勒索软件流行态势分析

2025 年 11 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，为需要帮助的用户提供 360 反勒索服务。

2025 年 11 月，全球新增的双重勒索软件有 Tridentlocker 家族，传统勒索软件新增 QuickLock、Kazu、BlackHeolas 等多个家族。

近半年在国内持续热门的 Top2 家族 Wmansvcs 进行了一次变种，加密后缀由之前的.peng 变成了.wman，攻击方式依旧是远程桌面协议登录投毒并同时加密共享设备。

本月 360 发布了仅在国内传播的 SnowSoul 勒索软件技术分析与独家解密方案，充分体现了 360 反勒索服务的技术能力与长期守护的决心。

以下是本月值得关注的部分热点：

1. **OnSolve CodeRED 网络攻击扰乱全美紧急警报系统**
2. **《华盛顿邮报》数据泄露事件影响近 10 万名员工和承包商**
3. **媒体巨头日经新闻通报数据泄露事件影响 17000 人**

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 33.54%居首位，第二 Wmansvcs 家族占比 26.08%，LockBit 家族占比 11.8%位居第三。

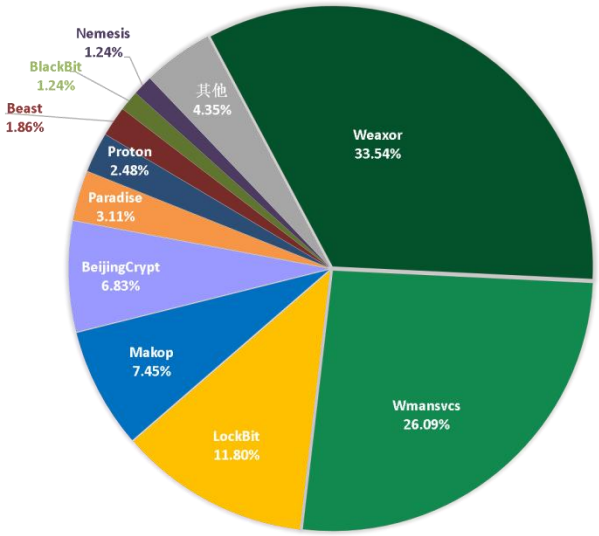

图 1. 2025 年 11 月勒索软件家族占比

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。

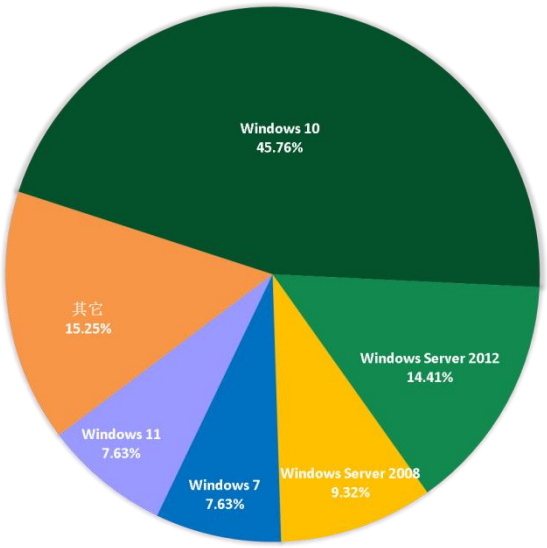

图 2. 2025 年 11 月勒索软件入侵操作系统占比

2025 年 11 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。

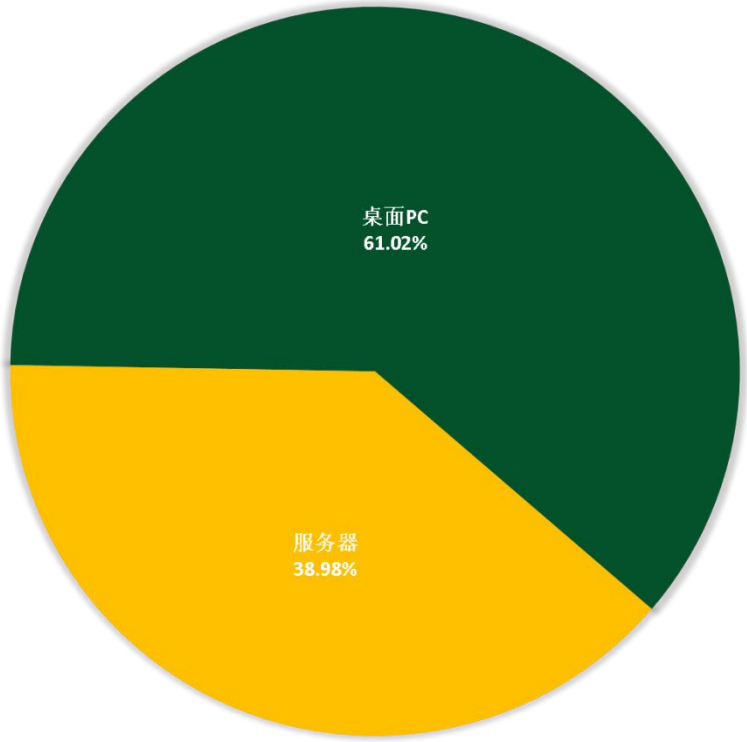

图 3. 2025 年 11 月勒索软件入侵操作系统类型占比

勒索软件热点事件

OnSolve CodeRED 网络攻击扰乱全美紧急警报系统

OnSolve CodeRED 平台遭遇网络攻击，导致美国各州和地方政府、警察部门、消防机构等公共安全单位紧急通知系统瘫痪。Crisis24 公司确认，该平台遭到网络犯罪集团攻击，迫使其停用旧版 CodeRED 系统，并开始恢复新的 CodeRED 系统。虽然攻击只影响了 CodeRED 平台，并未波及其他系统，但攻击者从平台窃取了大量用户数据，包括姓名、地址、电子邮件、电话号码和密码。Crisis24 表示，虽然数据被窃取，但目前没有证据表明数据已公开发布。

同时，Crisis24 的调查显示，黑客使用了 INC Ransom 勒索软件家族，并于 2025 年 11 月 1 日入侵 OnSolve 系统，11 月 10 日加密文件。勒索集团要求支付赎金，但因未收到赎金，黑客已将偷取的数据出售。数据泄露后，客户被建议重置 CodeRED 账户的密码。该勒索软件家族自 2023 年 7 月起活跃，已攻击多个行业的组织，包括教育、医疗、政府等。

《华盛顿邮报》数据泄露事件影响近 10 万名员工和承包商

《华盛顿邮报》近日通知近 10000 名员工和承包商，他们的部分个人和财务数据在 Oracle 数据泄露事件中遭到曝光。攻击发生在 2025 年 7 月 10 日至 8 月 22 日之间，黑客利用 Oracle E-Business Suite 软件中的零日漏洞侵入了《华盛顿邮报》的网络。该软件广泛用于企业资源规划（ERP），包括人力资源、财务和供应链管理。黑客窃取了敏感数据，并在 9 月末尝试向《华盛顿邮报》勒索。调查显示，攻击者利用这一漏洞侵入了多个大公司，包括哈佛大学、美国航空子公司 Envoy Air 和日立旗下的 GlobalLogic。

根据《华盛顿邮报》的调查，约 9,720 名员工和承包商的个人信息被泄露，包括姓名、银行账户信息、社保号码、税号和身份证号。受影响者已获得为期 12 个月的免费身份保护服务，并被建议冻结信用档案和设置欺诈警报。

尽管攻击者未被明确指名，但已知 Clop 勒索软件团伙与这些攻击事件相关，该团伙利用了现在被追踪为 CVE-2025-61884 的零日漏洞。值得注意的是，今年早些时候，《华盛顿邮报》的记者电子邮件账户也曾遭到外国国家行为者的攻击，且两起事件似乎有某种联系。

媒体巨头日经新闻通报数据泄露事件影响 17000 人

日本媒体巨头日经（Nikkei）近日报告了一起数据泄露事件，涉及超过 17,000 名员工和商业合作伙伴。该公司透露，攻击者通过盗取员工计算机感染恶意软件后获取的认证凭证，成功访问了日经的 Slack 消息平台。泄露的个人信息包括 17,368 名 Slack 用户的姓名、电子邮件地址和聊天记录。

日经在 9 月发现了此次安全漏洞后，立即采取了安全措施，包括强制修改密码等。尽管事件的规模较大，但日经表示泄露的信息不符合日本《个人信息保护法》的报告要求，因此没有法律强制报告。但公司仍自愿向日本个人信息保护委员会通报，并强调透明度和事件的“重要性”。

日经还表示，泄露的数据不包括机密消息源或报道活动相关的信息，且用于新闻工作的个人数据未受影响。此次事件显示出日经对个人信息管理的重视，承诺加强管理以防止类似事件再次发生。

黑客信息披露

以下是本月收集到的黑客邮箱信息:

ruizback@proton.me	edfr789@tutanota.com	fffacai888@tutamail.com
Rheinland01@privatemail.com	edfr789@tutamail.com	goodluckmail@onionmail.org
lockbit_black@zohomail.com	recover300dollars@gmail.com	joedecryption@gmail.com
lockbit_black@groupoffice.ch	madmaxxx8@protonmail.com	Decryptionfile@gmail.com
cianbang@mailum.com	madmaxxx8@cock.li	Dani@mailum.com
sentinel_supp@proton.me	datahelpernew@proton.me	kotaneex@onionmail.org
troyaThe@proton.me	nudasurg@cyberfear.com	kotaneex2@onionmail.com
info@cloudminerapp.com	SloanAlbert@protonmail.com	key2030@cyberfear.com
mikazeg@onionmail.org	orbbec@mailum.com	key2030@firemail.de
cabasetra2030@onionmail.org	BlackHeolasSupport@onionmail.org	itkey2030@proton.me
nudasurg@tuta.io	fastnas@fea.st	suppdec2@aol.com
thewandpos@zohomail.eu	gds134s@mm.st	Ross.dec1966@gmail.com
javesus@email.tg	icq-is-firefox20@ctemplar.com	bobofdc@tutamail.com
sanert99@tuta.io	telegramfirefox2029@protonmail.com	begins@colocasia.org
IndiAdams@onionmail.org	anon@gartnersdwan.top	bilbo@colocasia.org
jimmyhendricks@tutanota.com	anon2025@keemail.me	frodo@colocasia.org
karlironsterson122@protonmail.com	Evoteam.sup@gmail.com	trevor@thwonderfulday.com
AsuxidOruraep1999@o2.pl	Evo.team1992@gmail.com	bob@thwonderfulday.com
thevigorousransom@onionmail.org	restore_data@gmx.de	bil@thwonderfulday.com
opnkey@gmail.com	restore_data2@mein.gmx	redbl00df0cker@proton.me
n0deByte@Tutamail.com	bitcoin1@foxmail.com	reopeningvip@gmail.com
JanayshaKennin95@mail.com	lockjimmy@onionmail.org	rdp21@onionmail.org
MarzocchiZadok95@mail.com	decrypt2024@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）。

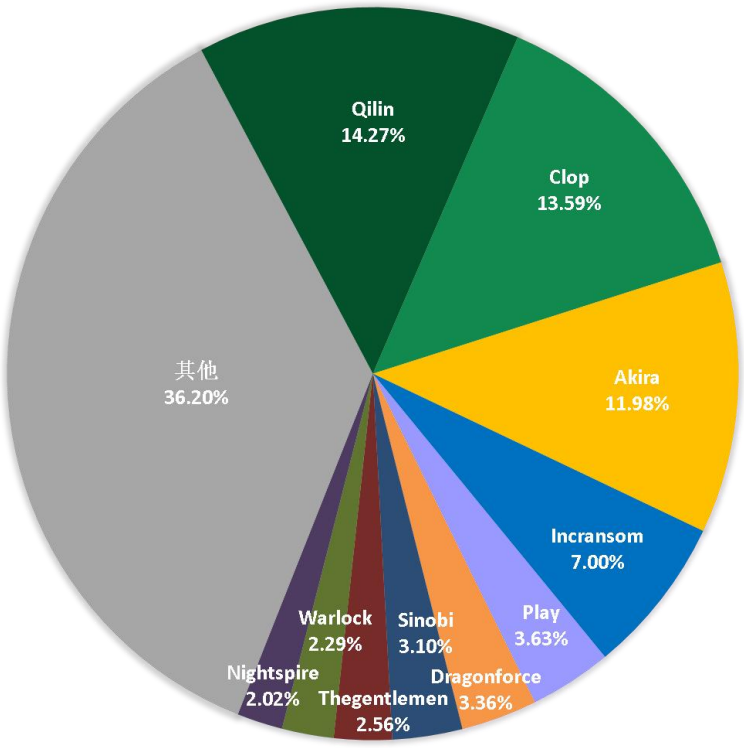

图 4. 2025 年 11 月通过数据泄露获利的勒索软件家族占比

以下是本月被双重勒索软件家族攻击的企业或个人。若未发现数据存在泄漏风险的企业或个人也请第一时间自查，做好数据已被泄露准备，采取补救措施。

本月总共有 696 个组织/企业遭遇双重勒索/多重勒索攻击，其中包含中国 8 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 22 个组织/企业未被标明，因此不在以下表格中。

Concord Academy	CIGAM Software Corporativo Ltda	Fulgar S.p.A.
Veton Ai	SAExploration	Irwin Car
ILCA Targhe s.r.l.	Kewaunee Scientific	Brenda Richardson Memorial Care Home LLC

Battaglioli	classiccenter.com	Olive Branch Family Medical Center
Division 10	Cimertex	DARTMOUTH.EDU
TBC Consoles	Fayette County	glendaleobgyn.com
CJW	Radio Sound	S.B. Conrad, Inc
Chenango Valley Technologies	Applied Energy Systems	Continental Global Group
Asia Condominium Association	Artesian Insurance	Lows Orkney
Bomchil	One Source Associates	Manusos General Contracting, Inc
Rasen Insaat Ve Yatirim Ticaret A.S.	N C Machinery	Barry Sallinger Law
Badan Pengelola Keuangan Haji	Highmark Companies	Miromar
GuestTek	FELA (EVYTRA)	Rhodes Young Black &Duncan RYBD
Advantage 360	GREENBALL.COM	Brian-Kyles Construction
iqs	SUMITOMOCHEMICAL.COM	Public Safety Mutual Benefit Fund
LMG Holdings	MICHELIN.COM	Octomeca Oy
EnQuest	WELLBIZBRANDS.COM	National Civil Service Commission of Colombia
Calmec	DOONEY.COM	Defensor í a del Pueblo de Colombia
typecaseinc	SIU.EDU (EBS)	Doctor Alliance
asiawba	ALJOMAIHAUTO.COM	omniumint.com
Everbiz Industrial Co. Ltd.	FRUIT.COM	Polidano Group
vviewisd.net	FRONTROL.COM	himmelstein.com
Williamson County, TX	HUMANA.COM	Paul Hildebrandt
Zoya	ORACLE.COM	Vascara, Vietnam
Weiss	ABBOTT.COM	PAFL.COM.PK
Kleber and Associates	MAZDA.COM	SAMCRETE.COM
Lone Rock Timber	MASHOLDINGS.COM	GAEAGLOBAL.COM
Casting House	CANON.COM	P2ENERGYSERVICES.COM
Parrish Tire	TRANETECHNOLOGIES.COM	GLOBUSANDCOSMOS.COM
Panini Kabob Grill	GRUPOBIMBO.COM	ENNVEE.COM
Family Farm and Home	BECHTEL.COM	CARGLASS.DE
Gershow Recycling	ELCOMPANIES.COM	VITAMIX.COM
Design Team Sign Company	RIDERTA.COM	GARDENOFLIFE.COM
K2d	BROADCOM.COM	NHS.UK
Morton LTC	Wright ArchitecturalMillwork	Middlesex Endodontics
Devereux Advanced Behavioral Health	Swift Filters	Hongji Metal
Ingenieurbü ro Laudi	A10NETWORKS.COM	Sarulla Operation
Mid South Pulmonary & Sleep Specialists	ENVOY.COM	www.modcomedia.com
Comansco	ALSHAYA.COM	SIAD
Enerre Pharma Lda	FLEETSHIP.COM	AGFA
Caros co	MAZDAUSA.COM	Easterseals Arc of Northeast Indiana
ERR Raumplaner	WORLEY.COM	Community Unit School District 201
Bcfpers	LLPRODUCTS.COM	ielplumbing.com
United Volleyball Supply	TREETGROUP.COM	Heart South Cardiovascular Group

Mechanical Systems	PHOENIX.EDU	Yaesu
Hitech	Teamglobal	Garvin Promotion Group
Crucible Industries	Sakol Energy Public	Jean-Georges
Asl Consulting	Mae Krathing Power Company	Kwik Mix Materials
Country Club Enterprises	N15 Technology	Ioxo & Stream Computers
Kelly Wearstler Gallery	Hydroscand	Darvin Furniture
Santa Paula	AJ Jersey	Land Title Guaranty
PFMI	Makro	OMS
WLR Precision Engineering	Söllner	Mciver Engineering & Controls
Rama Judicial	naffco.com	Ami Bearings
Shelbra International	HostingFest	MARCK Industries
The American School Foundation	Croft	Weintraub Traub Tracy & Virk Cra's LLP
Secure Network Solutions	CHANGEPOND	LMHT Associates
St. Johns River Water Management District	IGT	Seward County, KS
Zoetis	American Trust Administrators	CapitalPlus Exchange
Fineline Architectural Millwork	future.com.bo	ikad.com.au - A 5-Month Staycation in the Defense Supply Chain
Healthcare Retroactive Audits	Orchid Island Golf and Beach Club	Servicios del Valle del Fuerte, Mexico
FIT	Modern Display	Fidelity Pension Managers, Nigeria
ADC Aerospace	The InterTech Group	Eastern Cape Department of Human Settlements
suzuki-ploiesti.ro	CYTIVALIFESCIENCES.COM	Instituto Nacional de Oftalmologia
poliserv.ro	Pearl River Valley Electric Power Association	Atrium Living Centers
mazda-ploiesti.ro	NCH.COM	Gullco International
dacia-ploiesti.ro	ENOVIS.COM	Ringmor
sevci.org	ELKAY.COM	Punjab Forensic Science Agency
K.M. Packaging	LIFEFITNESS.COM	Noroaco
Transpedrosa	TULANE.EDU	Hitzinger
Clemar Assessoria e Logística em Comércio Internacional	RFSUNY.ORG	JC Auto Accident Law Firm
Meinhardt Malaysia	BELFUSE.COM	Gadge USA
Electricidad Panamericana	GARLANDISDSCHOOLS.NET	Ponzini S.p.A.
AGS	AVAILINFRA.COM	Advanced Delivery Services
Stacey L Tokunaga	Perry Brothers Oil	Wasserverband Wulkatal
Church of the Ascension Anglican	Aarco	SHRM New Mexico
Bergeson	reidhurstnagy.com	Scouts Canada
Dobco	mcchemical.com	Mold In Graphic Systems
Pacific Railway Enterprises	ARENCON	DCS TECHNOLOGIES INC.
FloorHeat	Cardinal Services	GB Mail
Globatech	Stoss Landscape Urbanism	Shollenberger Januzzi & Wolfe
Williams & Sparages	Marine Foods Express LTD	Marine Turbine Technologies

Trolec	B&J Rocket Sales	Clackamas Community College
ITL Systemhaus	FSGROUP-Engineering	PT Kalimantan Prima Persada
Arabia Holding	Genrose Stone + Tile	Village of New Lenox
Emond Publishing	heywood.org	Klae Construction
Burnham Brown	Spark Innovation	Soapy Joe's Car Wash
Eastek International	TFC Poultry	Shands Elbert
Workflow Concepts	istitutocomprensivo-cavaglia.edu.it	PLP SoCal
BioPharma Services	puertoricowarehousing.com	Koch & Co, Inc.
Disston	adesursas.com	Aptura Group & Central Indiana Hardware
Carlton Fields	aussenwelten.ch	Rex-Hide
AllerVie Health	simmonsbb.com	Studio Corvo Parma
Kids & Company	baisyaakov.ca	www.wilmar.co.id
National Money Mart Company	continuumindia.com	www.danareksa.com
Paal	ripleyacademy.org	www.marjane.ma
Inspire Communities	grandeprairie.org	Health Dimensions Group
New England Tractor Trailer Training School	Bleyl Engineering	ZANACO.CO.ZM
Christofle	datenlotsen.de	WASHINGTONPOST.COM
Columbia Medical Practice	zadroinc.com	Ketat Grundstücksverwertungs GmbH
Lake Superior State University	Regional Business Systems	prutsch-ra.at
Rochester Philharmonic Orchestra	General Distributing	MusikComputer GmbH
Accord Carton	FDC Interiors	UScraft
Iberia	MFE Formwork Technology	Provincial Department of Health Services Sri Lanka
amcor	Nationwide Legal LLC	pmsp.at
Universidade Municipal de São Caetano	Kensington Court	elektroanlagen
WR Comercial	QuaLex Manufacturing	Sai Mai Hospital
cryopur.com	INNOVEX HOLDINGS CO., LTD	PCB Uitvaartzorg
Standing Chapter 13 Trustee	Smoll & Banning, CPAs	INFORMA.COM (EBS)
Schmidt's	dulay.ca	RHEEM.COM
Rempe Construction	Kdr Real Estate Services	WOODPLC.COM
MSK	Air Design Systems	ELSEWEDYELECTRIC.COM
Marlex Human Capital	Lincoln IT	KIER.CO.UK
Balkrishna Paper Mills LTD, India	H G Reynolds	zebra.or.at
NONC, India	Charles Rutenberg Realty	Ville de MontLaurier
LAMAICA, Egypt	Poe's Accounting Services	Tass Meister Patent Firm
StatMedPlus LLC	Quinn Jay Patent	Systems Integrated
Nottingham Village	Law Office of Ronald W. Hillberg	LOGITECH.COM
Zecher	LG Energy Solution	Black Hills Bentonite
Blue Projects	Eagle Oil & Gas	DRD Communications
Amcore	ARH Associates	First Resources
Ecuacorriente S.A.	Petrobras / SAExploration	E-First Aid Supplies

HYTORC	UNDER ARMOUR	INTERNATIONAL.COM
Southern Lion Sdn Bhd	AkroStar Technology Co., Ltd. Akrostar	KIRBYCORP.COM
AirMiles España, S.A	BOLD Furniture	TRIMBLE.COM
Swedish Arts Council	MOBI Technologies	MKS.COM
Issaqueena Pediatric Dentistry	Lotus Powergear Pvt. Ltd, India	Dermatology Associates
omegatoolcorp.com	United Enterprise Fund	Noble Compañ a de Seguros
Talarico	Maresa Log í stica	speedmais
Kl ü ber Lubrication	https://www.bew.co.th	vratatech
Lithographix	SES Soci é t é Energies Services	Brihta
NovAtel (belongs to Hexagon)	FREEDL GROUP s.r.l.	energogroup.net
Westrian Group	Horst Realty	goldenline.com
Chairmans Foods	Spoleta Construction	bengineered.com.au
Akehurst Landscape Service	Cera Stribley	mnpease.ca
dynamichomerepair.com	Kaener Personal	metro.local
rehmann.de	Ninas Jewellery	cybervector.co.uk
Adept	University of Gävle	fabrity.local
Collge Superieur De Montreal	Saude Fortaleza	miltech.local
Advanced Dental	Stark Shipping	mytune.me
Access Search	ANG BROTHERS (M&E) PTE. LTD. (P1)	atg.cz
Liberty Gold Fruit	SWISS ROSE Factory	tein.co.jp
NBCAPITAL JOINT STOCK COMPANY	Medidores Industriales y Medicos SA de CV	bel.quadra.ru
Singapore City Development Company Limited (SINGCONS)	Spark Power	ippm.org
AiHealth	Force Brokerage	sf.walltopia.com
KIM Dental	Sol Trading	nartis.ru
Homestead Museum	killinglyschools.org	alphasys.bo
ANG BROTHERS (M&E) PTE. LTD. (P2)	eakas.com	silanosn.local
Pacific Holdings Group JSC.	Jefferson Enterprises, LLC	The Union League of Philadelphia
Maheu&Maheu	Platinum Healthcare Staffing	Francehopital
Cal-Comp Electronics Public	UNOde50	LaRosa’s Pizzeria
mToilet	Herman & Chamow	Oscars Group
Cayuga Milk Ingredients	Aero Precision	www.oucru.org
The Hunnicutt Law Group	Valley Banks	Nobu Restaurants
Berts Electric	Trigg Laboratories	The Fence People
Capp Shupak	Valley Plains Equipment	Maine Course Hospitality Group
Coral Clubes - Mexico	Sellers Publishing	KISS FM
National Institute of Materials Physics	BK Precision	Shelbyville Police Department
Outback Pharmacies	Barbizon Lighting Company, Roseburrough Tool, Mqd, McKay Empire, Victor Insulators.	sensationalteeth.com

Nissan Capital	A-B Communications	Pine Pharmaceuticals
Bodega San Huberto	Kaan Cronenberg & Partners Law	Christina Development
Parsirang	Waukegan Steel	mcintoshlabs.com
Summit Construction Supply	Basin Harbor	SAIGON INDUSTRIAL SERVICE
Nugent Supply	Barnhart	Coilplus
Fueling Solutions Inc.	The Foot Doctor's	SERAPHITA GmbH
Healthcare & More	facadeinnovations.com.au	Habib Bank
Nuclebrás Equipamentos Pesados	www.northcroftme.com	Durvet
Barr Trucking Inc.	kellylegal.com.au	Enem Nostrum Remedies Pvt. Ltd
F-W-S Countertops	wafergrind.com	ConvExx
Mmlk	duboiswood.com	Sellars Absorbent Materials
Katch Kan	GLOBALLOGIC.COM	American PowerNet
Keystone Fabricating	rosemontexpo.com	thevisapro.com
Turkstra Trusses	Metropolitan Adjustment Bureau	Property Finder / PropSpace
vanteceurope.com	AFLGLOBAL.COM	Mango's Tropical Cafe
St. Joseph's Healthcare Hamilton	INTEGRALIFE.COM	Prova
C&M Software	MARITZ.COM	MS Metal Solutions
onsolve.com	HELIXESG.COM	Palacios Marine & Industrial
Kajima Europe	TPICOMPOSITES.COM	Benda Grace Stulz
Medical Center, LLP	FLUKE.COM	Elliott Tax Service
Interlink Trade Services	SATO-GLOBAL.COM	St Stephen's International
Woom GmbH	FORBESMARSHALL.COM	Automated Logistics Systems
Sansala	PENS.COM	General Micro Systems
gsccca.org	ENTRUST.COM	Invacare
Colliers	avrind.com	DOVERN Import
procure.com	Viabizzuno	Rios Espinosa
Alma Realty	Muskoka Brewery	Crown Automotive Sales
XOX Mobile	Fundidora de Cananea, S.A	www.heitech.com.my
Electro Mechanical Industries	FullBeauty Brands	www.myriversidedentaloffice.com
PM Plastics, Reliable Van & Storage, Landis, Whitinger Strategic Services, Kimber Manufact	Lung Rose Voss Wagnild	Irwin Car
First Fruits Farms	Coral	LV.COM
HCMSPARTNERS.COM	Hyundai Nishat Motor	Morris Communications Company LLC
DMC-ME.COM	YPC MALAYSIA	Moonlight Basin
MSG.COM	Smith Gardner	Designs for Vision
INTELLINUM.COM	confortchem.com & rogitex.com	Mecanex USA
KNEXTECH.COM	PACCAR	Bishop Ireton High School
ANYWHERE.RE	Avery Dennison	Pinto Coates Kyre & Bowers
GOLDSTARPENS.COM	Cinvestav	Montage Marketing Services
NEWLINECLOUD.COM	SGK INC	Seasons Federal Credit Union
Fucerep	Goldhorse Capital Management	Dayal Metal Containers Factory LLC
NAMA.OM	Vikor Scientific, LLC / Korgene	BR Group

NORTHEASTERNCORP.COM	KorPath	UnitedLayer
AQM.COM.SA	Cornerstone Staffing Solutions	afton.loc
MACYS.COM	www.pointcag.com	Vitalmex
HYPERTHERM.COM	Persians - Cortinas - Todos - Alfombrass	G. Hauswirth Architects
KOREANAIRCND.COM	libertyshoes, Inc	Kingcan Holdings Limited , Fuzhen Group
INVENTIVE-IT.COM	Newgen Digitalwork	ANCO
INTEROIL.COM.CO	MultistateTax Inc	Gerson & Schwartz Accident & Injury Lawyers
MAFAS.COM	Carvimsa	Victorian Chemical
VIPAPPSCONSULTING.COM	simsekas, Inc	REPECHAGE
ZAIN.COM	M&BM, Inc	https://www.unterkofler.info
ACRONI.SI	iconinternational.com	www.automotiveml.com
EIGHTEENPK.COM	doversd.org	Mayco International
IBIZSOFTINC.COM	KohaFoods Hawaii	Castilla
LEGACYCLASSIC.COM	latamlex (gyg.local)	Deco Dental
AOSOM.COM	Znojma Czechia	Lidera Network
INCENTIVECONCEPTS.COM	Soleol	Central Plate Services Limitited
ALASEEL.COM.SA	Vennerhus Weine AG	Kobayashi
Wachusett School District MA	Grupo Via Argentina	Professional's Choice Sports
UAM	bridge-housing-corp	Encore Repair Services
Kettle, Sánchez & Co	forensicmed.com	Tavo Packaging Inc
Du	galileo.it	Wright Tool
PAN	Treetop Companies	Red Phoenix Construction
Gruenberg Kelly Della	ctfc.cat	New Toyo International Holdings Ltd
Superintendencia Nacional de Fiscalización Laboral	AsahiKASEI MICRODEVICES	juntalocal.cdmx.gob.mx
PATLITE	Wiraswasta Gemilang	

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。

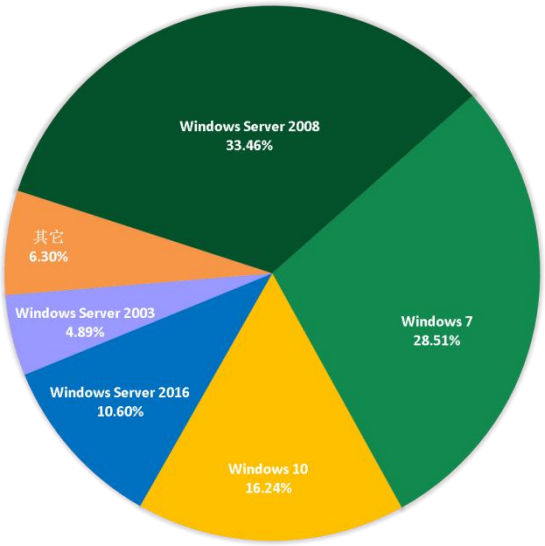

图 5 2025 年 11 月受攻击系统占比

对 2025 年 11 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。

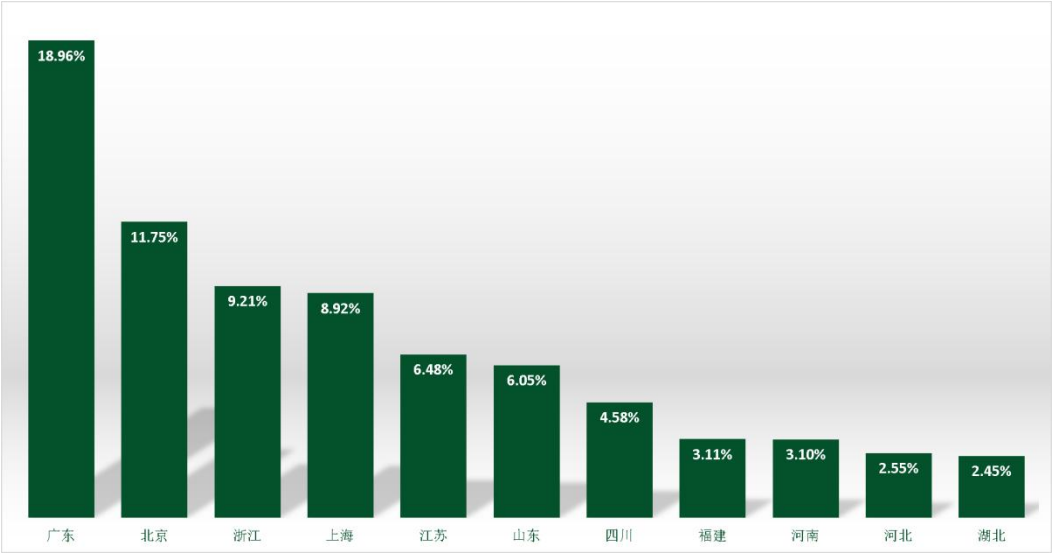

图 6. 2025 年 11 月国内受攻击地区占比排名

通过观察 2025 年 11 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。

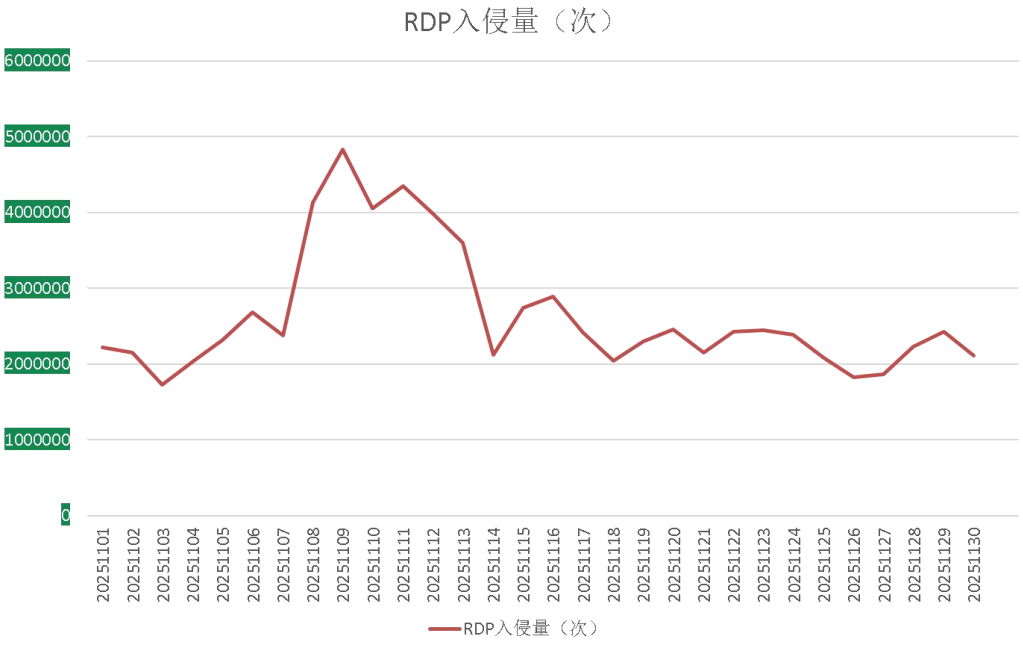

图 7. 2025 年 11 月监控到的 RDP 入侵量

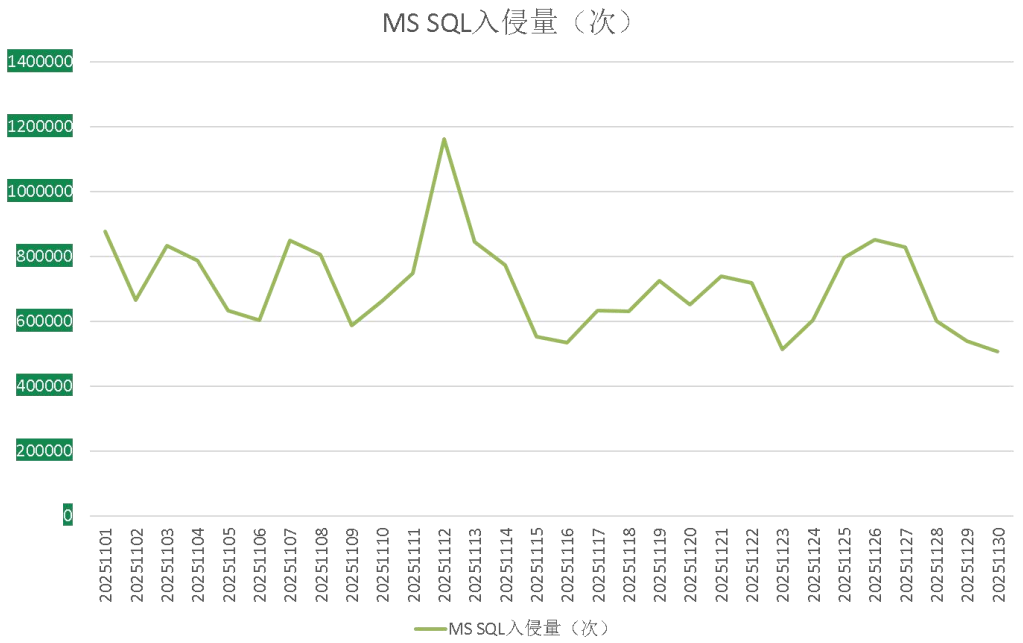

图 8. 2025 年 11 月监控到的 MS SQL 入侵量

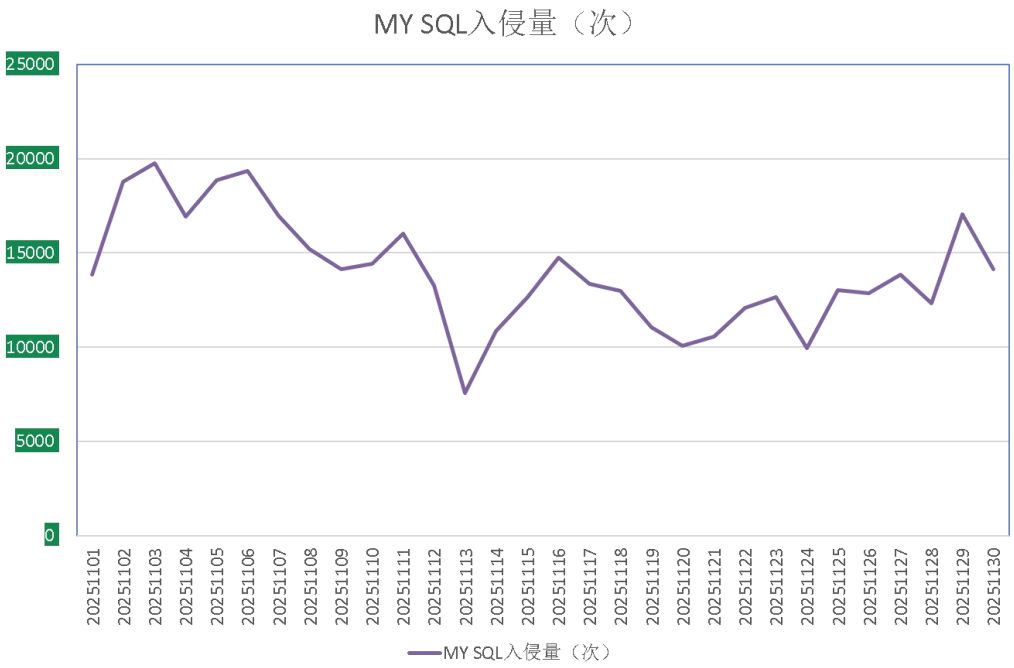

图 9. 2025 年 11 月监控到的 MYSQL 入侵量

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。
- **bixi**：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。
- **roxaew**：同 wax。
- **pdmkzc3cx**：属于 LockBit 家族，以 LockBit 家族泄露代码为基础开发的国内传播版本。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。
- **reco**：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。
- **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。
- **wstop**：属于 RNTC 勒索软件家族，该家族的主要传播方式为：通过暴力破解远程桌面口令成功后手动投毒，同时通过 smb 共享方式加密其他设备。
- **babylocker**：目前此扩展名反馈的用户均未提供溯源信息，暂未研判家族归属和攻击方式。
- **helper**：属于 TargetOwner 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与数据库口令，成功后手动投毒。

- ✧ **taps**：属于 Paradise 勒索软件家族，该家族目前的主要传播方式为：通过暴力破解远程桌面口令与数据库弱口令成功后手动投毒。
- ✧ **nezha**：同 reco

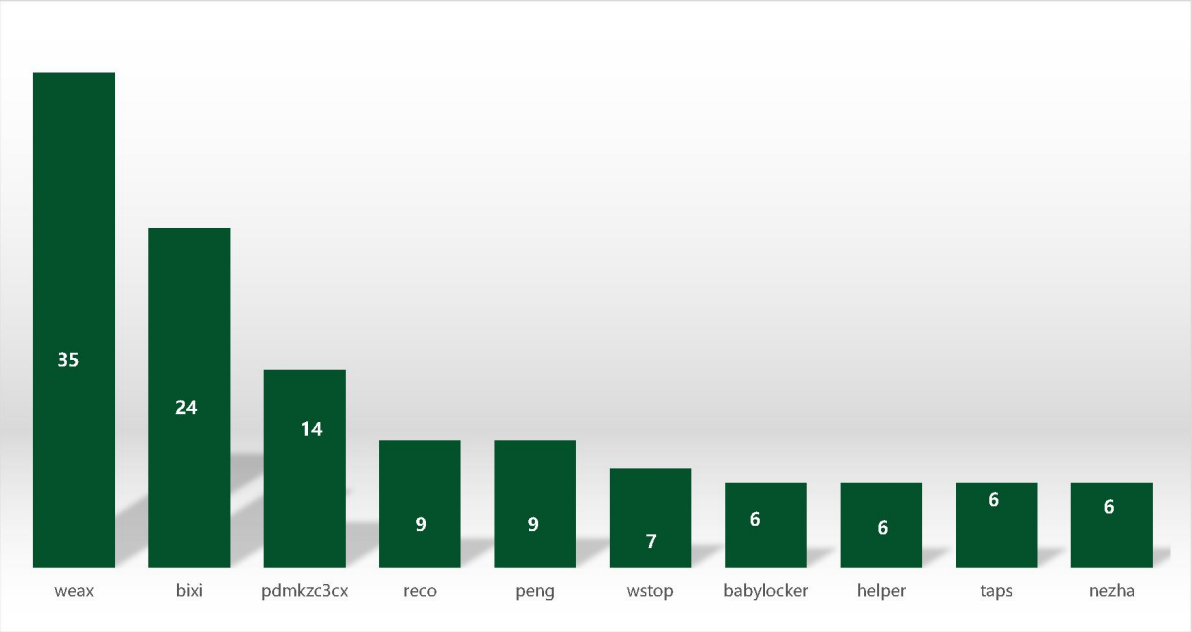

图 10 2025 年 11 月反病毒搜索引擎关键词搜索排名

解密大师

从解密大师本月解密数据看，解密量最大的是 Phobos，其次是 FreeFix。使用解密大师解密文件的用户，数量最高的是被 Crysis 家族加密的设备。

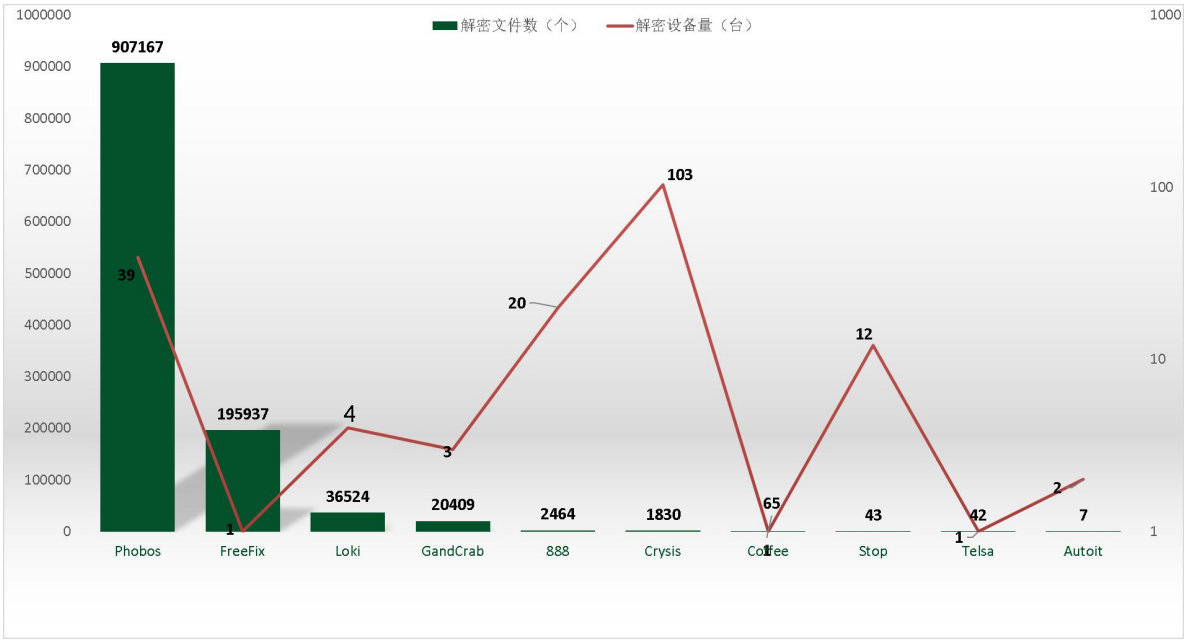

图 11. 2025 年 11 月解密大师解密文件数及设备数排名