

勒索软件流行态势分析

2025 年 8 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 反勒索服务已累计收到数万次勒索软件感染求助。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监测与防御，为需要帮助用户提供 360 反勒索服务。

2025 年 8 月，全球新增的双重勒索软件有 Desolator 家族，传统勒索软件家族新增 Cephalus、Pear、Charon 等家族。本月安全研究人员发现了首款使用 AI 模型驱动的勒索软件 PromptLock，使用 Go 语言编写，通过 Ollama API 与本地托管的 LLM 通信。

目前尚处在演进阶段的 PromptLock 勒索软件的攻击流程：

1. 生成恶意脚本

通过硬编码的提示词，利用大语言模型动态生成跨平台兼容的 Lua 脚本。这些脚本支持 Windows、Linux 和 MacOS 系统。

2. 枚举文件系统

生成的 Lua 脚本会遍历本地文件系统，识别并定位目标文件。

3. 检查目标文件

对已识别的文件进行内容分析，筛选出符合条件（如敏感数据或特定文件类型）的目标文件。

4. 数据外泄

将筛选后的目标文件通过隐蔽通道外泄至攻击者控制的服务器，可用于后续勒索威胁。

5. 文件加密

使用 SPECK 128 位加密算法对目标文件进行加密，使受害者无法访问原始数据。加密完成后，通常会留下勒索信息要求支付赎金。

此类勒索攻击手法由于 Lua 脚本的跨平台兼容性，攻击流程在不同操作系统中具有有一致性。借助 AI 的动态生成能力，可能使攻击行为更灵活，例如，根据目标环境调整文件筛选逻辑或加密策略。

360 安全大脑预测，后续随着 AI 能力的扩展，此类勒索软件在用户环境下可能的演进方向将包含：

1. 检测本地系统与软件环境，创建对应环境的漏洞利用脚本，进行提权与持

- 久化。
2. 针对本地环境中使用 Lua 脚本的游戏与应用软件进行白利用劫持，以绕过绝大部分安全软件检测。
 3. 针对自身创建脚本进行混淆，以及利用多种技术方式，尝试致盲、关闭本地的安全防护。
 4. 根据本地检测到的环境信息与对攻击目标的画像理解，生成可信度更高的、定制化的勒索信文件与电子邮件。
 5. 检测选择非工作时段且无用户操作的时机进行文件加密，同时删除各类企业备份数据，断绝目标及时止损的可能。

以下是本月值得关注的部分热点：

- 1 日产确认设计工作室数据泄露并遭 Qilin 勒索软件
- 2 Colt 在 Warlock 勒索软件拍卖文件后确认客户数据被盗
- 3 人力资源巨头 Workday 在 Salesforce 攻击后披露数据泄露

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 51.82%居首位，第二的是 Wmansvcs 占比 13.18%，LockBit 家族以 8.64%位居第三。

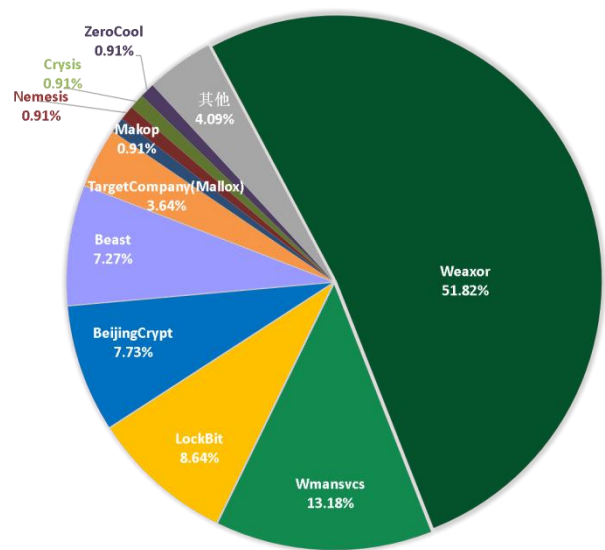


图 1. 2025 年 8 月勒索软件家族占比

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。

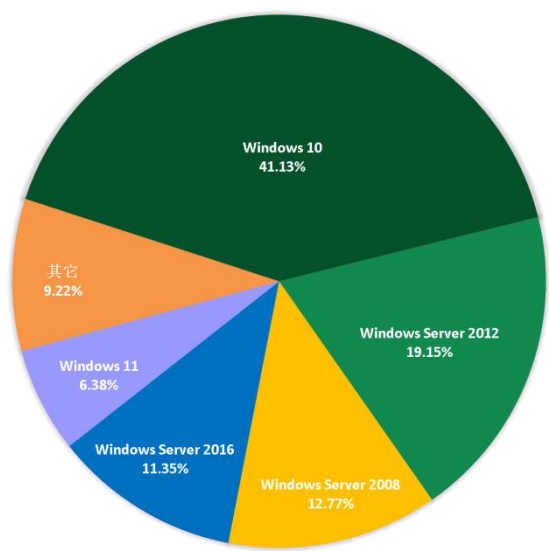


图 2. 2025 年 8 月勒索软件入侵操作系统占比

2025 年 8 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 小幅领先于服务器。

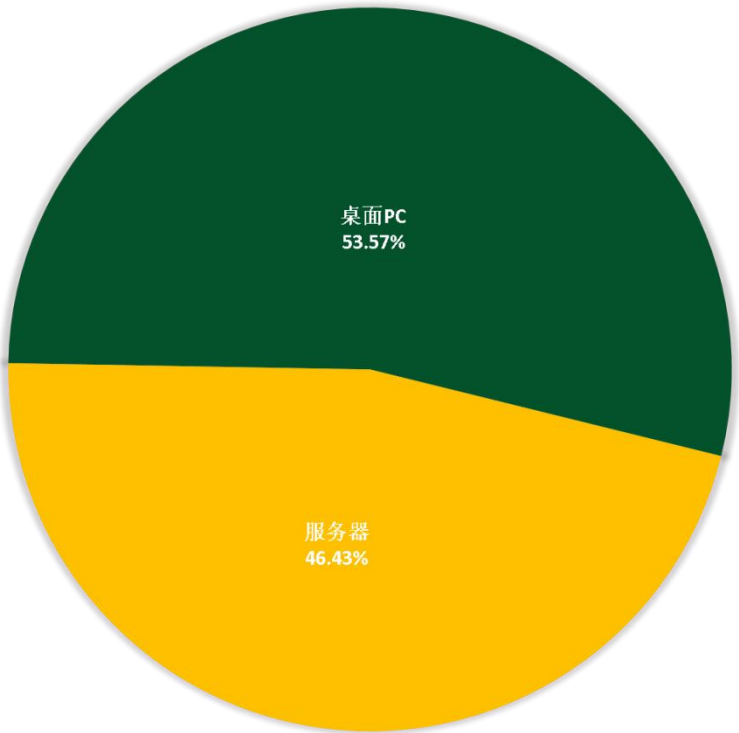


图 3. 2025 年 8 月勒索软件入侵操作系统类型占比

勒索软件热点事件

日产确认设计工作室数据泄露并遭 Qilin 勒索软件勒索

日产日本公司向媒体证实，攻击者在未经授权的情况下访问了其子公司 Creative Box Inc. (CBI) 的服务器，导致数据泄露。

2025 年 8 月 16 日，日产签约的设计公司 CBI 在其数据服务器上检测到可疑访问。该公司立即实施紧急措施，如阻止所有访问服务器等，以减轻风险，并向警方报告了该事件。

而 Qilin 勒索软件于 2025 年 8 月 20 日在暗网上的勒索门户网站上添加了 CBI 条目，并声称窃取了所有设计项目，还威胁要将其公之于众，使竞争对手获得优势。同时，攻击者还发布了 16 张被盗数据的照片，作为他们勒索的证据，这些照片描绘了 3D 汽车设计、电子表格、文档和汽车内部图像。

日产表示，目前正在对该事件进行调查，但已经证实了数据泄露事件。日产表示，泄露的数据只会影响日产，因为日产是 CBI 的唯一客户。因此，被盗数据不会暴露客户、承包商或任何其他公司或个人。

Colt 在 Warlock 勒索软件拍卖文件后确认客户数据被盗

英国电信公司 Colt Technology Services 证实，随着 Warlock 勒索软件团伙拍卖其窃取到的文件，该公司的部分客户文件已被泄露。这家英国电信和网络服务提供商此前披露其 8 月 12 日曾遭到攻击，但这是他们第一次确认数据被盗。该声明是在 Warlock 集团在 Ramp 网络犯罪论坛上出售他们声称从 Colt 窃取 100 万份文件之后发表的，这些文件以 20 万美元的价格出售，据称包含财务信息、网络架构数据和客户信息。

媒体已确认论坛帖子中列出的 Tox ID 与早期版本勒索软件团伙所使用的 ID 相匹配。虽然目前尚不确定本次对 Colt 勒索的赎金金额具体是多少，但此前该勒索软件团伙的

赎金诉求通常在 45 万至数百万美元之间。

人力资源巨头 Workday 在 Salesforce 攻击后披露数据泄露

在最近的一次社会工程学攻击中，人力资源巨头 Workday 被攻击者窃取了对第三方客户关系管理（CRM）平台的访问权限后，披露了此次数据泄露事件。8 月 15 日，该公司透露，攻击者可以访问存储在受损的 CRM 系统上的一些信息，并补充说没有客户账户受到影响。然而，目前此次事件中被窃取的一些业务联系信息已经曝光，包括可用于后续攻击的客户数据——其中重要的是一些常见的商业联系信息，如姓名、电子邮件地址和电话号码，这些数据可能会进一步推动攻击者的社会工程骗局。

在发给可能受影响的客户的另一份通知中，该公司补充说该漏洞大约是在 8 月 6 日发现的。攻击者通过短信或电话与员工联系，假装来自人力资源或 IT 部门，试图诱骗他们泄露账户访问或个人信息。虽然该公司没有直接确认，但据媒体了解，本次事件可能是与 ShinyHunters 勒索集团相关的一波安全漏洞的一部分，该勒索集团通过社会工程学和语音网络钓鱼攻击 Salesforce CRM 实例。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

sadklajsdioqw@proton.me	hyebwma@protonmail.com	alekstraza@bigmir.net
nobackups@mailum.com	hsbwabwy@xmpp.jp	BM-2cXFq2HvWpBCesbm7F7hw7MBkTaalyfwW v@bitmessage.ch
pompey@tutanota.com	Decryptionhelping@aol.com	cephalus@onionmail.org
pompey@cock.li	Helpingdecryption@cyberfear.com	bonar.c@aol.com
recovery2@salamat.i.vip	grepmord@protonmail.com	peruginos@aol.com
recovery2@amniyat.xyz	reopening2025@gmail.com	elliott.i@aol.com
realsupport@bigmir.net	reopening25@gmail.com	pilondru@aol.com
China.helper@aol.com	shirleyrichardsoncrpty@onionmail. org	demetrius.bassell@aol.com

China.helper@india.com	Ionia@mailfence.com	payransom@qq.com
pear@onionmail.org	austinmecca@onionmail.org	PAYKTER@gmail.com
dongmin.liu@earlylight.com.hk	shadowmatrix@onionmail.org	Answer:Encsgi2@gmail.com
zoomnism@protonmail.com	dat@mailum.com	veronica.stein1998@onionmail.com
recovery1@salamati.vip	datret@tuta.com	jacobmccole1967@onionmail.com
recovery1@amniyat.xyz	Johnycryptor@hackermail.com	compsupp@techie.com
kixonw@gmail.com	Johnycryptor@india.com	paymeuk@consultant.com
kixonw@tutanota.com	partfile@airmail.cc	Serina5Murrock@email.com
backups1@mail2tor.co	worm01@india.com	recovery7@salamati.vip
4569f6322bc3b22e9@proton.me	BQTlock@tutamail.com	recovery7@amniyat.xyz
MariaJTipton@protonmail.com	samurai@aolonline.top	deepwhale9@outlook.com
364482@jabber.hot-chilli.net	bitpandacom@qq.com	deepwhale9@hotmail.com
supp@msg.ws	btcduess@outlook.com	jessicarnels2025@outlook.com
OopsCharon@proton.me	duesbtc@2mail.co	ithelpnetwork@decorous.cyou
restoring_sup@india.com	NeZhaderyption@mailum.com	ithelpnetwork@wholeness.business
restoring_sup@computer4u.com	NeZhaderyption@cyberfear.com	miragesity@hotmail.com
restoring_reserve@india.com	kayla7tzpntompson@aol.com	lilyb6esdgarcia@aol.com
traders@mailum.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，勒索软件带来的数据泄露风险也越来越大。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）。

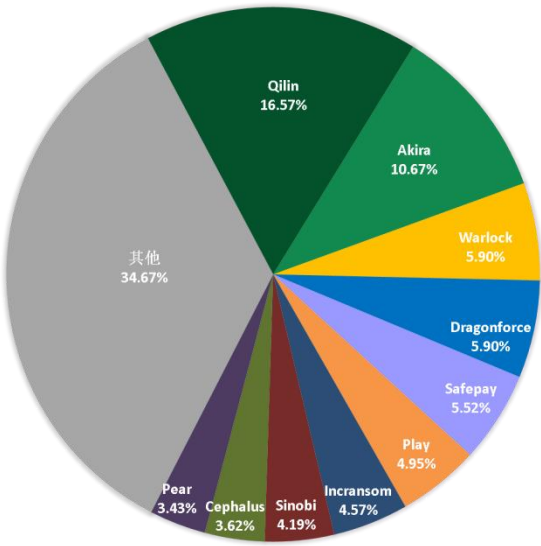


图 4. 2025 年 8 月通过数据泄露获利的勒索软件家族占比

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。

本月共有 519 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/企业遭遇了双重勒索/多重勒索，有 12 个组织/企业未被标明，因此不在以下表格中。

L&S Proline	EUROFILM MANTZAPHSE	Travancore Analytics
Tecnología Especializada Asociada de México	hmsaojose.com	Rite Track
ESIC_TR	Bizcom Electronics	agrofair
Tri Thuc Software	abfe	empur
Construcciones Sala	lee-irvine.com	Woodside
ABM Wireless INC	haaker.com	Bondtech
Hilco Metal Building & Roofing Supply	insoca.es	Wytech Industries
Park Country Club	netfusionconsulting.com	GWU-Umwelttechnik GmbH
Toowoomba Friendly Society Dispensary	garnertrucking.com	Microcosm
Provalve Armaturen GmbH & Co. KG	idscorporation.com	TRS Industries
Engineered Components	RA Services	Sterling Card Solutions
sandersonmanagement.com	Steel Encounters	Geotec
OB GYN Associates	LandWorks	SPEEDLOGISTIK
atlanta neighborhood charter school	RAVEN Mechanical	The Law Offices of Hicks & Demps
lipcare.de	Advanced Blending Solutions	Safty First
companionsandhomemakers.com	HK Hardware & Engineering	Aurora Air Products
camaravalencia.com	Elkhart Independent School District	Sweetener Supply
dasmeshschool.com	Netstar_South_Africa	ESD
zanettisrl.it	Expert E-commerce GmbH	Architectural DesignWest
uwock.ca	Florarte	Spring Footwear
hardwicktactical.com	Din Bolig	The Law Company
templemanu-el.org	DUC App: Global Money Movement, Simplified	Anderson Packaging
thecelestehotel.com	southweststone.net	Atlas Transfer & Storage
allphaselandscape.net	Burger & Brown Engineering	Insero & Co. CPAs, LLP
ibew1547.org	Mutual Screw & Supply	Louis Tieu DDS MD
ogdenpubs.com	Horizon Hydraulics	Community Services of Missouri
Loyola College	Stewart Home School	Chemtron RiverBend

RMO	T&D Engineers	Alascom
www.sbd1.net	TRANTRONICS	L3Harris Technologies
BÜCHNER BARELLA Holding	Mediate Management	St Thomas More Catholic High School
The Fredericks	MPOWERHealth	getech.com
BDO Perú	childrenscouncil.org	jtekt.eu
Manesa	Nicke	formacompany
One-LUX	Bobcat Central	Howard Financial & Associates
Shropdoc	Electro-Tech	European Business Server Cluster
Shelbourne Accountants	Rare Editions	NEAS
Delta Information Systems	True World Group LLC	RHI Supply
Town of Chatham, MASSACHUSETTS	Inotiv, Inc	CFI Tire Service
CPK Interior Products Inc	Outdoor School	Wstg-steuerberater.de
gmcontractinginc.com	Cain Electric	Drive & Shine
Kafka Conveyors & Equipment Inc	Maxell Asia	Viking Automation
TOYOTA ASIA TOYOTA INDIA	albertaindustrialcontrols.com	Dyson Corp.
decor-metall.de	listgrove.com	mauilodging.com
Firelands Scientific	transelectric.co.il	CIMEXSTEEL.CZ
summitcollege.edu/USA/370GB	batemangroundworks.co.uk	Pacific HealthWorks
Colorado Health Network Inc	godbyhearth.com	La Perouse
Texas Pregnancy Care Network	Doctocliq	multichem.net
wilderlawfirm	Uganda Electricity Transmission Company Limited	Admiral Gaming Network
CoCo Yachts	apderm.com	Main Electric Supply Co.
TRAF Industrial Products Inc	infoniqa.com	shinko plastics co. ltd
climaxportable.com	Palmgold Management Sdn Bhd	Belmont christian college
The Smile Spa	Advanced Security Systems	ryeco.com
Grupo DIRIA	IQgistics	lpco.co
allmaxnutrition.com	Escauto Centro Automotivo	eyeqmonitoring.com
Weathercraft Companies	Justicia Penal Militar	avosinamed.com
Dance Brothers	SEGUROS AMÉRICA	camdon.ca
ZCORP	Seoul Guarantee Insurance	lodipd.org
Echo	International Freight & Commerce	csrepair.com
Ben's Asphalt	Welcome Financial Group	studebakersubmetering.com
Baycoat	Matiss	sotaconstruction.com
brebeuf.org	Rehabilitative Health Svc	azurewave.com
singersf.com	gmtaconline	Prime Beverage Group
dafo.se	woodbourne	The Gisborne Group
Inox Laghi	STRGOME	Neway Valve
Sterlings Accountancy Solutions	argeninta	BRIDGEWATER ASSOCIATES
Hanson Chambers	houara	MAGELLAN FINANCIAL GROUP
Aldagi	houxt	ONEX CANADA ASSET MANAGEMENT INC
Logan & Mencuccini	getdomain	TSAI CAPITAL
Edward J McKarski	kipl	MIZUHA FINANCIAL GROUP

Banville Wine Merchants	nszi	Triveneta Vetro
Galaxy Freightline	accsnet.com	PANSARD & ASSOCIES
Premier Realty Group	advion.com	Jamco Aerospace
Motor Controls Inc.	mysecop.com	Emprise
Sneg Proprete	atcmanufacturing	Brad's Bedding Plants
Sika Footwear	orange.com	The Magni Group
Springs Christian Academy	anthembio.com	Kengen
txpregnancy.org - Fake Abortion Clinics Exposed	syspro.com	ferrocortes
Town of Vienna, VA	brightwork.com	MGM Transformer
Lewis Baach Kaufmann Middlemiss PLLC	starsalliance.com	Payme Ltd
Lee & Associates	sipecom.com	LEARN is a Regional Educational Service Center
Sherman, Silverstein, Kohl, Rose & Podolsky, P.A.	wytechnology.local	CLEARSYNTH LABS LIMITED
Guerrero Mears LLP	webcids.com	PROMOSFERA S.r.l. promosfera.com
LPL Financial	rougine-mfg.com	Cash and carry - COSAEN GRUP
K Strategies Marketing and Public Relations	magcpa.com	KINAS SOLICITORS kinas.co.uk
BAR Architects & Interiors	wfd2027uae.ae	Quality Data Service, Inc.
SystemExec Co., Ltd.	tagorg.com	Dragonfly CO. LTD dragonflygame.com
CareSTL Health	hitachi-hta.com	CILI
akd-ekbo.de	primrose.com	CHABAA BANGKOK
jphrs-waghaeusel.de	clearybuilding.us	F&P Georgia Mfg Inc
parksidegroup.co.uk	colt.net	Afpa
ferienwohnungen.de	Panorama	CK Power Public Company Limited
phillips66lubricants.com	mycpaconnection.com	TANI & ABE
faltner.de	Hytrol	Harinera del Valle
optimosa.com	CMS Legal Services EEIG	Metro Heating
rivertoncabinets.com	THE MILLENNIUM GROUP	Consumer Electronics & Computers Retail Retail
schliessmeyer.de	VINSON & ELKINS LLP	Brunton-Shaw
gibbswire.com	ethicalpackaging.co.uk	EMMCORP.COM
hydrometrics.com	Xperthair	Heart of America Medical Centr (HAMC)
www.nuggetent.com	Pequannock Township School District	Diversified Project Services International
Accident Injury Solicitors	MJets	cibraco
marlboroughpartners.com	Töller	Neff Specialties
Security First Credit Union	Grand Rapids Controls	Hamilton Park
Huntwood Industries	ACMARK	Brookside Homes
Pocono Farms Country Club	ZMM	Clarkston First Baptist Church
nrlassoc.com	DAT AUTOHUS AG	Bromack Manufacturing

airfastindonesia.com	Philadelphia Investment Partners	Ail Hospitality Group
Van Hook Dental Studio	Voltus GmbH	Twin Oaks Presbyterian Church
Exel Composites	BRIJU.PL	ThinkBig Health Care Solutions
tricol76.org/USA/180GB	MYVISAJOBS.COM	Tas Nz Bay Limited
Aroeira Salles Advogados	SFA Engineering	Alt Vision
Bolt Nut Manufacturing	Barlows Electrical	Preferred Homes Realty
Dynacast	marma.com.pl	The Job Shop
台灣東洋國際儀表股份有限公司	Morgenstern AG	The Danvers Law Offices
Wine Works Australia	Karndean International, LLC	Kalchschmid GmbH & Co. KG
DLCOSMETICS O. E.	Maselli Misure S.p.A. Information	U.S. Battery
diversifiedcpc.com	Peggy Sage	JWiz
swanforlife.com	Norwest Venture Partners	Hankin & Mazel, PLLC
Colabor	L-Pimenta (etdeletronic)	Garrison Law Firm
medosweet.com	www.captrade.com	ridgefield.org
Graphite Construction Group	liabergamo.it	HCK Capital Group
Prosegur	ABcom	Kingsford Development
Dottori Commercialisti Associati	Greenscape Pump Services	melland.bright-futures.co.uk
George Haney & Son	eShipGlobal	Carrollton Ear Nose and Throat
Selartex	NextLabs	Newton Electrical Contractors
GEA Consulting Engineers	Ranshu, Meridian Auto Parts, Visionaire	aym.com.mx
www.ecodemolizionisrl.com	Erdy McHenry Architecture	ppmrecruit.com
Inicio - Ganadería Revuelta	smefazur.fr	Origene
Wier Boerner Allin	Avv Emilio Marco Casali	alpresor.se
Quadrangle Imaging Center	Immigration Advice Service	ruff.com.br
Mark Edward Partners	ksubsea-group	www.diethelmtravel.com
Carmichael Engineering	Lundberg Design	Bucks County Opportunity Council, INC.
Hill Peterson CarperBee & Deitzler	Rusin Law	Scania.com
Exotherm	Manhattan Retirement Foundation	easternadjustment.com
Hogan Construction Group	Barbas Nunez Sanders Butler & Hovsepian	Phoenix Lighting
Fullcolour.com Limited	Comprehensive Pain Centers	Backstage Library Works
Clinical Diagnosis	J Derenzo	White Horse Packaging
www.wyongleagues.com.au	One Way Solutions	Terillium
Mobal Trucking	TELACU College	Weisman Children's
Jack's Lawn Service, Inc.	ECM Consultants	bw-lv.de
www.greneker.com	Advanced HPC	K2L
www.gillette-ac.com	Charak Center for Health	Wedlich
fiermann-eller.de	ffs.com	Koenig Hausverwaltung
TechSourceOne IT Solutions Provider	Ahtna Incorporated	Frontline Bioenergy
InEar hear the difference	Cooks County Family Health	Banco Guanabara
Krewett	FranceLink	Aggressive Air Compressor & co

IT-Welt und Telekommunikation verschmelzen	Cevital	DIMERCO
Tomb Multimedia Productions	Litchfield Cavo LLP	BIG ROCK RESORT
Sonitrol Security Solutions (SecureFL)	Box Elder County	MONTE-CARLO
Dualinfor hito inovation	Hygrade Components	gid-it.de
Spohn + Burkhardt GmbH & Co KG	Eagan Insurance	Clemens Construction
Colmar Industrial Supplies	Energy Developments	Pitman Farms
PLN	Harmony Electronics Corp	Onegolditalia.it
Huron Regional Medical Center	EB Farmaceutica	www.pefco.com
Sofo Foods	bvasd.net	Cookeville Regional Medical Center
seabridge.eu+efico.com	northernconstruction.com	Lincoln Law
Blazer Building	syncadd.com	cadex.com
Burt Process Equipment	venturecreditunion.com	envac.es
Nissan CBI	Haeger & Schmidt Logistics	fortsmithschools.org
Universal Group For Engineering and Consulting	Assisted Living Pharmacy Service LLC	Meissner Fenstertechnik
All Truck Transportation Co	Epperson Law Group	chamberlainhuckriede.com
Ambitek	Nutis Press	Hölscher Holding
Fullerton Surgical Center (FSC)	Trans-Tex	Herrman Law Firm
Ocean Edge Resort & Golf Club	MMA TRANSFERS	Guyana Sugar
CBG Surveying Texas	burmann.de	Great Lakes Carpet &Tile
welldone.com.tw	Çağrı Group	Radford City Schools
Omega Global Technologies	MBM Intellectual Property Law	Franklin Pierce Schools
awmedicalvillage.org	City of St Paul	White Coffee Corporation
DAOR E&C Co., Ltd	The Scharine Group	Framon S. p. A.
Greater Pittsburgh Orthopaedic Associates	Bluewater Yacht Sales	PK Contracting

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。

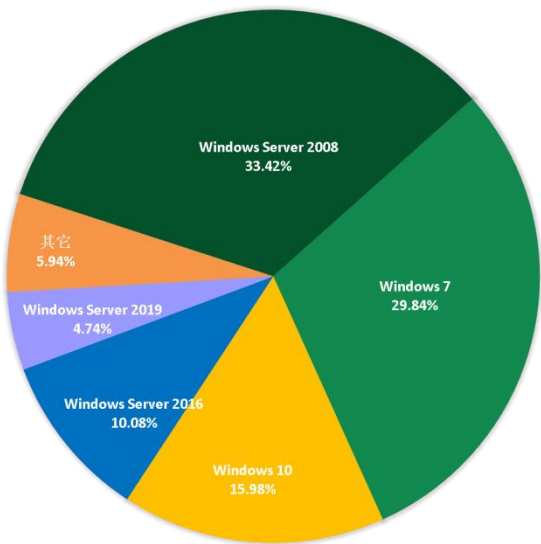


图 5 2025 年 8 月受攻击系统占比

对 2025 年 8 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受攻击的主要对象。

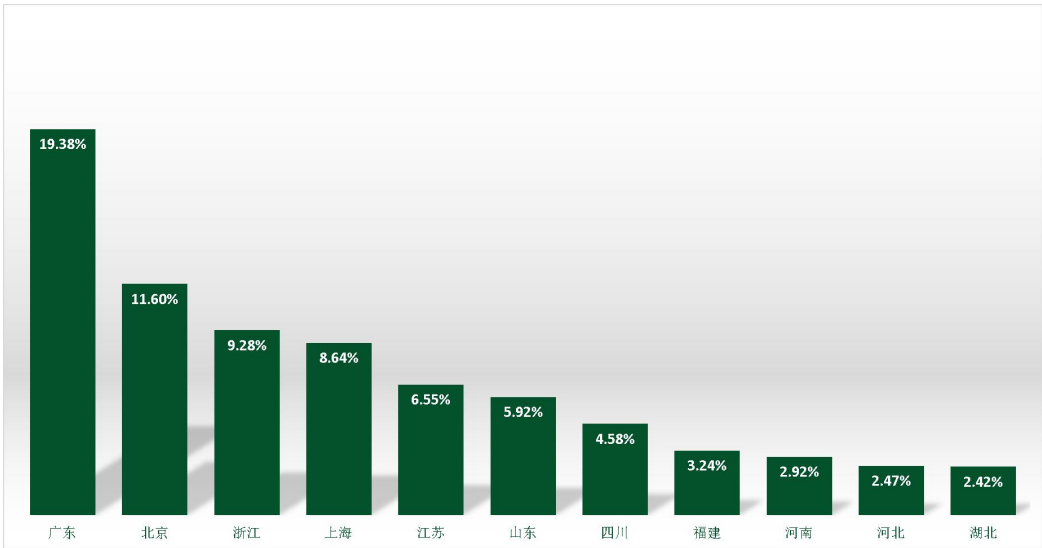


图 6. 2025 年 8 月国内受攻击地区占比排名

通过观察 2025 年 8 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。

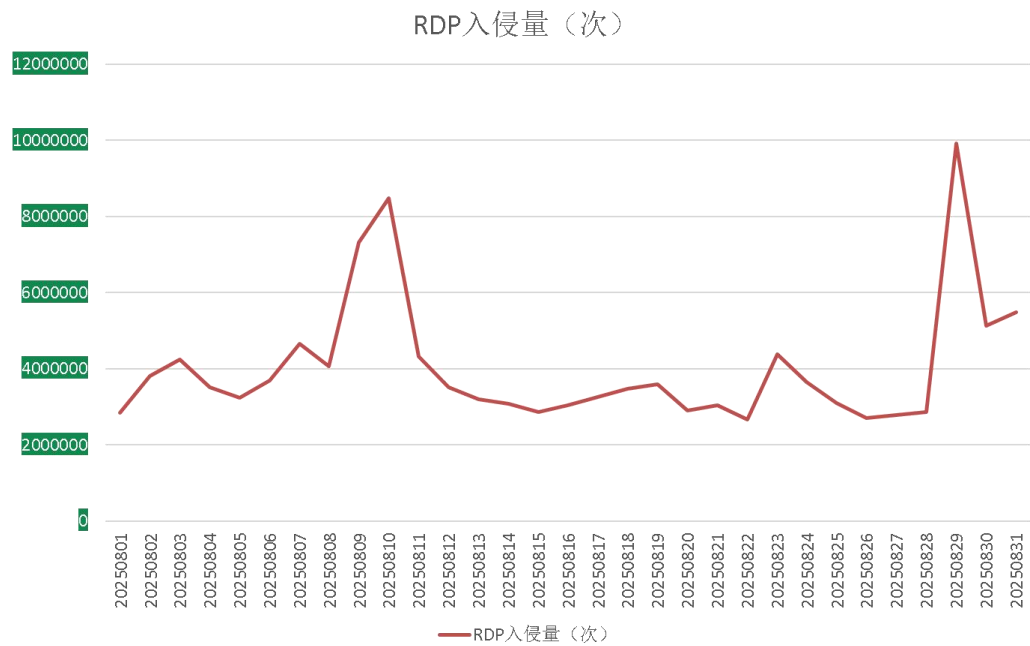


图 7. 2025 年 8 月监控到的 RDP 入侵量

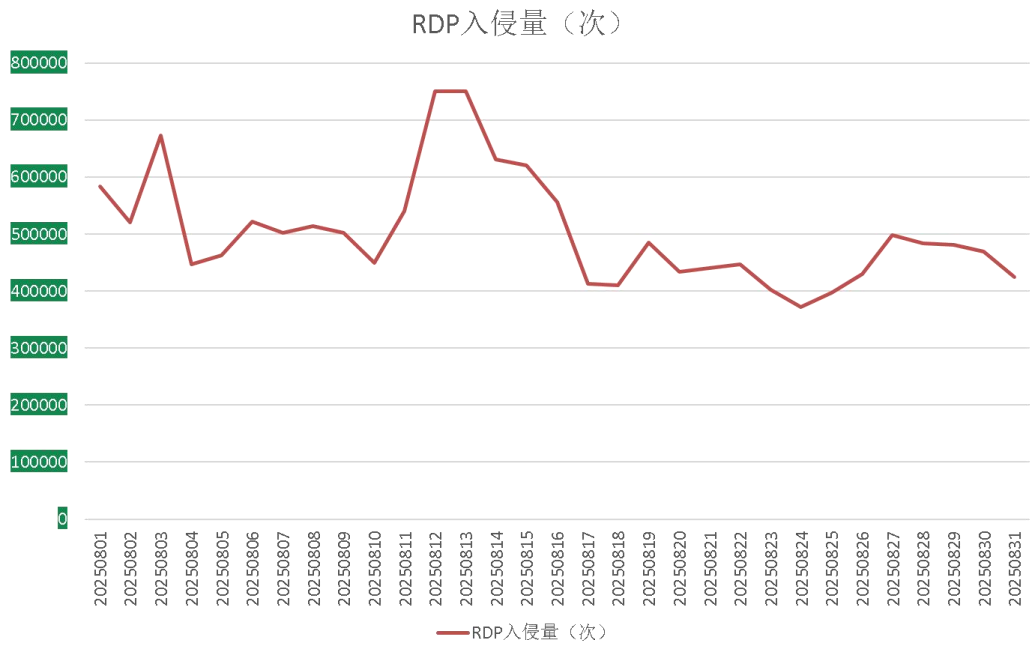


图 8. 2025 年 8 月监控到的 MS SQL 入侵量

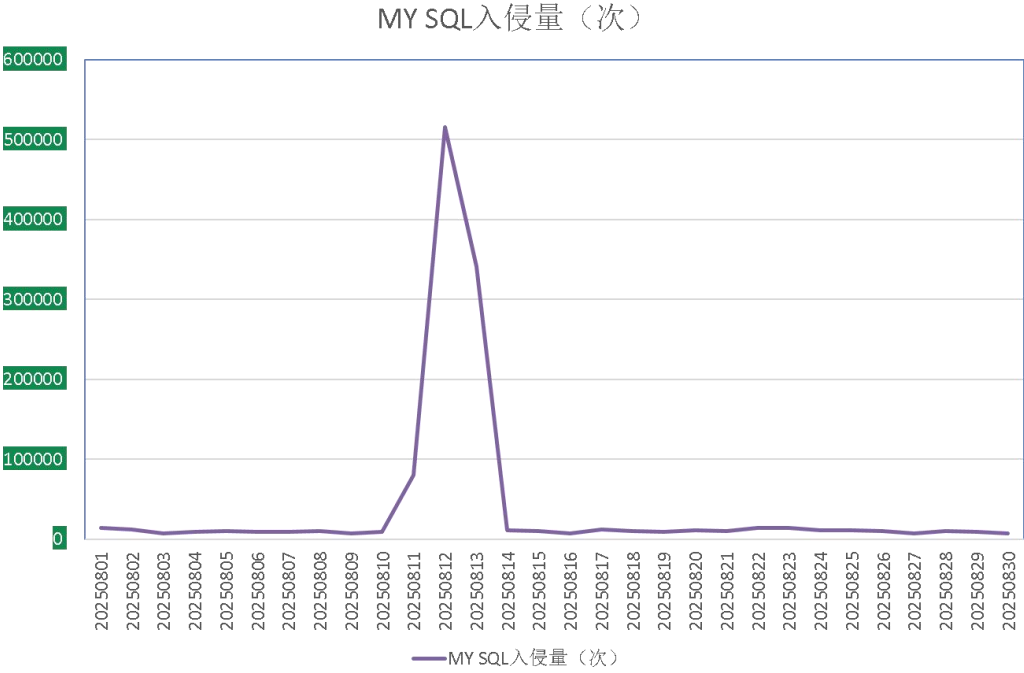


图 9. 2025 年 8 月监控到的 MYSQL 入侵量

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。

✧ roxaew

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 加载攻击载荷并与安全软件进行内核对抗。

✧ weaxor

同 roxaew。

✧ 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。

✧ baxia

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。

✧ bixi

同 baxia。

✧ wxx

同 roxaew。

✧ enzo

属于 ZeroCool 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或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。

✧ 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。

✧ **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。

✧ **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。

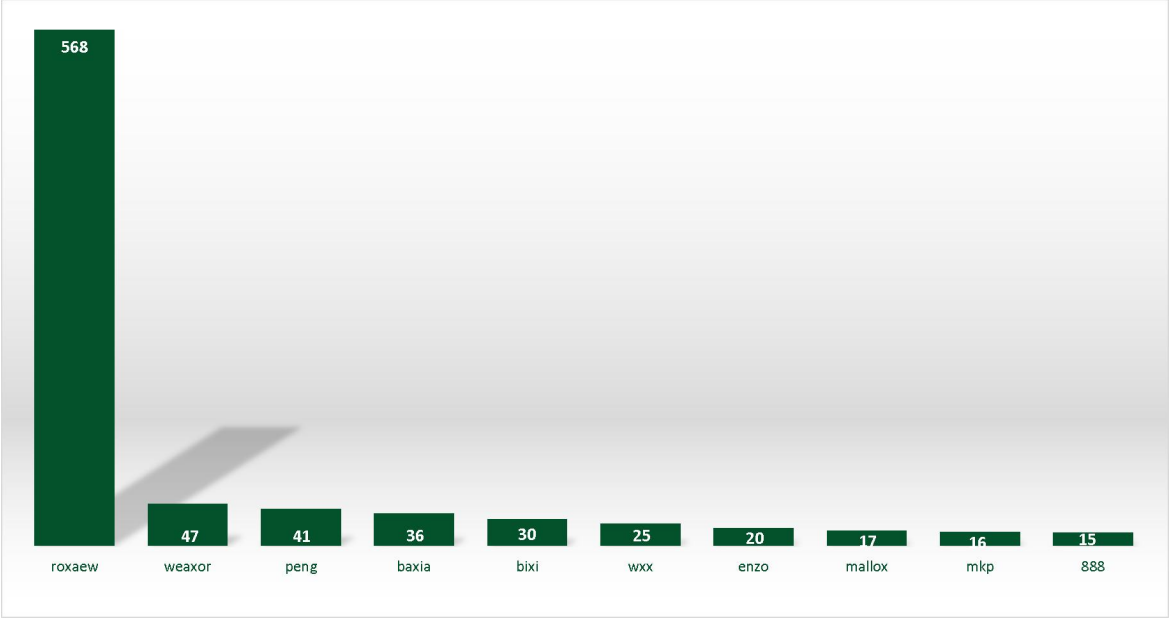


图 10 2025 年 8 月反病毒搜索引擎关键词搜索排名

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 Loki。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。

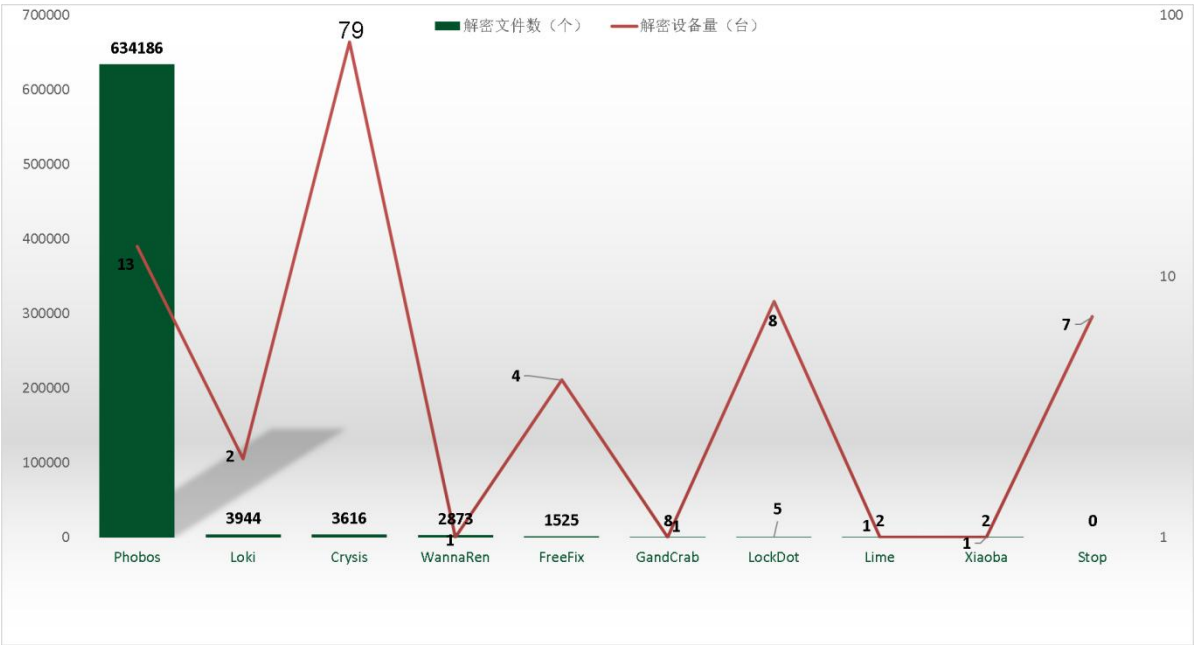


图 11. 2025 年 8 月解密大师解密文件数及设备数排名