

2026 年 8 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，勒索金额在数百万到近亿美元的勒索案件中持续出现。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。

2026 年 8 月，全球新增的双重勒索软件有 Falcon、Panzer、Majinahanashi、Storm、L group 等家族，传统勒索软件家族新增 GoldenWoolf、Kreepr、GmCry、Kimo、Fiasco 等家族。

本月仅在国内传播的 SnowSoul 家族的变种恢复传播，360 对此家族的部分版本支持解密，需联系 360 反勒索团队进行人工鉴定。

以下是本月值得关注的部分热点：

- ① 国家计算机病毒应急处理中心通报新型“Sorry”勒索病毒
- ② C10p 勒索团伙利用 PTC Windchill 漏洞入侵全球数十家制造业
- ③ Krybit 勒索组织集中攻击亚太及中东多个目标

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。

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占比达到 57.52%，而未正常启用 360 安全软件的设备数量则占比 20.33%，安装了其他安全软件的设备则占比 22.15%。

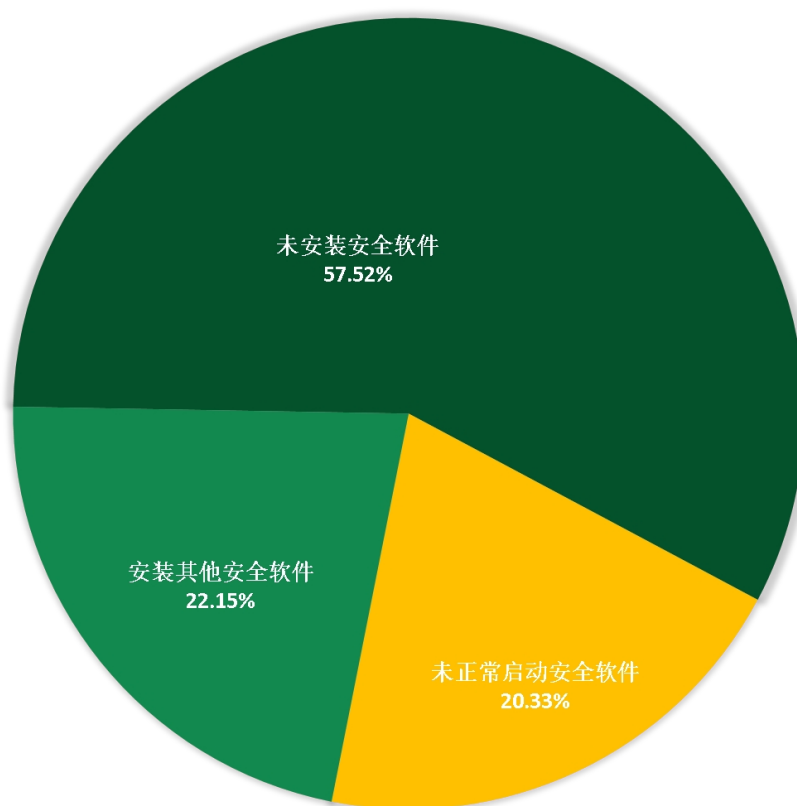


图 1. 2026 年 8 月勒索软件中招设备中安装的安全软件占比

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 65.74%居首位，第二的是 BrzCrypt，占比 11.11%；LockBit 家族以 5.56%占比位居第三。

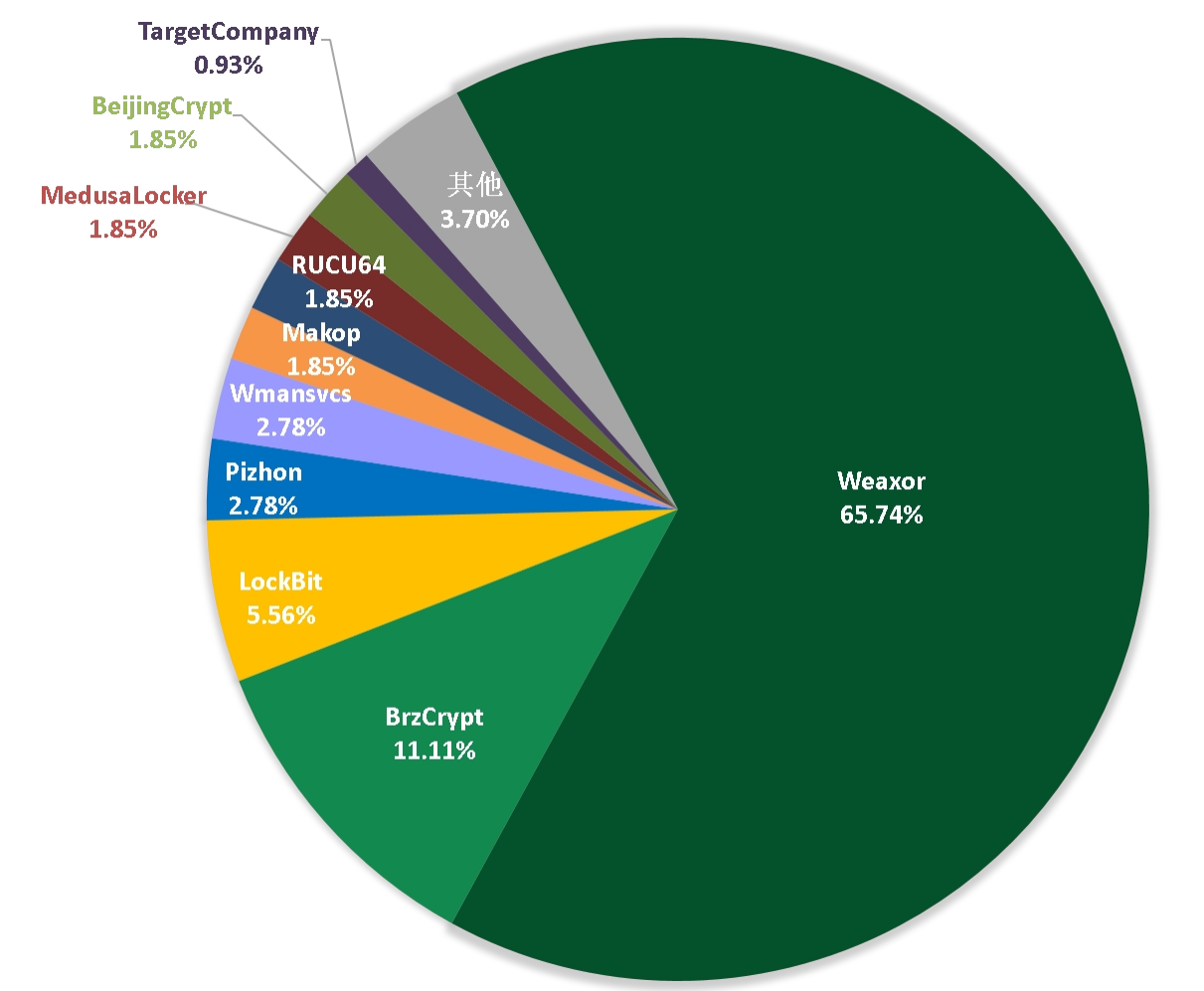


图 2. 2026 年 8 月勒索软件家族占比

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。

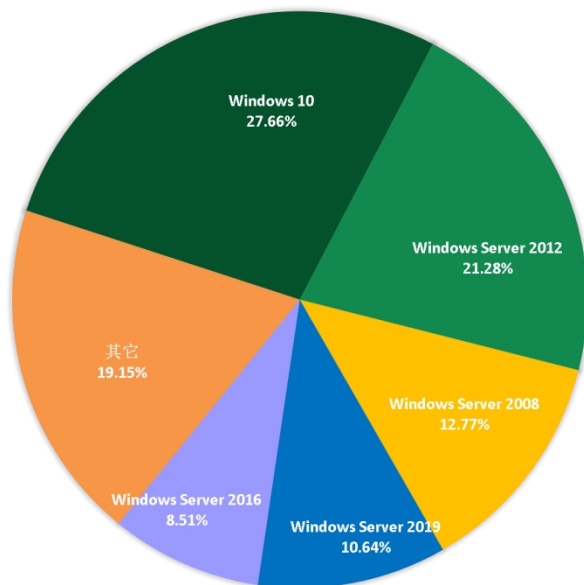


图 3. 2026 年 8 月勒索软件入侵操作系统占比

2026 年 8 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。

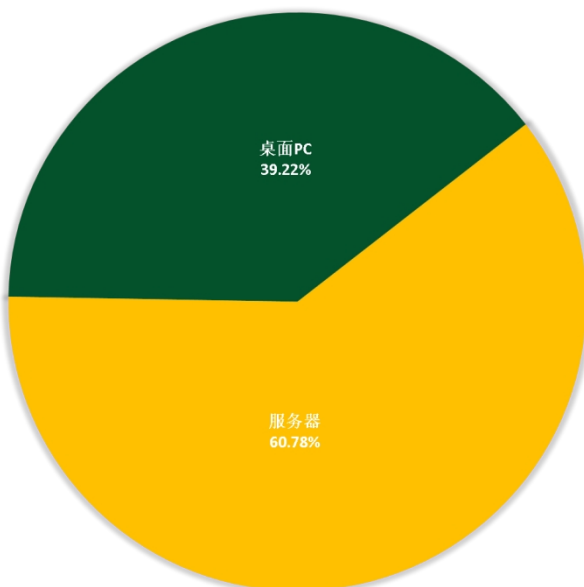


图 4. 2026 年 8 月勒索软件入侵操作系统类型占比

勒索软件热点事件

国家计算机病毒应急处理中心通报新型“Sorry”勒索病毒

2026 年 8 月 10 日，国家计算机病毒应急处理中心和计算机病毒防治技术国家工程实验室联合发布预警报告，通报在我国境内发现多起新型“Sorry”勒索病毒攻击事件。该病毒归属于 2026 年新出现的勒索病毒家族，由攻击者使用 GO 语言编写，主要针对在互联网上暴露的 Linux Web 服务器。被感染后，用户重要文件被加密并添加“.sorry”后缀，攻击者同时在主机上留下勒索信，要求用户下载加密通信工具与其联系。据披露，攻击者利用 WebProscPanel 授权问题漏洞（CNNVD-202604-5641、CVE-2026-41940）获取服务器管理权限，投放病毒后伪装成 sshd 进程运行，随后终止数据库、安全防护及备份服务，窃取数据并进行文件加密，最终通过 SSH 弱口令向内网横向扩散。

该病毒经过 Garble 混淆处理，符号破坏率超过 99%，具备 SSH 自动化横向移动、混合加密、反响应清理、Tor 隐蔽通信等完整攻击能力，对内网服务器集群威胁极大。国家计算机病毒应急处理中心明确表示，在没有解密密钥的条件下，被加密的数据暂时没有可靠的恢复方法。

360 早在今年 4 月已发布 Sorry 家族 Windows 版本的深度分析报告并预告了 Linux 版本的存在，5 月其 Linux 版本率先在境外大面积爆发。随着 AI 技术的发展与深度参与攻防，越来越多的跨平台攻击成

为真实威胁。该事件影响范围涉及国内主流 Linux 及信创系统，是目前国内针对 Linux 服务器最具威胁性的新型勒索病毒之一。建议相关单位及时修补漏洞、强化口令管理、启用离线备份，并避免使用来源不明的解密工具。

C10p 勒索团伙利用 PTC Windchill 漏洞入侵全球数十家制造企业

2026 年 8 月下旬，据台湾 iThome 及多家安全机构报道，勒索软件团伙 C10p 被指专门针对 PTC 公司旗下 Windchill 与 FlexPLM 产品线开发定制化 WebShell，利用高危漏洞 CVE-2026-12569 (CVSS 评分 9.3) 实施大规模入侵。该漏洞源于 Windchill 发布模块缺乏身份校验机制，攻击者通过组合利用未授权信息泄露与反序列化漏洞，无需任何认证即可直接获取系统权限，并在受害系统植入定制化 JSP 后门，实现长期驻留。其攻击链路涵盖精准资产测绘、漏洞利用、数据窃取与勒索施压，隐蔽性极强，传统安全设备难以检测。

据 C10p 团伙自曝及多家安全厂商分析，此次攻击已波及飞利浦、壳牌、通用电气、Fiserv 等全球近 50 家制造企业，受影响版本覆盖 Windchill PDMLink 11.1 至 13.1 及 FlexPLM 全系列。与 C10p 惯用的加密勒索手法不同，本轮攻击主要以窃取核心知识产权数据（如三维数模、工艺文档、产品设计资料）而非加密文件为主，部分企业早在 8 月 19 日、20 日便已收到勒索通知。该事件表明，工业软件供应链漏

洞正成为勒索团伙规模化渗透制造行业的新型突破口，对航空、汽车等高度依赖 PLM 系统的企业知识产权安全构成严重威胁。

Krybit 勒索组织集中攻击亚太及中东多个目标

2026 年 8 月底至 9 月初，新兴勒索软件团伙 Krybit 集中现身，一周内连续公开声称攻击多个亚太与中东目标，攻击节奏密集、行业跨度大。据安全情报机构 DeXpose 及多源监测，9 月 1 日 Krybit 攻击泰国豪华地产开发商 Reignwood Park Thailand，威胁泄露其敏感数据；同日还被指攻击科威特阿拉伯海上石油运输公司，危及能源航运领域敏感信息；随后又瞄准印度 Vedantaa 医学科学研究院，对患者与科研数据安全构成威胁；9 月 2 日进一步攻击印度泰米尔纳德邦 IT 企业 Southsign Technologies。此外，8 月 28 日 Krybit 还曾攻击泰国 Sunsea 塑料制造公司并泄露数据。

Krybit 的快速扩张呈现出典型的勒索软件即服务（RaaS）扩散特征：以数据窃取与公开泄露为主要施压手段，集中打击防御相对薄弱的中型组织，并在短期内通过多起公开声明制造声量、扩大影响力。从受害企业分布看，该组织明显聚焦亚太地区，泰国、印度为重灾区，行业覆盖房地产、医疗、能源运输、制造业与 IT 服务，反映出其对高价值数据资产与供应链环节的偏好。安全研究人员提醒，泄密网站上攻击者单方面公布的受害者名单无法逐一独立验证，但 Krybit 短时间

内多点开花的态势值得持续追踪，相关地区企业应加强凭据治理、离线备份与外部暴露面收敛，防范其数据勒索攻击。

黑客信息披露

本月收集到的黑客邮箱信息如下：

e.jayong@proton.me	RansomHrkwnCS0e5@gmail.com	qdtikdfoplmcv@proton.me
lena.weiss83@outlook.com	dbger@protonmail.com	brcd5102@onionmail.org
finn.bauer0423@proton.me	konedieyp@airmail.cc	lab-9-15@protonmail.com
crimson@onionmail.org	uenwonken@memail.com	Dacremain@tuta.com
keepvmn@onionmail.org	cyclops_faggot@proton.me	universejohn@tutamail.com
Ares.support@mailum.com	ransomhunters2026@gmail.com	JackLeomp@gmail.com
a00f105546345756@proton.me	opilqwertyuio@gmail.com	Answer:jackleomp@tuta.io
ilovemycubscout@gmail.com	wowsmith123456@posteo.net	quannilai@outlook.com
6449a3cle612168526@proton.me	corpovigiligiurati@onionmail.org	quannilai@hotmail.com
moneymaker2@india.com	corpovigiligiuratii@mailfence.com	aldetron@outlook.com
zawooorecover@onionmail.org		

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）。

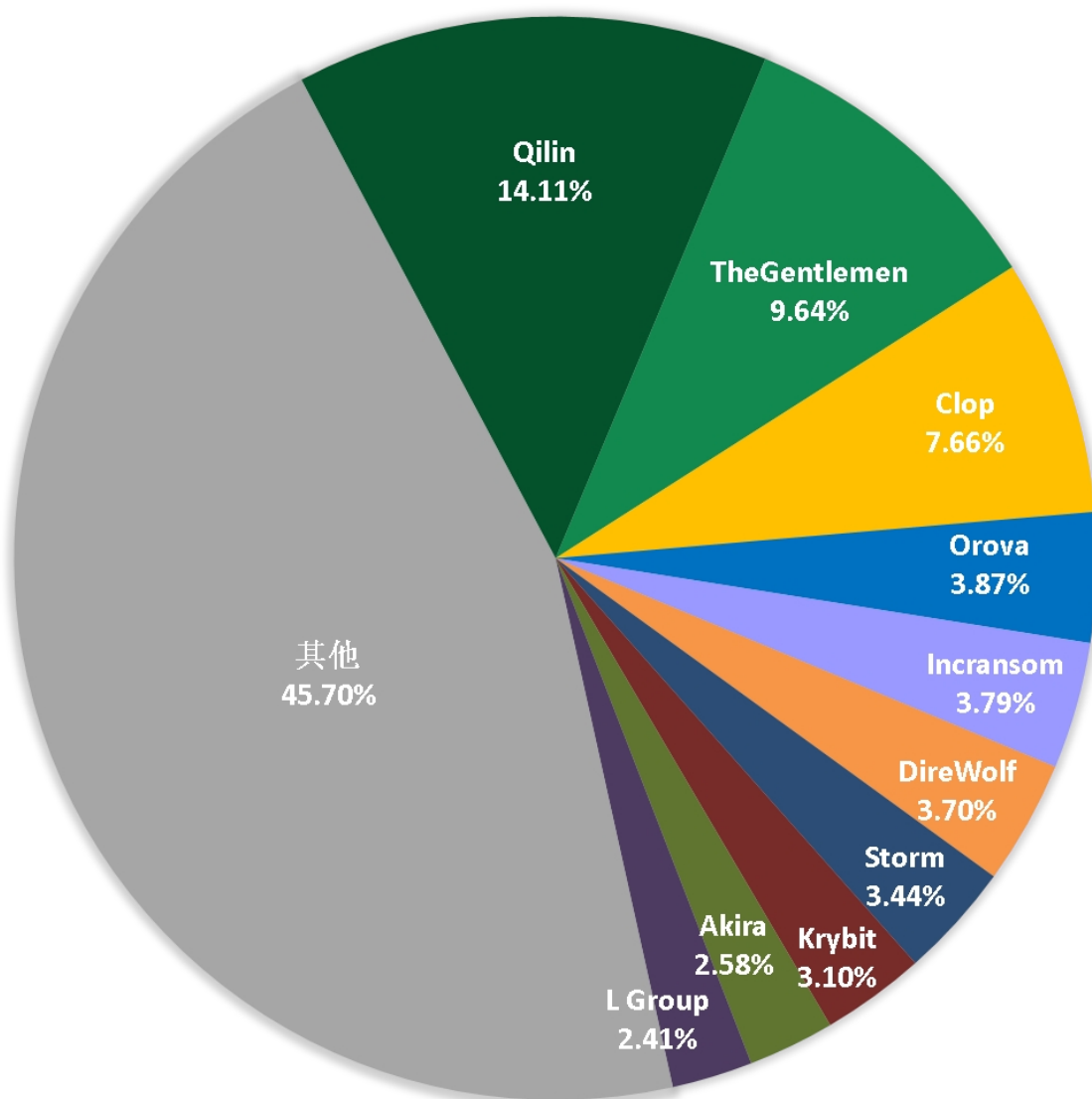


图 5. 2026 年 8 月通过数据泄露获利的勒索软件家族占比

以下是本月被双重勒索软件家族攻击的企业或个人。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，做好数据已被泄漏准备，采取补救措施。

本月总共有 1162 个组织/企业遭遇双重勒索/多重勒索攻击，其中

包含中国 40 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 59 个组织/企业未被标明，因此不在以下表格中。

Inmac	LOG Systems	Crown Group
icot.es	Magdalena Grand Beach Golf Resort	Ganzhou Xinye Craft Co., Ltd.
aeiconsultants.com	Akatake Engineering	Xpress Tech
syc.es	ESCON Group	powdr.com
Adviesbureau De Beuckelaer BV	Almeer	firstdigital.com
ahadandco.com	Geb Sas	flowco-inc.com
sago.com	ARBEITERKAMMERN	oligo.de
crmeyer.com	Aquasea	QPC Global
ccsperfusion.com	CAZ Investments	Service Evaluation Concepts
Easyoga	Oceanica Internacional	profinrg.nl
Truckworx	Ariel Energia	advancedtaxsolutions.com
R L Fine Chem Pvt. Ltd.	Hogan Omid P.C.	AngMar Companies
Allied Recycling	Yoma Fleet	B&B Hydraulik
ASYS Corporation	avkvalves.com	St ü cheli Architekten
Fu Sheng Industrial Co., Ltd	gt-tele.com	Baya Technologies
svfcu.org	NorthStar	www.kilpi-koskinen.fi
hoaattorneys.com	Aztec Software	www.apsanet.com.ar
manhattanloft.co.uk	The Revel Collective	tommer construction
Super Systems Inc	ProSim Aviation Research	Leafwell
WEMS	Authenticate Information Systems	FREYWILLE
zonarsystems.com	Diaco Global	BigSpark
Hayward Holdings	iSON EXPERIENCES	Cleaver-Brooks
New Century Ophthalmology Group	Deer Creek-Mackinaw CUSD	LT Group / Fortune Tobacco Corp
MEQ	Allstar Industries	Consolidated Medical Practices of Memphis
Figgins Family Wine Estates	HP Carriers	Interim HealthCare (Oklahoma and Tulsa)
KRC Machine Tool Solutions	MCT Group of Companies	Chat Jur í dico

Meteor Group	Reviso Cloud Accounting Limited	Merge
Metro Tulsa Foot	Studee	HIGEN MOTOR(critical data)
diversifiedbodyandpaint.com	The University of Delhi (DU)	Swyft Inc.
howardlumber.com	Gruppo Spaggiari Parma	AliveCor, Inc.
hatch.group	Ayuntamiento de Velilla de San Antonio	Statista GmbH
zayo.com	regencycenters	Quironsalud
cfsnow.com	acima	Health Carousel
transcar.com	marvin	Fondo
KFZ-MEISTERBETRIEB JOST GmbH	NetExam	Osmo Wallet
Gale Credit Union	Be Media	Elettrica System
Cedar County Memorial Hospital	Latoplast	Coggins Insurance Agency
EP Manufacturing Bhd	Qualiflex Datacenter HWZ-Studiengnge (fh-hwz.ch), myenb.ch, etc	Verona 83
Saudi Consulting Services SAUD CONSULT	Termotecnica Industriale S.r.l.	Presentations.AI
zummocorp.com	Frisian Flag Indonesia	Alcast
www.lichtvision.com	CTP S. r. l.	The Minor Food Group
www.renorefractories.com	Alto Calore Servizi SPA	One Vision Imaging
cimbsecurities.com	Tedesco & Partners STP srl	i4 Solutions
zenithtechnology.co.nz	POEMA S. r. l.	MACOFIN HELLAS S. A.
fes-sport.de	AYUDHYA TH Insurance	City of Winchester
bartelsbv.nl	GUSTO College GLMS	B Wright Drywall
vkj.nl	Indonesian Police Database	Cook Remodeling
allsteelproducts.nl	Job Net .COM.MM	Southern Metals
bkc.org	Strategy First International College	TRP International
Ishbia & Gagleard, P.C.	Cascade Coffee	Supportive Insurance Services
AFSARD	BioPharma	T. RAD North America
Crystalpharmatech	CONDOR SPA	Black Hills Bentonite
Absolute Consultancy Services	Elbor S.p. A.	Elix International SA
Black Cat Engineering Construction W11	CCA Bank	DECK APP TECHNOLOGIES PTE. LTD

Andover	Deas Millwork	PharmaEssentia
THQ Nordic	TECNOLOGICA S.r.l.	CONTAC Ingenieros
Erdem Hospital	Medical Arts Chemists and Surgicals	RAK Construction
Hospital Clínico Universidad de Chile	Club One Casino	Lancesoft India
Globus Medical	Practi-Cal	AIMS Group
DistributionNOW (DNow Inc.)	Austin Plastic Surgery Institute	AnMed
Glassdoor	ELCON MEGARAD S.p.A	NTU Alumni Club
G R Infraprojects	Questronix	Canopy Support Services
Northwest Trophy	Provite	Mikel Coffee
General Gruppo	Trends And Concepts	Hong Kong Baptist University
Ixa Systems	Grand Ion Delemen Hotel	Eva Care
Tecno Accion	The Margo Hotel	Premier Pigs
Probe Test System	JP Molyneux Studio	Zion Contracting
SUNSEA	Kingston Technology	MIE Solutions
Thai Film Industries PCL	Experts Entrepreneurs	Rilpa Enterprises
Adkisson Group	Grupo DT	Marconi Industrial Services
ESB Puerto Rico Corp	Capgemini Engineering	Synergy Interactive
Nutrypollo	usbank.com	pm-energy Die Solarexperten
Brebur	Semana	Energetic Development Corp
MB Associates	Delek US	Panda Logistics Taichung Branch
Exacta Optech Labcenter	UFOC	East Field Corporation
Servicios Aereos Estrella	Global Terminal Services	Chun Tai Sing Chemical Industry
zenithtechnology	Mihuru	Price Shoes
fessport	Ericksen Krentel	Naval Interior Team
esopartnerscpa	sunsea.co.th	Constellation HomeBuilder Systems
vectorsoft.de	Crowe	Harplast SRL
winterdienst-berlin.com	Advanced Engineering Consultants	Phithan Phanich
hd-werkstaetten.de	Aurora Health Management	Grupo Diestra
ng-engineering.de	DL HOLDINGS GROUP	Université Libre de Bruxelles
berghotel-oberhof.de	Southeastern Oklahoma State	Lucidmotors

	University	
rsk-immobilien.de	BANGKOKCABLE	Service d'usage 9002
montronix.de	UNIPLASTICS.COM	studiotibaldi.it
kdynium.cz	CDGARVINLAW	Siam Oil Product
frm.ind.br	EXEL	Daily Trust
acqbuilt.com	Thrifty Building Supply	Impact Centre Chrétien
BOTEC-CZ	Estech	Louisville Bar Association
n-tree.com	Constructora Jimenez	Clausing
hoerbuerger	Movitecnica	CLLS Co Ltd
wmdn.net	www.mestojilemnice.cz	Ingersoll Rand
FE CREDIT	automotoresrosedal.com.ar	Omnicell
i-one	sipresitalia.it	United Group of Companies
Neogen Corporation	www.hsi.info	Sawyer Savings Bank
Bandit Industries	WIS LOGISTICS	MEDICOS
LAPoco Architects	InVentry	OTEGROUP
Neumaticos Corral S.A.	Philippe Hottinguer Finance	Hitech Distribuzione Informatica S.r.l. (HTDI)
Uniguacu	Medochemie	Astro Electroplating
The Frame Group	Smart Energies	Filtronic
La Maison Des Travaux	Integraduanas	EISNER ZT GMBH
BLISS 1041	mecasem.org	John C Saunders, CPA
CareClinics	CRASL	Nikan Awasisak Agency
lindner-group.com	Senvest Capital	Depona
wittmann	Roadvision Systems	Pioneer Bank
ITC Properties Group Limited	Babcock	Hartfiel Automation
AUM Construction	Photon Health, Inc.	Alya Construtora
South Pacific Hotel Limited	InfoFlo CRM	CONTINENTAL AERO
MONTCAU	PayUp	MINDRAY.COM
trc-companies	Lifesum	ATMS
apatpa.com	Troutman Pepper Locke	uva.edu.br

cutlercapital	T... P... L...	ausfec1.com.au
Oilquip Inc	R & D Machine and Engineering	rosekennedygreenway.org
McKesson Corporation	Borchert & LaSpina	jean-petit.lu
SITTNAK Lojistik A.Ş.	Coltrane Systems	atp.chaco.gob.ar
Akpera Gayrimenkul Yatırım A.Ş.	Logitech/ Streamlabs	l-a.com.vn
Elekta AB	Berlin Brandenburgische Wohnungsbaugenossenschaft	automobile-mueller.info
Jack Henry & Associates	BOMOHSA	laticrete.com.cn
H.W. Lochner	SpearFin Ltd	mygoalseek.com
Alter Consultores Legales	ssf-int.com ssf-ing.de	psec.com.ar
Newton County School System	nyklawfirm.com nyk.ae	bouygues-es.fr
corematerials.com	Foresee Pharmaceuticals	ferretornillos.com
macallister.com	Prefeitura Municipal de Arcos	ratnasagar.com
Alumax	Valor Defense Solutions, Inc	brdigital.net.br
Valley Health Team	Standard Tool & Die	daycohost.com
Vigilia	Westco Motors Cairns	venezolanadepinturas.com
Hangzhou Qihan Biotech Co., Ltd.	WindRose Health Network	nokotapackers.com
Shanghai Tunnel Engineering Co Ltd	Penfold	immobilia.hu
Atcomm	Ramsey Bros	gslusa.com
DigiGround	Scholle IPN / SIG	www.racheljulien.com
Tramigo	SD Associates Sdn Bhd	coastproduce.com
Cosmocolor SA de CV	Third Coast Bancshares	zuckers.com
BEPeterson	American contractors insurance group	onsite-eng.ca
JRT Mechanical	Wcmanagement.info	doclv.com
ProCare	Alphanumeric.com	www.upbrand.com
Hanwha Renewables	Am-bition.jp	cookieskids.com
Infinnium	Grecosteel.com	INKA Group GmbH Co
Whitehouse	Makfreight.com	Vitex Pharmaceuticals
amzur.com	Adl embedded solutions	Mdj Management
Directorate-General for Education	GSW Gemeinschaftsstadtwerke GmbH	Hst

Bayview Real Estate WARNING	White-Daters & Associates, Inc	Groupe BPCE
Caduceus Medical Group	The University of the West Indies	Axson Teknik
tnmed.org	EmpireWorks	Ponti
ETNA Software	Codinter	Godollo
singleton.com	Bridgeport Capital Services	Hoang Chiropractic Center
Globalport Terminals	Sam Pack Auto Group	aZaaS
fpmanagement.nl	Woodhaven Association	HIWIN
Agrimac	terra-petra.com	National Furniture Outlet
Sprachakademie Rhein-Ruhr	BMW Group	TESI
Otto Sieve GmbH	Lansing Urgent Care	Intranet Gov Brasil
ITD Informations technologie	The Rubber Group	Feraboli Zootech
Our Hospice Of South Central Indiana	DL E&C	Nobema
National Salvage	4M REALTY COMPANY	Vemec
Zion Construction	Planungsgruppe M+M AG	LensAss Architekten
BENCIVIL	Arizona State University (ASU)	Phase Technologies
Kling Automaten	Wishfully Studios	Holborn European Marketing
Dotlines	Rx Networks	ZS Salovnova
Ipro.com(revealddata.com) customer DB + full database backup	Mighty Kingdom	Halliday Watkins Mann
GPS Grothkopp und Partner	Eva AI Limited	YY Business Solutions
Rohloff Group	Natco Home Group	NCA Alarms
Cetylite	Castilla La Mancha	Nelson Manufacturing
CGP MEP	Doimo Cucine	Southern Indiana Radiological Associates
Seabrook Island	Lloyd Coils Europe	Liberty Healthcare Corporation
Ruby Seven Studios	Otter Tail County, Minnesota	EvansPetree
DAB Investments	Vermont XCenter	OVP Health
Displaydata	Moores	Venture Logistics
Providence Investments	Albania's Official National Teacher Training Portal	Uber
LGG Advisors	Euroscreen	Highwoods Properties
Open Sports	Albania's official national teacher	Morguard

	training portal.	
takt.be	Teikoku USA	Westland Insurance
SCA Logistik & Fulfillment GmbH	AGUNSA	reflet2000.fr
dece.cz	Coface	www.actini.com
Capitol Mechanics	Spoonful of Comfort	www.ernat-bureau-etudes.fr
Jgsee	SAGASTA sro	www.serengetiestates.co.za
Servifruit	Mulino Padano	www.hymiasa.com
Hungry Lion	WEBA Meubelen	Crystal Pharmatech
Qualisteel	Moscord	Mayer Brown
Health	galmack.com.ec	Signature Services
NEXT LEVEL MEDICAL, LLC	airoyal.biz	GCATS Investments
theheartcenterofmemphis.com	tiltstudio.com	Platinum Group
proampac	Twal Family IT Lab	www.jerryleigh.com
Sanatorio Modelo de Caseros	All Parts Dry Cleaning	www.talbotdes.org
KenEp Resources	Idex Group	King International LLC
mat-holdings-inc	Bija Industrie	Akuur Law Firm
finodayacapital.com	Thecourierguy	AmSpec
cgcgabon.com	Kennedy Jenks	ALIZE (alize-sud.fr)
karkinos.in	actua.fr	Jakle & Alexander
ferretornillos.gt	dupouy-associés.fr	Park Place Behavioral Health Care
www.sankovn.com	agricolagalbusera.it	J&T Bank and Trust
Party Rental	tecoshim.com	MITC AG
TEC Container	vgrn.de	TECHVENTURES BANK S.A.
Verbux	MOSAID Technologies	City of Beacon
Espinos	INVENSITY	EduSpa
Incolur	Megawide	lya Construtora
www.neooftalmo.com.br	Infosat	Basic Grain Products
lemonfarm.com	Desatera Sdn Bhd	Pharma Test Apparatebau AG
wmiemporium.com	Loescher editore Torino	Bloom Financials
mimafoods.net	Botek	First Baptist Church of Bellevue

sysconth.com	Zanichelli	City of McMinnville OR
jindallifescience.com	Jone Précision	Hilliard's Air Conditioning & Heating Inc
vascara.com	Arnall Golden Gregory	Gemstone UK
Oral and Maxillofacial Surgery	ASCII Group	Hope's Windows
PA-ID	DELTA WAYS	Primary Eye Care
Simplex Engineering	motorenmaier gmbh	St Theresa Catholic Church
Demidov Steel Group	Double H Equipment	Stoneybrook West Master Association, Inc
Gill Rock Drill	Smartsoft	Stonecrest POA
ATF	PIO PIO	Magnolia Dental
WireCo	BONJOUR GROUP	Country Oaks Veterinary Clinic
Metal Conversions	KT RESTAURANT	David King Architect
California Truck Equipment	Dynatrace	Woodside Ranch
Northern Leasing Systems	Oz Hair & Beauty	Ferrell
ERPIS LLC	RapidFort	Micro-Comm Inc.
MEMSIC	DodoPayments	Namyang Industrial Co., Ltd.
Morgan Services	AAM:HOA Management	RS Automation Co., Ltd.
Hamilton	TOTVS	clubonecasino.com
Integrex RCM	Colla Health	vprj.org
Air International Thermal Systems	PayrHealth	Surakarta University
Brazosport College	DXS International	Festina Group
Central Florida Civil LLC	servmarmg.cl	Nitrex Chemicals India
Arich Enterprise Co., Ltd.	SEARS (Grupo Sanborns)	Mera Metal
Bai-chi CPA Firm	VR Advogados	Pavillon
industry.airliquide.kr	www.amca.org.ar	P. A. Inc. (Performance Alloys)
parkderochie.com	www.shalina.com	Mike Graham Heating And Air Conditioning
mwalker.com	Interim HealthCare	STADLER Sensorik CNC-Technik
copcp.com	Alpine Electronics Europe	tomorrowsoffice.com
National Kidney Registry	FERRARI MANGIMI SRL	Long-Lewis Automotive Group
Studio Legale ESE	granjarinya.com	Henshaw Law

Tiseo Paving	Columbia University Information (Dental)	Stade Francais
Johnson City Honda	Connections	The Metropolitan Entertainment & Convention Authority
Lockheed Architectural Solutions, Inc.	Connell Enterprises LLC	Formulatrix
Sinar Mas Agribusiness and Food Golden Agri-Resources)	Turner and Townsend	Laurel Institutes
SC PaderTeG Cabluri Electricce	Serruya private equity	Oasis Legal Group
A-Plus Software Limited	Sweet Water Holdings	Conway Analytics
Knottingham Trent University	Keystops	Ohio Living Home Health & Hospice
WINTER Ingenieure	Cozad Asset Management	Greenbotz
STRUCTURED SETTLEMENT CAPITAL LLC	FiferFox Minecraft Server	Labpharma
Davis & Ferber	Satellite Developer Server	Ruhrpumpen
AGROLAND S. A.	Aletex Group	Thermo King
Pump Engineering Company	Pierce Township	Storer Transportation and Storer Coachways
PCA Group Sdn. Bhd.	Radiant	Allied Telesis
Dentist in New Britain, CT	Lercher Werkzeugbau	Genesis Engineering Group
Cosmon	3f	Dharma Group
Consultores de Seguros	PenLink	Mayco International
SHAHEEN LAW GROUP PLC – Richmond, Virginia, USA	Urban Worldwide	Sutherland Packaging
FBC	tecnoabi.com	Brainhunter Companies LLC. and Brainhunter Systems Ltd.
lagegepesca.it	Hinman Straub	Al-Futtaim Group
The Liberty Group	3-point Australia	Leviton
Jones, Little & Co., CPAs, LLP	Rood & Riddle Equine Hospital	Aptara
Design-Aire Engineering, INC	Canadian Mental Health Association	The Family Medicine Clinic
Furnished Quarters	Tapper Cuddy LLP	Powerweave
Bihl	Integra Castings	Rocky Mount Recyclers
Frato	Metabase	Mansfield Family Dentistry
Criba	Sharecare, Inc.	The Miller Group
FFKR Architects	IPS	Stadler Rail

Brookview Financial	Carhartt, Inc.	TSC Logistics
Wozair	Gfeller Treuhand und Verwaltungs	Keysight
Davroc	Cook Medical LLC	Reid Electric Service, Inc
Chernyy & Associates	Gravity Coffee	Mile Bluff Medical Center
ManagementPro	Baxter International, Inc.	PontoBR Sistemas
Mark' Techno	Ollies Place Kidswear	PT All Cosmos Biotek
Government of Vojvodina	The Coffee Bean	FixIT Tek
Coldfish Seafood	KFC Kosova	lantisnet.com
www.ptesm.com	First Coast Heart Vascular Center	Loyalist College
Meridian Forest Services	Cityside Homes	Arkin Group / Arkin Casino,
Country-Wide Insurance	Retail Business Management Systems	Galvin Brothers
Federis Abogados	TOA	RUPP Spritzguss
Senvibe	Tempel	cesmac. edu. br
A&E + SMA Design	Plaza Auto Mall	TRULITE GLASS & ALUMINUM SOLUTIONS
Sharp Motor Group	Avanta Maroc Ex Adecco	First Tek
City of Mitchell	EKEPIS	Preferred Financial Group
resi.com	Megalaser Industria Metalurgica LTDA	TopMark Funding
Hospitality Health ER (Longview)	Community Connections	Control Concepts Technology
Westwing Group SE	Acli	healthcarehighways.com
S. E. M. P. s. r. l.	Vector Two Technology	ADG Healthcare
CyrusOne, LLC.	ASCOM S.p.A. ascom-italy.it serviced by an IT company Emilcom S.r.l.	eSysTech
adt.com	Reminger	Northeastern Communications & Electrical
Aurore Development S.p.A.	https://pacific-construction.com/	Apollo Office System
Global Go	cambrialawfirm.com	EMPYREAN INT' L TECHNO DEVICES
Euroflora srl	Hitachi High-Tech	Texas Medical Screening
Tecnici Associati STP	ZEBRA.COM	Sc Regional Housing Authority
Studio BOLDRIN PAOLO	SIA Medical Centre	Bjs Insurance & Financial
compendiumusa.net	GB Group S.A	Wisdom Oral Surgery
Clear Align	D & J Beverage Service	SURE TRAVEL COMPANY

Difor	CF Supply	WD Masonry & Concrete
Black Cat Engineering & Construction WLL	Zara Investment Holding	worldtube
FRUCASTRO SL	DAISEN	SBI Manufacturing
PappyJoe: Healthcare Management System	Yaomasa	Agricultural Chemical Solutions
Instituto Ferrero de Neurología y Sueño	Safeware	DBM Reflex
Brazil Mobilemed: Cloud PACS Platform	clgroup	Ultra Fame
Canada Yocale: Appointment Management System	Portable Intelligence Inc	Cardiology Associates
PawlyClinic: Digital Veterinary Care Platform	Hightech Signs	Yost Home Improvements
Dr Akbar Niazi Teaching Hospital	Riker Danzig LLP	KINGSSON
Centro Médico Especializado OSI: Healthcare Solutions	gamaus.com	SSI HOLDING (FAR EAST) LIMITED
Meducar: Telemedicine and Patient Management System	Tianji Auto Care Service Company	Sanrio Hong Kong Co., Ltd
ConsultorioMovil: Telemedicine and Healthcare System	SHELL.COM (August 2026)	Tat Fung Textile Co., Ltd.
Woodlore International Inc.	Westbrook Greenhouse Systems	Integrated Site Management
Trailer Transit Inc	Enteroptyx Ophthalmology Products	Conceptual Designs, Inc.
Weber Water Resources	Jack Rutherford Customs Brokers Ltd	JK Capital Management Limited
MPA Pharma GmbH	United Association Local Union 345	Global Friction Products, Inc
Aquamar Inc	BEDC.COM.AU	GILDE Handwerk Macrander GmbH & Co. KG
Corona Corporation	diabetesandmetabolism.com	US Installation Group, Inc.
FactoryFive	GATE7LLC.COMGBBEV.COM	pushidrosal.id
Namyang Industrial Co., Ltd.	ENTERATEK.MXESBERBEVERAGE.COM	lccgroup.com
Clinical Associates of the Finger Lakes (CAFL)	NUVITIA.COM	https://geleximco.vn/
Ruggles Sign Company	IPMSOLUTIONS.SK	clintonhealthaccess.org
AutoDie	ECCELLENT.COM	Oleoductos del Valle
Proveli	STNET.IT	pradotuylaw.com
Pinnacle Hospital	QCPL.IN	naskdoorinc.com
Phoenix Group of Companies	FLUIDLOGIC.COM	new-point.it

Schardein Mechanical	MIDLANDIND.COM.AU	simonrack.com
The Cecilian Bank	ITKHOLDING.HU	hanan-hov.co.il
Crystal Pharmatech	G3AEROSPACE.COM	Cameron Regional Medical Center
AGS Cinemas	ARCHERGREY.COM	azn.co.jp [azn.co.jp]
Eyecare Center of Snohomish	OMNITANKER.COM	southshorerecycling.com
Gould Sherwood Consulting	LIFESTRAW.COM	cpu-ag.com
Espac	SPKAA.COM	multiaqua.com
Layher	IVALUESYS.COM	Winn-Dixie
Volktek	NUOVACMM.COM	BLACKBURN'S Physicians Pharmacy, Inc.
ReliaQuest, LLC	THERMOS.COM	PCL Holding
el-group	WATERLANDPE.COM	Service Electric
AmSpec	9ALTITUDES.COM	Albers Mechanical Contractors
Vietnam Electricity(EVNHANOI)	INTELLIHOT.COM	Belasco Electric
NovoCure Limited	INTELLIGENTGROWTHSOLUTIONS.COM	Baicizhan
BOK Financial	HONGHE-TECH.COM	TUI China
Integrated Health Systems	ATOMBERG.COM	Hans & Jos. Kronenberg GmbH
RXPE Group	CLOVER.COM	Freedom Claims Management
Tower Insurance	JPMGROUP.CO.IN	pcclimitedindia.com
Flecha Bus	BRILLONCONSUMER.COM (BRILLONCONSUMER.COM)	setic-pourtier.com
OTEIS Conseil & Ingénierie	SUUNTO.CN (SUUNTO.COM)	microphase.com
Longhorn Investments	SMAPCENTER.UAH.EDU	rai.com.br
Kessler Creative	TRISTAR.COM	www.prohealth.sg
Klasko Immigration Law Partners	MAMASANDPAPAS.COM	ecfa.org
Patel	CORNELIUS.COM	INTERTRUST AUSTRALIA PTY LTD
Abacus Advisors	MAMMUT.COM	Asset Flooring Group Australia
LifeBank Microfinance Foundation	PARTECH.COM	Mairie de Drancy
PT Perusahaan Jamu Air Mancur	STARKEY.COM	www.dcpartner.co.za
PT. Bank Perekonomian Rakyat Bintan	LARGAN.COM.TW	nigeria.asa-international.com
icnavais.com	TOASTTAB.COM	www.ville-rinxent.fr

UAE Customs (Federal Customs Authority) – ACCESS GRANTED !	IRCO.COM	countrymotors.com.mx
Dubai Airport – ed	ALDOGROUP.COM (ALDOSHOES.COM)	Moses & Singer
Kuwait Ministry Of Interior !	PHILIPS.COM	www.buzztrading104.co.za
Yad Vashem Museum !	FISERV.COM	Wire Products
holzmarkt chemnitz	GE.COM	Encore Enterprises, Inc.
Freelom	NETPOWER.COM	Questel SAS
Island Networks	COMPUTER COUNTRY AND NETWORKS	Alcon Inc.
Mogren, Glessner & Ahrens, P.S.	stuartandassociates.com	Lumenis Ltd.
CRI Electric	SON-VIDEO	Philippine Savings Bank
Everglades Boats	GRUPO STARFOODS	The Butcher Brothers
Meridian Logistics Group	CDA	Sigma Plastics Group
Victory Personal Care, Inc	WONDR DIAMONDS & D GEM MOUNT	Cambridge Management
cedarridge.org	CARIBE / SUBRA	quantinum.com
Nteitalia	SCHMITZ & NITTENWILM	Vernon & Waldrep
Cinépolis	Goccia S.p.A.	The Saturday Evening Post
Quaker State Mexico	Camandona SA	Commercial Furniture Interiors
iPic	ALTAIR	Dienst Pack Systems
Gindre India	UAB Biotecha	Ceragres
JC Sales	ETICOD	Pointe Property Group [pointecre.com]
Fairview Dental Group	CALICHE	Schreiner Trockenbau GmbH
Battle Creek Public Schools	City Government of Baguio	MTCO (Mahmoud Altaheni & Partners Trading Co)
Clifton Architectural Glass & Metal	hisstw.com	CEN and Cenelec
First Commerce LLC	labindia.com	MIM Fertility
The Pendas Law Firm	lhyk.com.sg	M. B. Kahn Construction Co.
Blake Services	Wanted	Xs Cad
Professional	BerlinerLuft. Technology GmbH	Kamph
UOLconsult	Holstrom, Block & Parke, A Professional Law	Basso Fedele & Figli S.r.l.
dlp motive	Philadelphia Insurance Companies	G. M. A. GRANDI MARCHE AUTOMOBILI – S. R. L

AWJ Holding	Lexacaucho	
-------------	------------	--

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 7 以及 Windows 10。

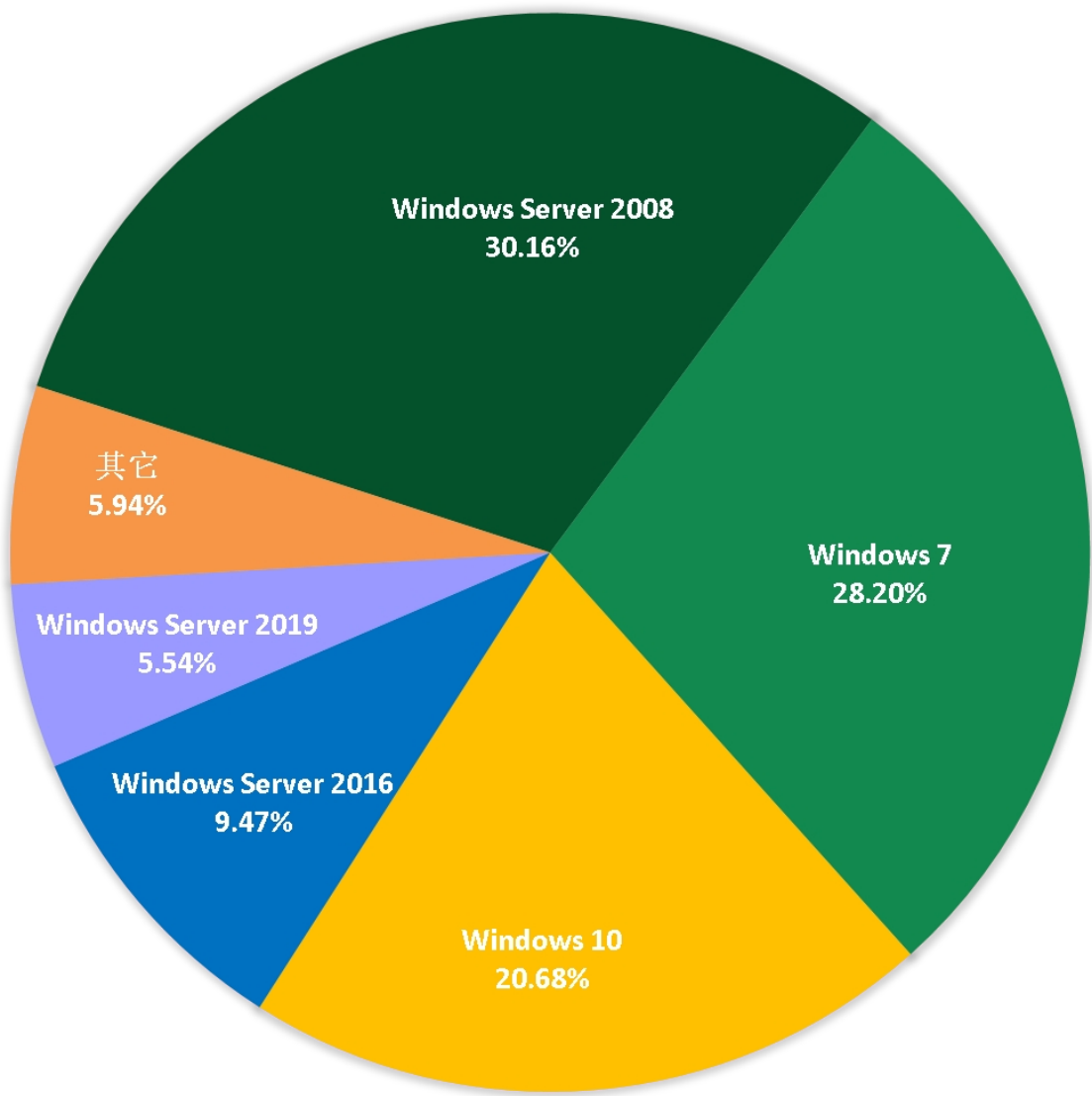


图 6. 2026 年 8 月受攻击系统占比

对 2026 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

仍是攻击的主要对象。

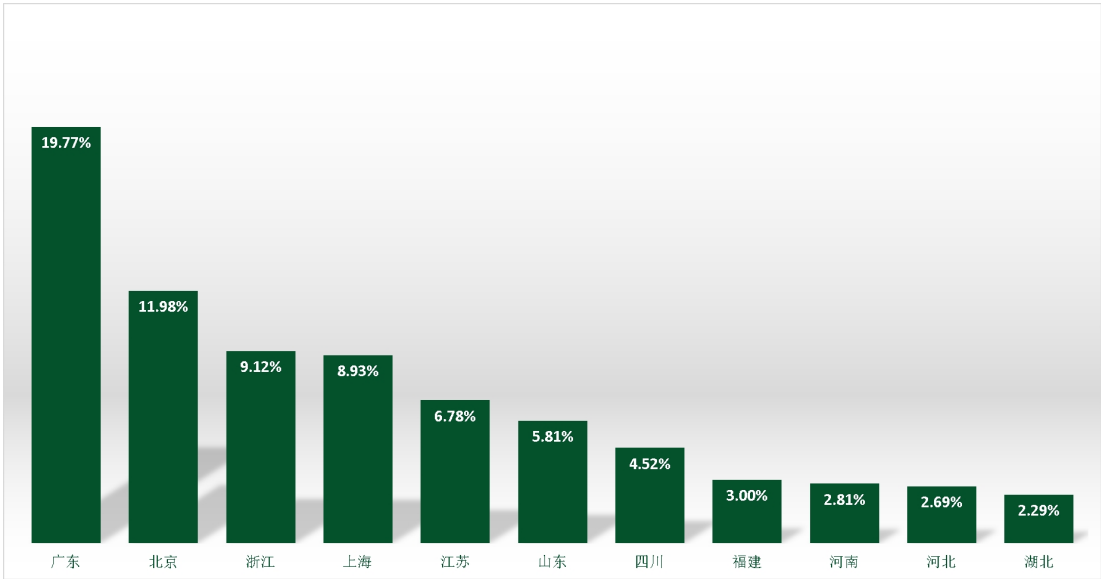


图 7. 2026 年 8 月国内受攻击地区占比排名

通过观察 2026 年 8 月弱口令攻击态势发现，RDP 弱口令攻击、MY SQL 弱口令攻击和 MSSQL 弱口令攻击，整体无较大波动。

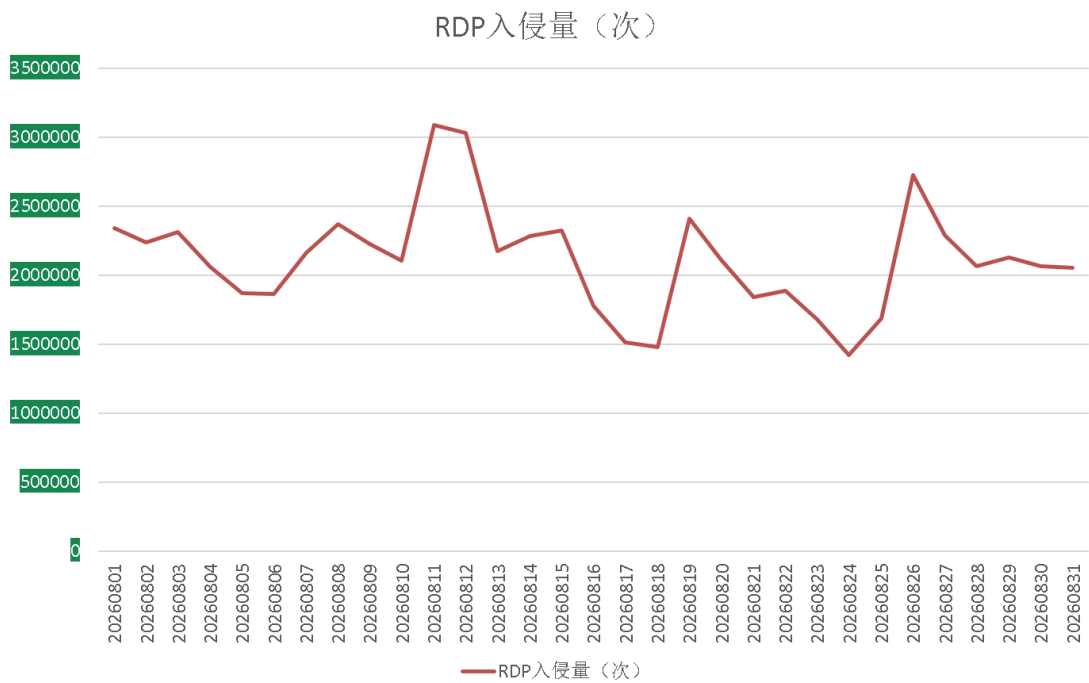


图 8. 2026 年 8 月监控到的 RDP 入侵量

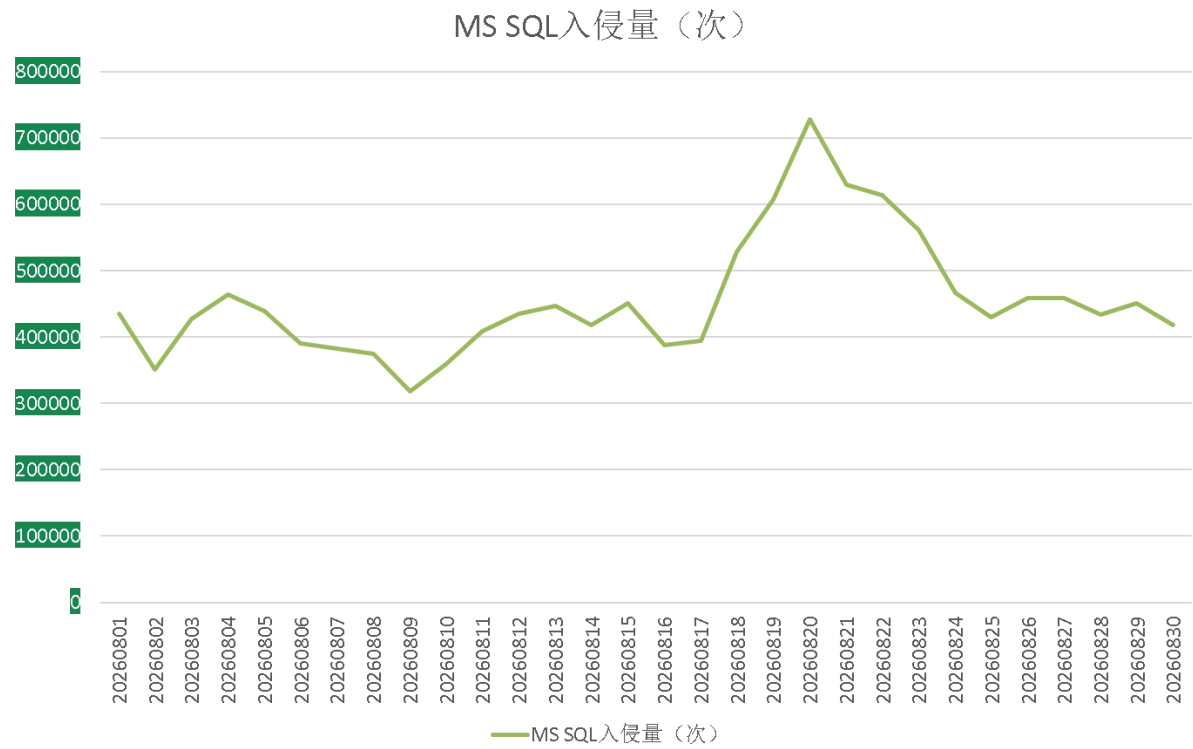


图 9. 2026 年 8 月监控到的 MS SQL 入侵量

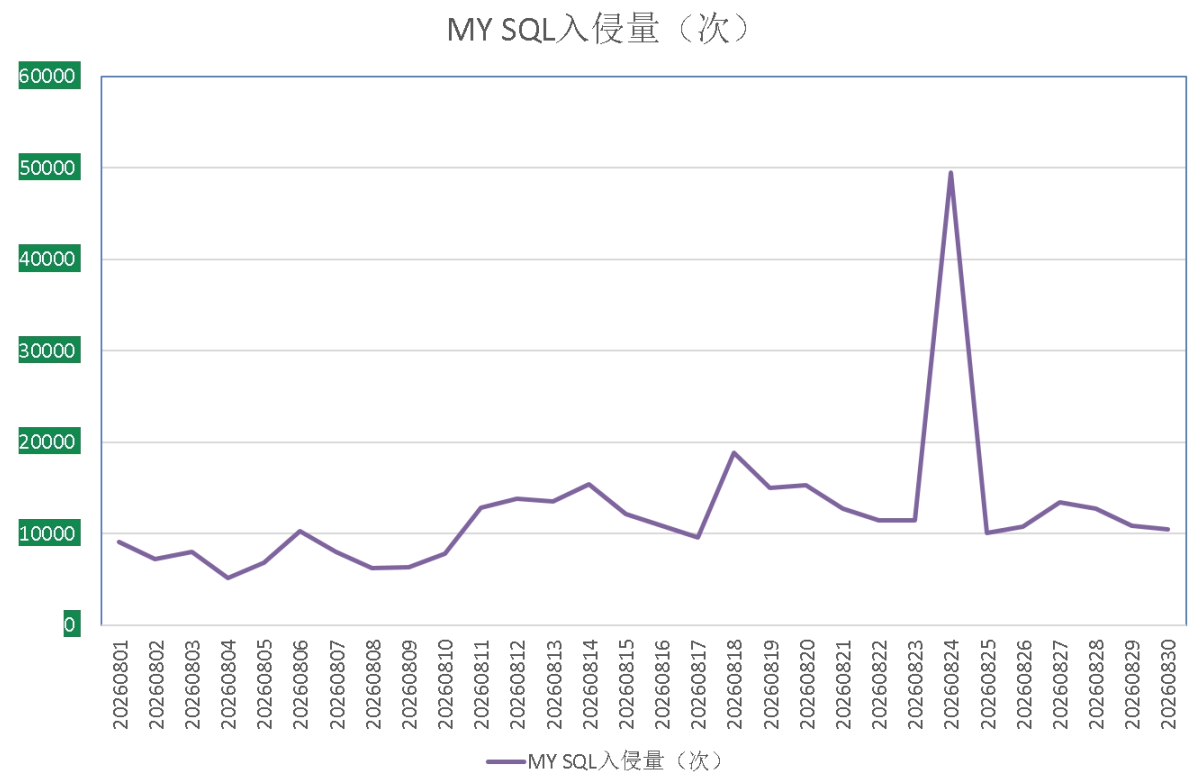


图 10. 2026 年 8 月监控到的 MYSQL 入侵量

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。

✧ 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。

✧ flex

属于 BrzCrypt 家族，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。

✧ sorry

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。

✧ kupala

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。

✧ 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、SQLGlobeImposter 渠道、漏洞利用、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。

✧ gen8

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。

✧ live

属于 live 家族，在国内已经不活跃，多为勒索验证与测试类传播。

✧ God8Dam

属于 Beast 家族，该家族的主要传播方式为：通过漏洞利用与暴力破解数据库口令，成功后手动投毒。

✧ rox （同 weax）

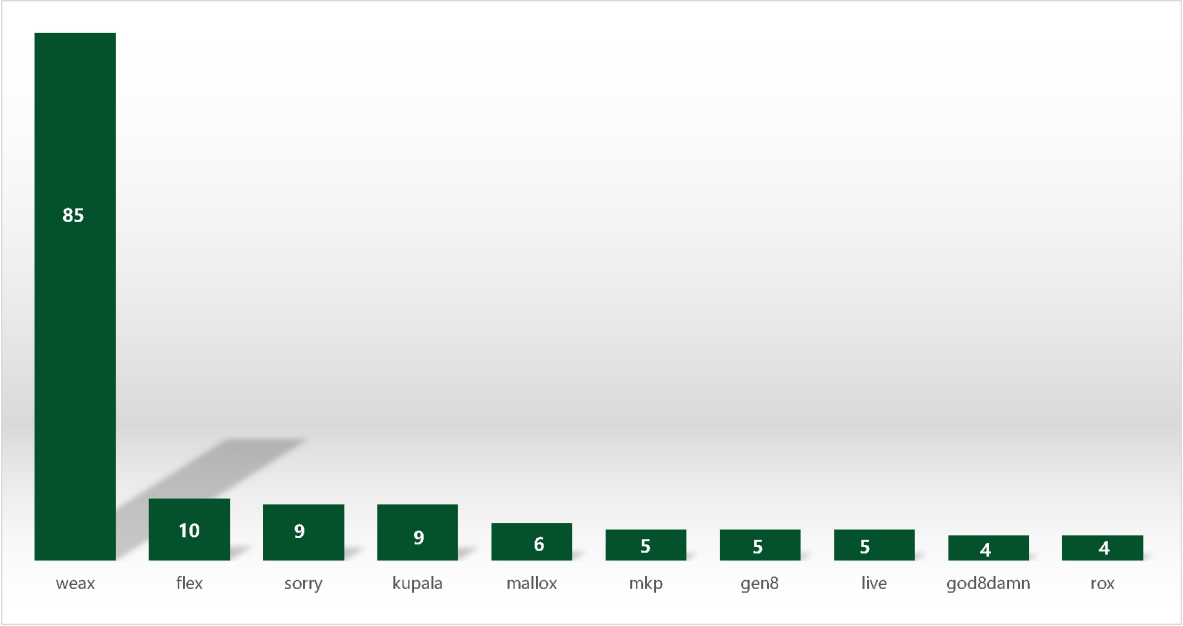


图 11. 2026 年 8 月反病毒搜索引擎关键词搜索排名

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 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。

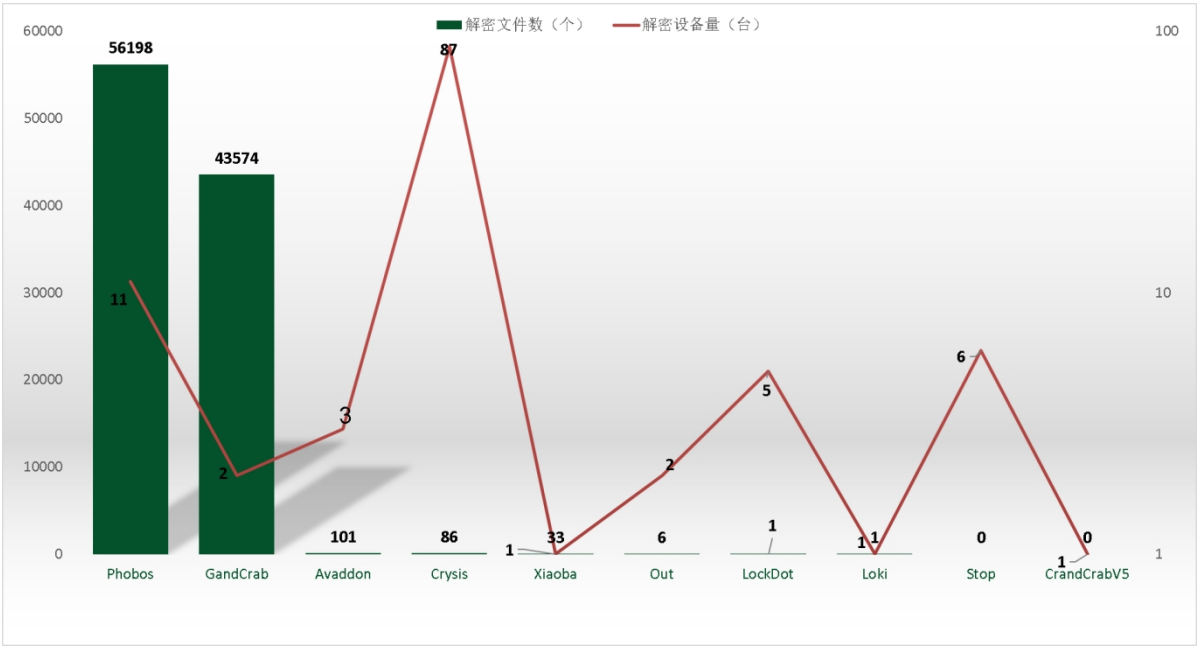


图 12. 2026 年 8 月解密大师解密文件数及设备数排名