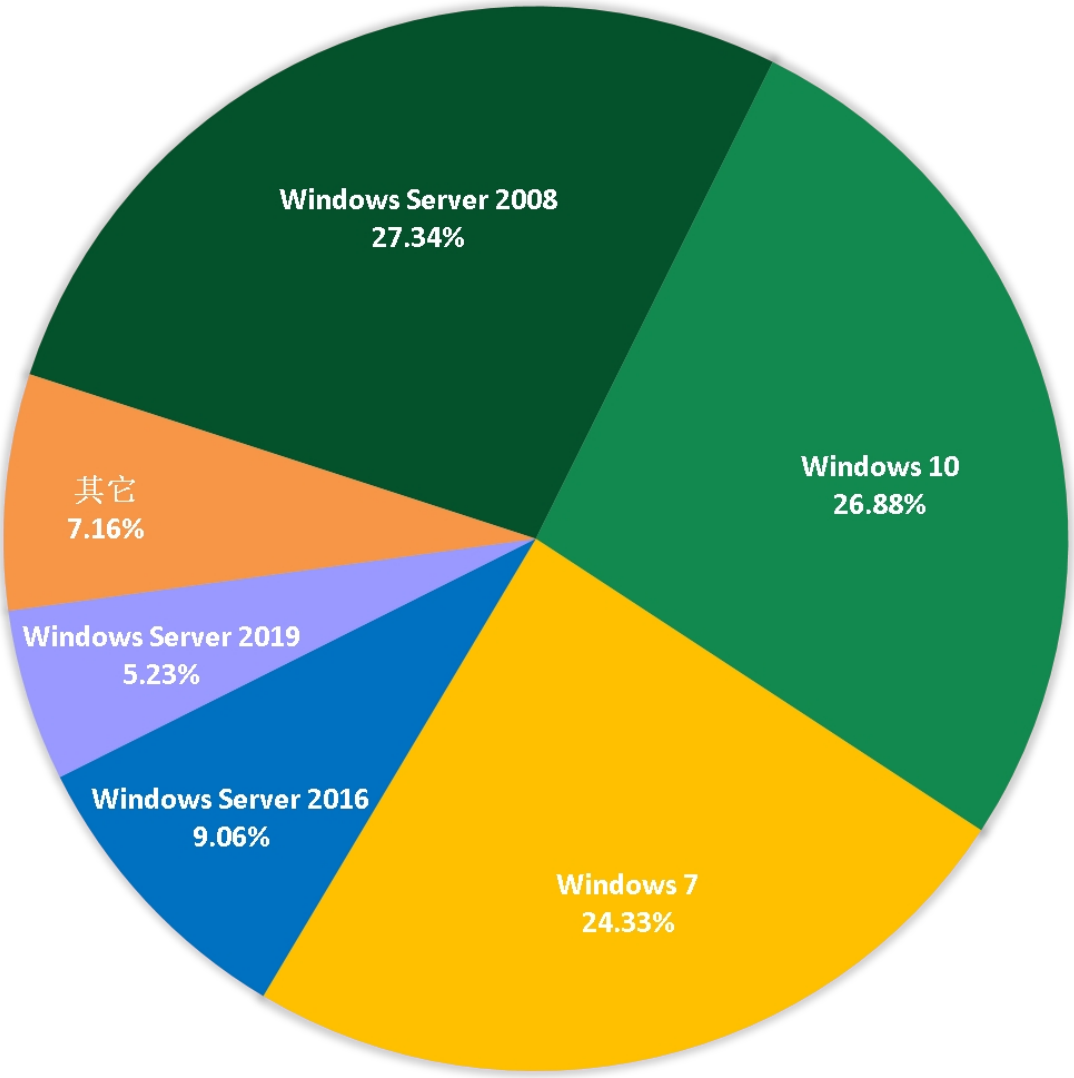


图 9. 2026 年 10 月受攻击系统占比

对 2026 年 10 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。

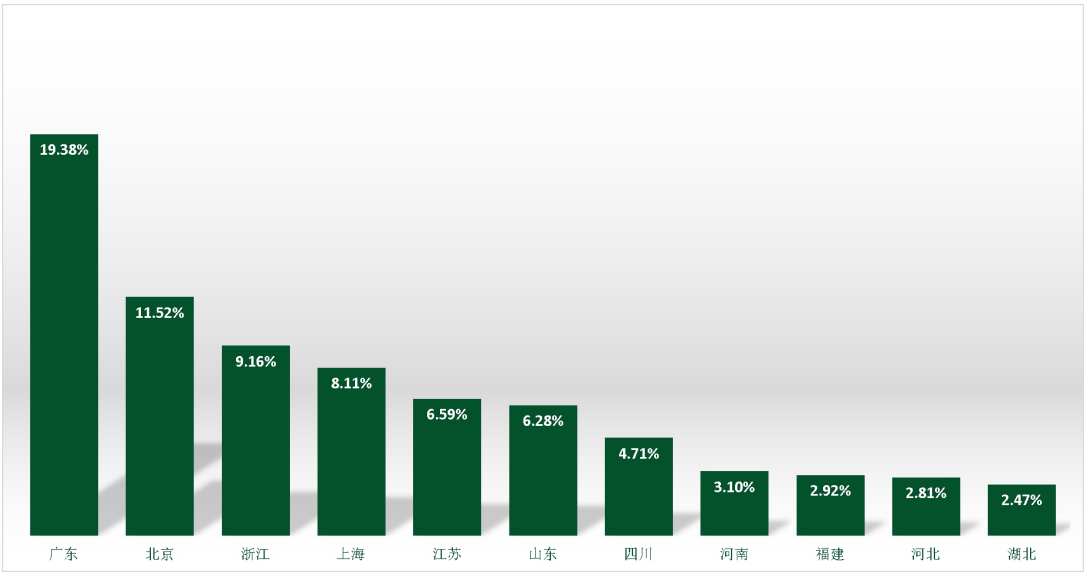


图 8. 2026 年 10 月国内受攻击地区占比排名

通过分析 2026 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。

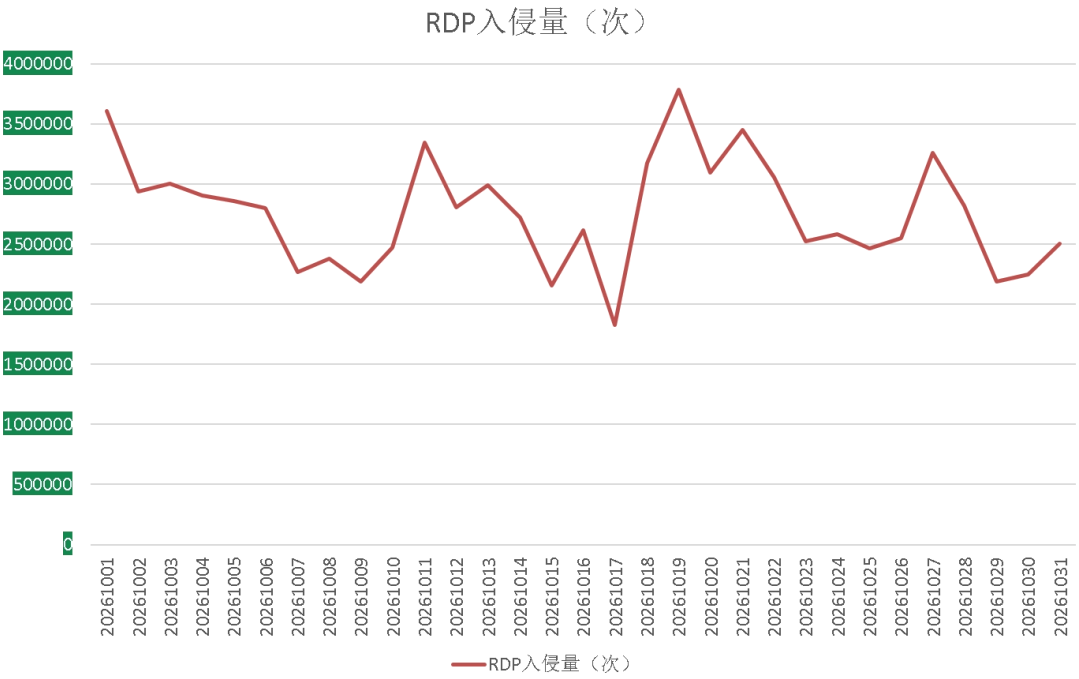


图 9. 2026 年 10 月监控到的 RDP 入侵量

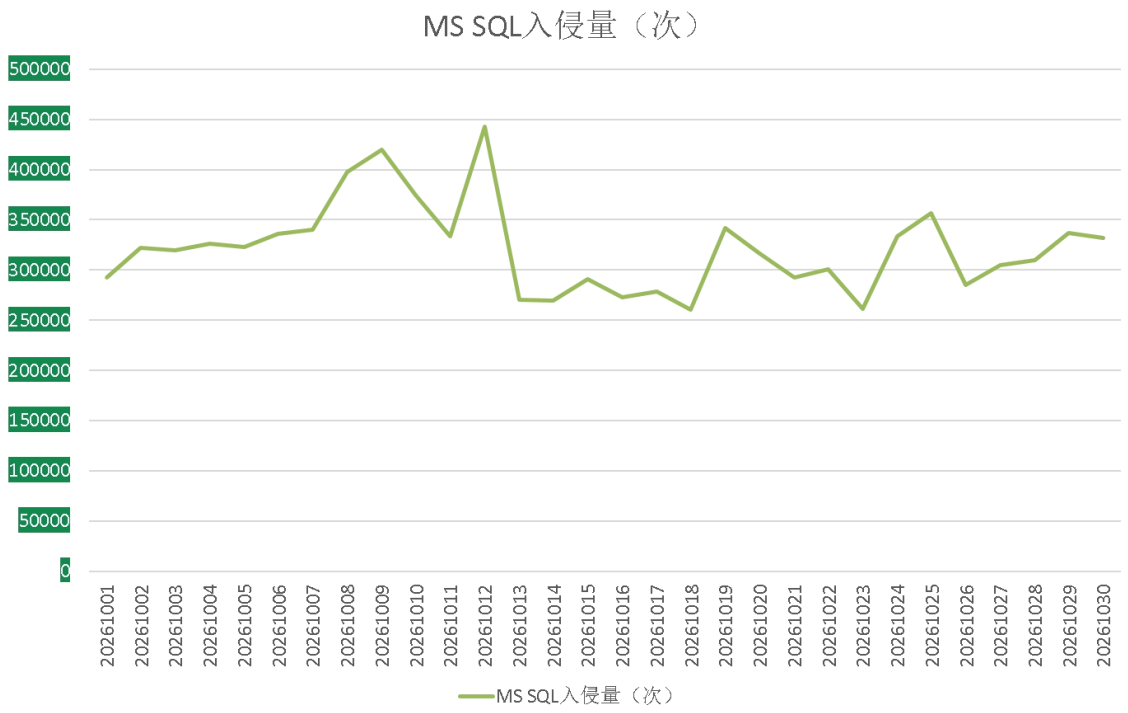


图 10. 2026 年 10 月监控到的 MS SQL 入侵量

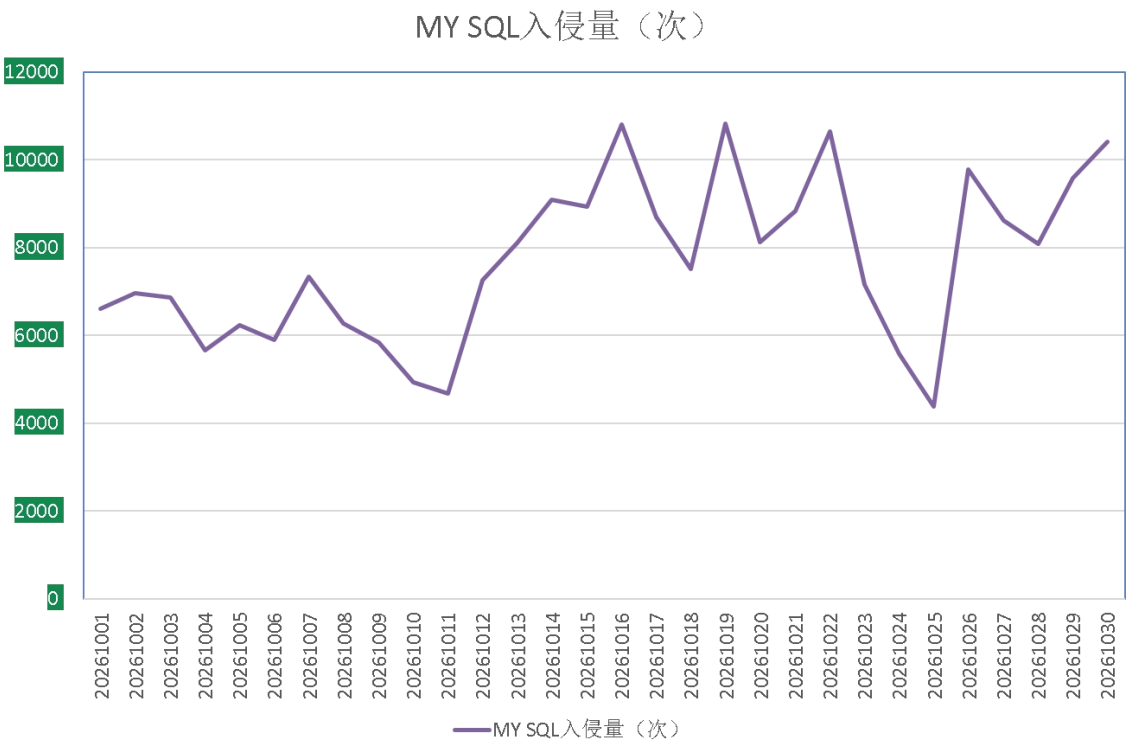


图 11. 2026 年 10 月监控到的 MYSQL 入侵量

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。

✧ 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。

✧ rox（同 weax）

✧ l0ck3d

属于 Cerber 勒索软件家族的 Linux 变种，该分支变种的主要传播方式为：利用 Linux/NAS 漏洞发起攻击。

✧ 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。

✧ xdata

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。

✧ lock3d（同 l0ck3d）

✧ weaxor（同 weax）

✧ 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。

✧ 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。

✧ 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。

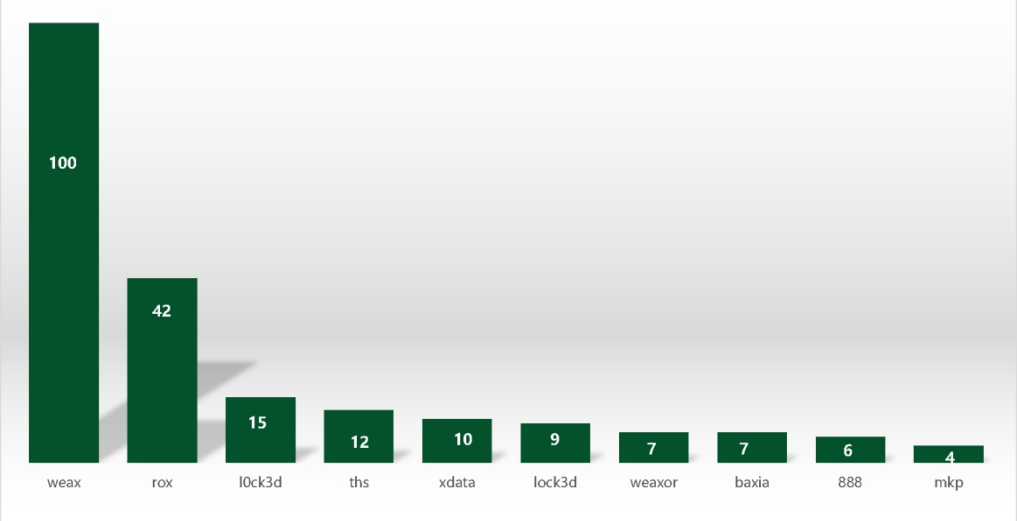


图 12. 2026 年 10 月反病毒搜索引擎关键词搜索排名

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 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。

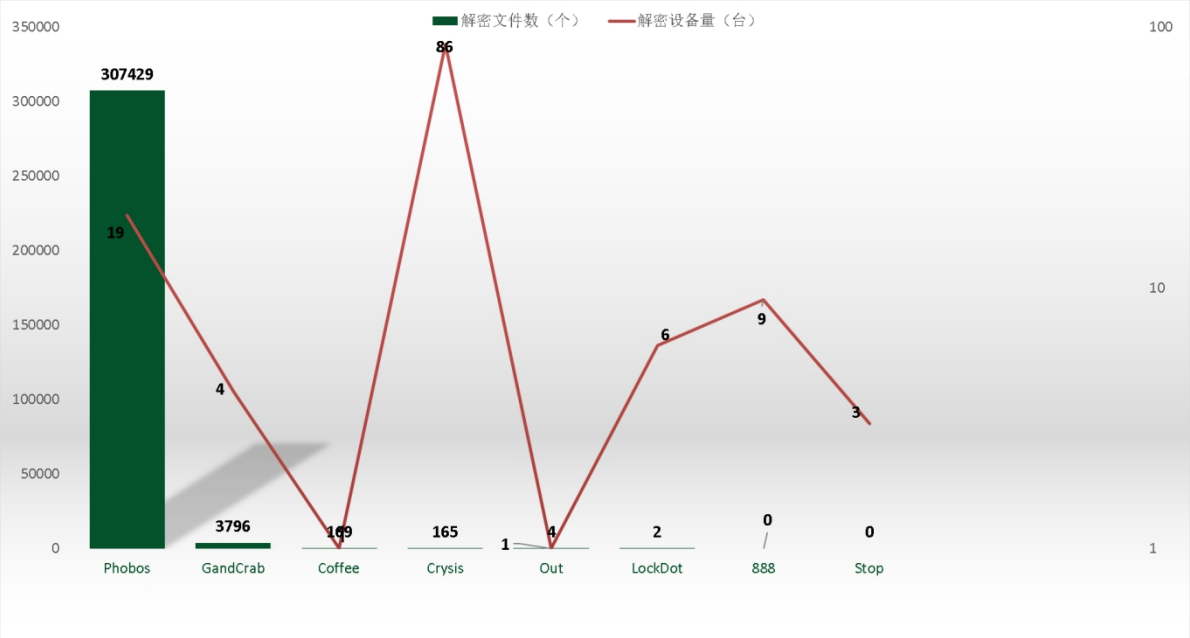


图 13. 2026 年 10 月解密大师解密文件数及设备数排名