

勒索软件流行态势分析

2025 年 7 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的监测与防御，为需要帮助用户提供 360 反勒索服务。

2025 年 7 月，全球新增的双重勒索软件有 BaqiyatLock、Satanlockv2 等多个新增家族。传统勒索软件家族新增 Darkness、Walocker、Mino 等家族。

其中 Darkness 在国内也有大量传播，并已经出现多个变种。Walocker 与 Mino 勒索软件分别所属的攻击组织则利用了一组被命名为 ToolShell 的 0day 漏洞对微软 SharePoint 服务器实现了高效入侵，突显了勒索攻击组织在新漏洞利用上的积极态势。

2025 年持续活跃的 Weaxor 勒索软件家族，其主流变种的加密后缀已更新为 .roxaew。此家族在保持每天变更代码混淆过的攻击载荷与多驱动加载的基础上，与银狐木马家族同步新增了针对 CVE-2024-51324 漏洞驱动的利用行为，这表明，以金钱获利目标为主的黑产组织在选择对抗手段上呈现出趋同态势。

以下是本月值得关注的部分热点：

- 1 Phobos 勒索软件终被破解，360 国内率先支持
- 2 SafePay 勒索软件攻击导致的 Ingram Micro 中断
- 3 俄罗斯职业篮球运动员因涉嫌参与勒索软件攻击而被捕

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

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 50.70%居首位，第二的是 Wmansvcs 占比 14.42%，Beast 家族以 7.91%位居第三。

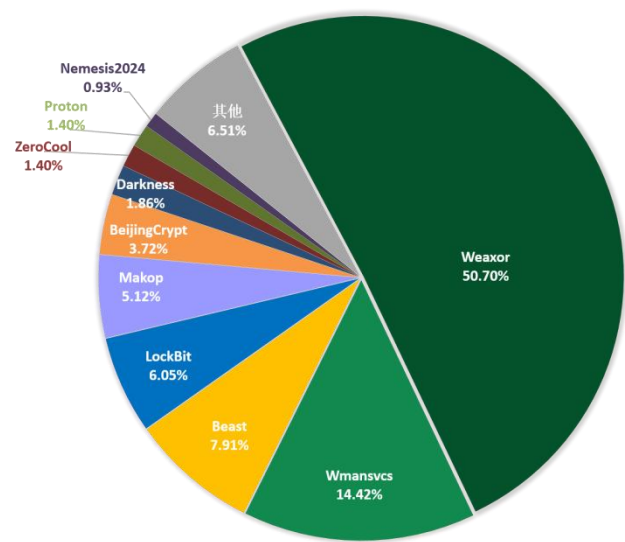


图 1. 2025 年 7 月勒索软件家族占比

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 2008 以及 Windows Server 2012。

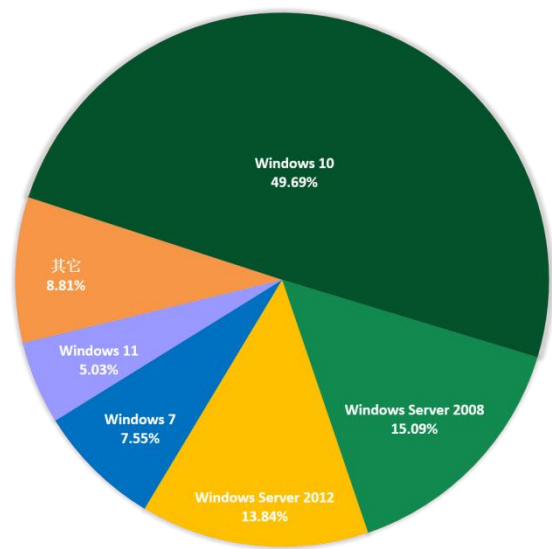


图 2. 2025 年 7 月勒索软件入侵操作系统占比

2025 年 7 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 大幅领先服务器。

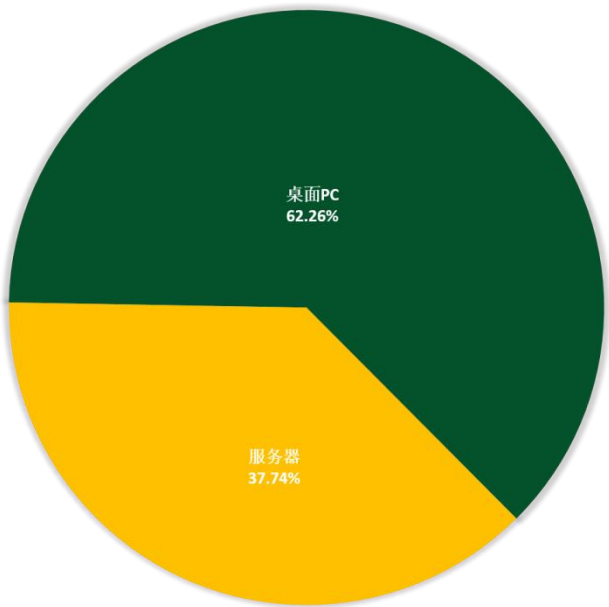


图 3. 2025 年 7 月勒索软件入侵操作系统类型占比

勒索软件热点事件

Phobos 勒索软件终被破解，360 国内率先支持

近日，国际执法机构公布了全球范围内广泛传播的 Phobos 及其变种 8Base 的解密信息。360 反病毒团队第一时间对该勒索家族样本开展深入分析，并基于获取的 14 个 RSA 私钥，在国内率先实现了对该勒索家族的解密支持，同时开发工具对多个 Phobos 及 8Base 变种实现有效解密。目前，360 解密大师是国内支持勒索软件解密最为全面的勒索解密工具。

如有被 Phobos 或 8Base 勒索家族加密数据的用户，欢迎联系 360 获取免费的解密协助。另外，对于以下一些不常见的扩展名文件，也可以联系我们尝试进行解密：

.2QZ3	.blackrock	.dewar	.GHOST	.NURRI
.6y8dghklp	.bqux	.DIKE	.grt	.OOH
.actin	.Caleb	.duck	.G-STARS	.OWN
.Acton	.Cales	.ebaka	.GUCCI	.phobos
.actor	.Caley	.eight	.jook	.phoenix
.Acuff	.calix	.eject	.KARLOS	.PLUT
.Acuna	.Calle	.eking	.karma	.slg2n3a4l
.acute	.Calum	.Elbie	.kmrox	.SHTORM
.adage	.Calvo	.elbow	.LIZARD	.STEEL
.Adair	.CAPITAL	.elder	.LOGAN	.unique

表 1. 支持破解的 Phobos/8Base 勒索软件扩展名

SafePay 勒索软件攻击导致的 Ingram Micro 中断

IT 巨头，全球最大的 C2C 技术分销商和服务提供商之一——Ingram Micro，此前的系统中断是由 SafePay 勒索软件攻击引起的，该攻击导致其内部系统关闭。7 月 3 日以来，Ingram Micro 的网站和在线订购系统一直处于瘫痪状态，但该公司并未透露问题的原因。据了解，系统中断是由 7 月 3 日凌晨发生的网络攻击引起的，其内部员工发现他们的设备上出现了勒索信息文件。

从勒索信息文件内容看，本次攻击与 SafePay 勒索软件有关，但目前尚不清楚设备

是否在攻击中被加密。应该注意的是，虽然勒索信息声称窃取了各种各样的信息，但这是所有 SafePay 勒索信息中使用的通用内容，并不代表本次针对 Ingram Micro 的攻击一定窃取到了这些信息。

据知情人士称，攻击者是通过其 GlobalProtect VPN 平台入侵了 Ingram Micro。该公司在发现攻击后关闭了内部系统，并通知其员工不要使用公司的 GlobalProtect VPN 进行访问。目前，Ingram Micro 已确认了攻击是来源于勒索攻击。

俄罗斯职业篮球运动员因涉嫌参与勒索软件攻击而被捕

俄罗斯职业篮球运动员 Daniil Kasatkin 应美国的要求在法国被捕，罪名是涉嫌充当勒索软件团伙的谈判代表。Daniil Kasatkin 是一名俄罗斯篮球运动员，在 2019 年返回俄罗斯之前，他曾在宾夕法尼亚州立大学短暂打过 NCAA 篮球。在 MBA-MAI 的四个赛季中他在离开球队前出场了 172 场比赛。

据法国媒体报道，Kasatkin 于 6 月 21 日与未婚妻一起抵达法国后，在巴黎戴高乐机场被捕。此次逮捕是美国国际逮捕令的一部分，因为他被指控为勒索软件团伙的谈判代表。

Kasatkin 现在被拘留，而美国正在寻求引渡他并面临“共谋实施计算机欺诈”和“计算机欺诈共谋”的指控。他的律师声称，Kasatkin 没有犯下这些罪行，这些问题与他购买的一台二手电脑有关。

虽然媒体并未披露勒索软件团伙的名称，但据报道，其在 2020 年至 2022 年期间参与了对 900 多家公司的攻击，其中包括两个联邦机构。此描述与臭名昭著的 Conti 勒索软件团伙非常相似，该团伙于 2020 年作为 Ryuk 的继任者出现，并在 2022 年因数据泄露而关闭。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

kyjpc@cock.li	zinkadvanc@tutamail.com	kawa4096@onionmail.org
kyjpc@mailum.com	iosif.lancmann@mail.ru	elijah@computernewb.com
weavercompany.e-co@cyberfear.com	adventurer@mailum.com	recovery_b@mailum.com
bruklin777@cyberfear.com	DarkxAnon7@gmail.com	Hall@firemail.cc
Enzo2003@firemail.de	decrypt@xentari.dark	Bluecrapteam@my.com
Enzo2003@cyberfear.com	tiwm30v0@hyplkao9.anonaddy.me	suppcowa@outlook.com
keypass@bitmessage.ch	exLgFiEf@tutamail.com	decryptdevelop@outlook.com
keypass@india.com	killback	mygodfather@xmpp.jp
ziver25@outlook.com	killback@mailum.com	ambulafixdata@zohomail.eu
darknessss11223@gmail.com	bashred-reAdmE.txt	ambulafixdata@onionmail.org
Darkness1@onionmail.org	bashID72@protonmail.com	m4_cruise@proton.me
onechance@mailum.com	Abandonfantasy00@proton.me	drnsrantr@gmail.com
backcontent@contractor.net	data-leakreport@onionmail.com	Bitrixdec@proton.me
backups@2mail.co	support-leakreport@onionmail.com	Bitrix@proton.me
zinkadvanc@onionmail.org	BlackBCruxSupport@onionmail.org	

表 2. 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，该数据仅包含未能第一时间缴纳赎金或拒缴纳赎金情况（已经支付赎金的企业或个人，可能不会出现在这个清单中）。

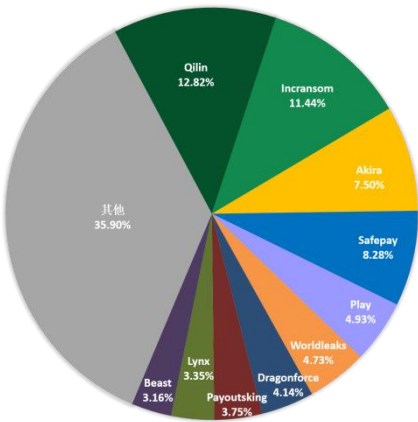


图 4. 2025 年 7 月通过数据泄露获利的勒索软件家族占比

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，做好数据已泄露的准备，采取补救措施。

本月总共有 507 个组织/企业遭遇双重勒索/多重勒索攻击，其中包含 8 个中国组织/企业在本月遭遇了双重勒索/多重勒索。其中有 17 个组织/企业未被标明，因此不在以下表格中。

Ieee-apscon.org	hitachi-tds.com	Darien Telephone
erichschleichgmbh.de	csaas.com	nexa.bb
carolynmyoung.com	nboat.com	www.intereum.com
bridgerecruit.co.uk	dtxstudio.com	fuld.com
wvpca.org	iBUYPOWER	City of Keene, NH
Thern	heartlineoklahoma.org	Websterhenry.com
Quartus Engineering	Protech Medical	LCM Construção e Comércio S/A
firstpresatl.org	SubsCorp	PACIFIC BIOLABS
eFunda, Inc.	danielslawgroupllc.com	Accu Reference Medical Lab
USA Military Alumni Networks	scaffoldsolutions.com	brennytransportation.com
lynkspot.com	Bronze Craft	tiergesundheitszentrum-koenigslut ter.de
deliastamales.com	chainstoreguide.com	bayviewci.org
whiteconlee.com	Thompson+Hanson	communitycareresources.com
iPROMOTEu	Studio Associato Callatroni Bianchi	SPANN Roofing & Sheet Metal
Grayscale Investments	DARA Pharma	Tara Pac
Mailchimp	Coalinga Regional Medical Center	nactarome.eu
www.afmco.jo	Somotsoft	www.wheelsauto.com
Devon	Integrated Silicon Solution Inc.	www.georgeallenconstruction.com
PDC www.cobranzasbeta.com.co	RattanIndia Power	Wispon
Tooling Systems Group	TCI Doors	Consorzio di Bonifica Adige Po
Bitbox	Act Legal	STE Energy S.r.l.
fsl.org	Plane Business Kayan Aero	Computer Ingenuity Associates
RUKU Tore - Türen	Proactive Engineering Consultants	Mack Energy Corp
restiani.com	Racine Olson	Microf
DARA Pharma	Becker Robotic	PPC Mechanical Seals
Lee & Associates	Operation PAR, Inc.	Confartigianato Imprese
Cpat Flex	NPK	Emphail.com
Towne Mortgage	Scherer Sanitätshaus Gruppe	TBC
Dollar Tree	Dell Technologies	Lamberts Business Systems
gimaex.com	Thomas Bennett & Hunter	Majestic
Winner School District 59-2	Kentfield Hospital	Ace Wire Spring & Form
Windsor Realty and Management	DP Systems	Stratascorp Technologies

Washington Court House	McNealy Brown	The Providence Warwick Convention
Sani-Tech Systems	InnoMedica	Doak Shirreff Lawyers
PROVAIL	Krusell	UPG Enterprises
JPS Consulting Engineers	pt.elis.com	MITACHI (HK) COMPANY LIMITED
Hafnia Law Firm	Universidad Mayor	INICIA
Grand Rapids Metrology	Anadolu Hastaneleri	Faria Braga Advogados Associados
El Paso Quality Dentistry	Pergamon Status Diş Ticaret A Ş	unyleya.edu.br
De Noordboom	Akribis Systems	snapav.com / resideo.com
Chevalier Machinery	TransCore ITS, LLC	Milberg
Campbell Sand & Gravel	Greeniverse	Wfmt
Aseguradora Fortaleza	Farben-Zentrum Schlegel	Wood, Patel & Associates
Acheson Doyle Partners Architects	RICHARD MILLE ASIA PTE. LTD & D'LEAGUE PTE. LTD.	Tyree Oil
ACMARK	erniesinceresco.com	Florida Hand Center
2FORM Architecture	Anderson & Karrenberg	Iran International
Built Environment Engineers	CB Quality Machining & Engineering	volpatoindustrie.it
Mid West Fabricating	City of Peabody, MA	BIG SILVER
KMDI	norpak.com	MAFATE BUSINESS ENTERPRISE
Custom Food Ingredients	diasdeprimavera.com.br	University of Puerto Rico Río Piedras Campus
tissot.com	gatlogistica.com.br	Cahill Seeds
ingrammicro.com	B&M – Expertise – Audit	Taiwan Digital Streaming Co Ltd
Druni	Burnham Nationwide	ELZAB
Hertz Farm Management	Sensical	silverdalebc.com
Mount Vernon Property Management	Tiger Communications	chirurgiemaxillo.com
First Baptist Church of Hammond	Polykar	lowcostspayneuterindiana.org
ci-Fabrics	Ritenour School District	avgouleaschool.gr
premiersurfacesinc	LeasePLUS	lewis-manning.org.uk
Software Design Consulting Group	Souleret Engineering(LSSE)	wmat.nsn.us
VIRTUALWEB.US	Home Solutions of Iowa	cascobay.org
mortensenlawoffices.com/USA/99GB	KEP Credit Union KEP	profile-ind.com
ACEA SpA	Sib-Tryck Holding	relucent.com
Dr. Falk Pharma	Fayrefield Foods	fmsarchitects.com
Albavision.tv	Multilift Logistic Group	ppa-eng.com.org
www.barobinson.com	GreenVest	caredig.co.uk
Yapi Teknik Proje	Goldberg & Osborne	Belmont Engineered Plastics
MGI Singapore PAC	Wingpoh_SG	BARIATRIX NUTRITION
W.L. FOODS	Crompton Lamps, UK	EvoluPharm
Aclarlar Ltd	HTC_Högtryckscenter_Sweden	Silent Gliss Italia
Votava Nantz & Johnson	Huize Sint-Augustinus_BE	Gateway Community
DA Whitacre Construction	Vitec	Arch-Con Corporation
Blanco Creek Farms	Comet-strip-enterprises-ltd	KOLBUS
Digitall Evolution	TERENCE C RINGLAND & CO PTY LTD	CR Architecture + Design

VINHAS E REDENSCHI ADVOGADOS	Secountryvets_AU	Institute of Culinary Education
CCI Torrevieja	lawforpersonalinjury.com	Crenshaw Community Hospital
College stj	Media Broadcast Satellite	Rhea Vendors Group SpA
tele-optics.com	mol.go.th	LTL
appswn.com	joseantoniorodriguez.com	Idgcayman.com
wta-inc.com	ashland.k12.ma.us	Lee Publications
bussepc.com	divgroup.eu	Allied Steel Buildings
swfldermatology.com	hlb.ie	Advance Ready Mix
havtechpa.com	palmasdelixcan.com	PHARMARON.COM
appagroup.com	accademia.it	Ridewill SRL
briar-group.com	GreenLight Biosciences	gatewaycsb.org
teamsignal.com	T2 Group	https://thesandersfirm.com/
Morrow Equipment	Ark Consultancy	heimhaus.de
CONTRAQI	Allstarmg	tsaworld.com
Cyme Servicios Médicos	Helpsonv	jubileejobs.org
Dithelm Travel Group	C3 Group	ITACCESS PTE. LTD.
Geomaticks Grecia	Joni L Janecki & Associates	Freedom Wood Doors Ltd
Medical Village LIV	Waverly Cabinets	Whim Hospitality
MukundRhotindian	Burnett and Son Meat	Southwest CARE Center
Rete Toscana Classica	Artemis Healthcare, Inc	Sermo
RTE	A-Qroup Şığorta Şirkəti	Prosecuting Attorneys' Council of Georgia
hptc.org	Tan Chong Motor Holdings Berhad	Eurofins
I.P. One LTD	Warisan TC Holdings Berhad	https://klinikdrindrajana.com/
Bouey & Black LLP	Larimart S.P.A	TBD HONG KONG
Dunlap Coddling	Morrison Companies	takachiho.co.jp
Helical Auto Technology (India)	IMSSA Manufacturing	elematec.com
jorgefernandez.es	Acetificio Andrea Milano	gotec.com
Astro Industries Inc.	5 d Sec	Hana Financial
moelco.es	Title XI	Silver Lining Herbs
lafavoritaservice.it	PEPRO	Assetlabs
Crumb1	Specialty Components	BD Group
Best Price Financial Services	ResourceEnergy	RG Mexico
md-labels-gmbh.com	Halvorsen Family Law Group	Your Building Centers
Emerson Chiropractic	Young Adjustment Company	fkk.ac.th
www.mada.com.kw	www.pomerandboccia.com	https://www.teligent.se/
salamanderresort.com	New American Funding	studionotarile.com
teampostop.net	WH Rogers Sheet Metal	cityofgardendale.com
seasonsfour.com	Inside One	Corinthian Media
BALNEARIO DE MONDARIZ	City of Green River	DKN Hotels
morgan911.org	Mausolff Immobilien	knightknox
foiegrasespinet	The Paul Wilkinson Law Firm	Apntelecom.com
moonsafari	Victoria Garden	Niflaot Hatzuna Ltd

Gallon, Takacs & Boissoneault	MEDIALAB	C B King Memorial School(branch)
jaegerndorfer.at	Adrian Kenya	Punta Del Agua
Donlar Construction	Greta Group	Cenomi Retail
Testa Heck Testa & White	ProActive Solutions USA	JFC Electric
Pilipili	BAF Management Consulting	Metric
Metricon Homes	Cardinal Services	All Choice Rentals
www.entecheng.com	Otjiwarongo Municipality	Biofloral
www.labiennale.org	Progressive Auto Group	Lydig Construction
www.lincecomercial.com	eehc.gov.eg	Kirkor Architects and Planners
Sementes Jotabasso	Mazzoleni	Sanderling
Creditinfo	The Colgin Companies	Vynopsis
Palm Bay International	www.marvimundo.com	Universal Softare Solutions
OKA	CF Construction Ltd	vresystems.com
Reimo	VM Racing	corpdvs.com
DelCampo	Schlemmer Holding GmbH	conlonproducts.net
APL	Culver's Lawn & Landscape, Inc.	https://www.injusa.com/
Vantage Finance	inspiredbeauty.com	QUINTADAMARINHA.com
Watchfinder & Co	Conasa	atlantissubmarines
https://eagleonline.net/	loraincountyauditor.gov	Allegheny Answering Service
Ka Logistics	Hulberg & Associates	HKG Duty Free
DA Whitacre Construction	Rockrose Development	JCC Rockland
blueridgesl.com	Belk	Oxford Universal Corp
rhschool.org	CARSTAR Business Group	The University of Zagreb Faculty of Science
qtmi.net	www.v4ulogistic.com/ Leaked by www.etornetworks.com	alereon.com
horanbarker.com	dwllp.ca/ Leaked by www.etornetworks.com	fcsserves.org
naxis.net	lstlaw.ca/ Leaked by www.etornetworks.com	Mainetti
landwilson.co.uk	Trilinklogistics Inc / Leacked by www.etornetworks.com/	Ivri, Kerner & Co
salemma.com.py	National Institute of Water Resources	dossenterprises.com
stichtingjohannesbosco.com	solidere.com	lafayettefamilyymca.org
bisa.com.pe	Twaweza	jansen-aschendorf.de
Nippn TH	Tuna Processors Phillipines, Inc	villagecoin.com
www.reliablecontrols.com	conasa infraestrutura s.a.	parsons-peebls.com
SOUBEIRAN CHOBET S.R.L.	pinnacle Roofing and Exteriors	capmark.org
Windsor Door	North Country HealthCare	Alert Medical Alarms
Pinnacle Woodwork	Rezayat Group	LP Charpente
Sogedis	Dansoft	Globalinks
TOMEI GROUP Inc.	nod.ro	Watermark Marine Systems

Able Home Care	bartec.com	exhibits-intl.com
http://www.balkankalip.com	Intercommunityct.org	tokiomarine-nichido.co.jp
Primoris	Tulsat	www.ogr-jp.com
ARCTICGROUP	INS Quebec	Cameron, Hodges, Coleman, LaPointe
www.optyma.co.uk	EIA Global	The Printing House
icmconv.com	CyberlinkASP	Kinik Gross Toptan Market
carestlhealth.org	FormWood Industries	Premier 1888 Ltd.
neues-leben.de	k12albemarle.org	JIEI CO., LTD
asi-group.com	Department of Culture and Tourism Abu Dhabi - Download link	Eversendai
reizenlaw.com	Ensemble Montplaisir	coruzcitywndata+
sbamh.org	Genesis Billing Services	Wegley Higginbotham & Associates
WIBAIE		

表 3. 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。

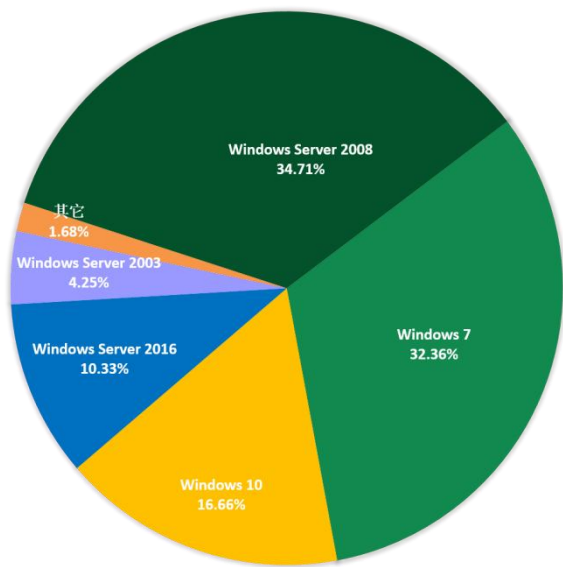


图 5 2025 年 7 月受攻击系统占比

对 2025 年 7 月被攻击系统所属地域进行统计，并与之前几个月采集到的数据进行对比发现，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。

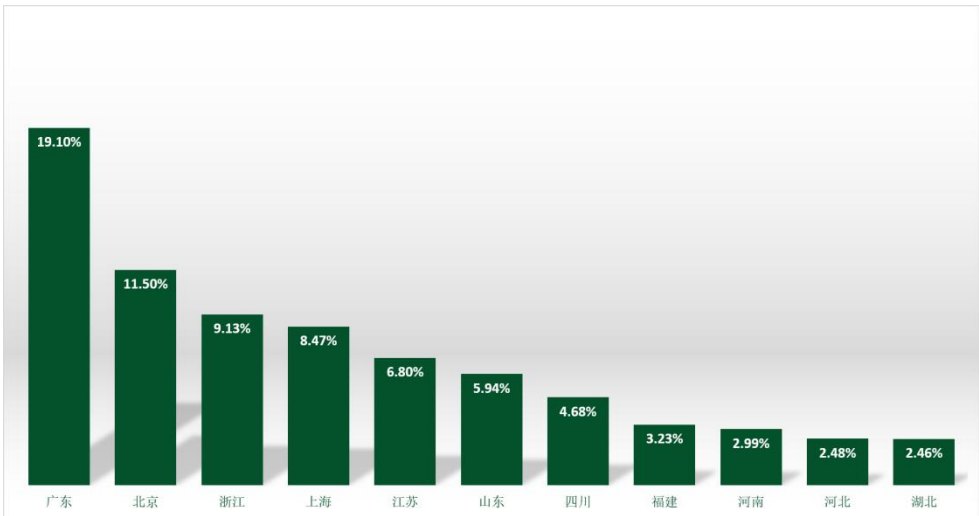


图 6. 2025 年 7 月国内受攻击地区占比排名

通过观察 2025 年 7 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。

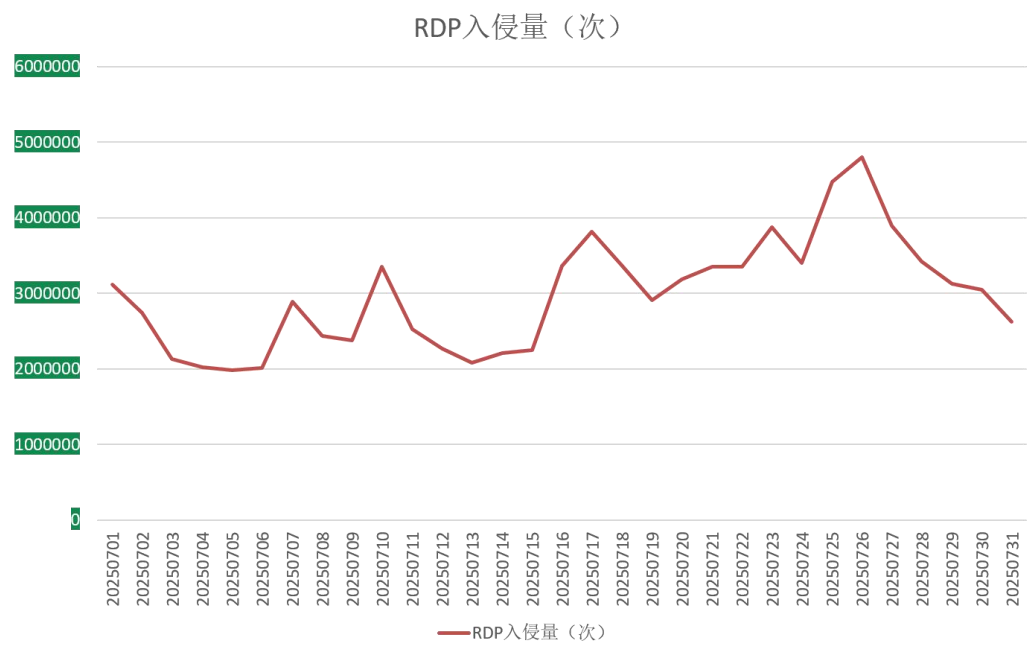


图 7. 2025 年 7 月监控到的 RDP 入侵量

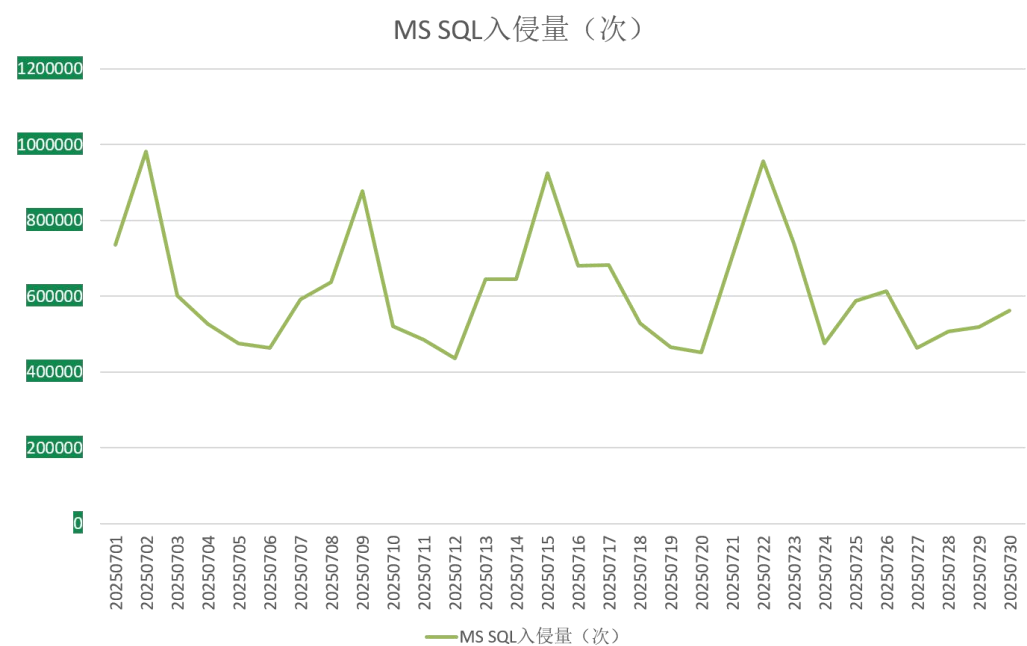


图 8. 2025 年 7 月监控到的 MS SQL 入侵量

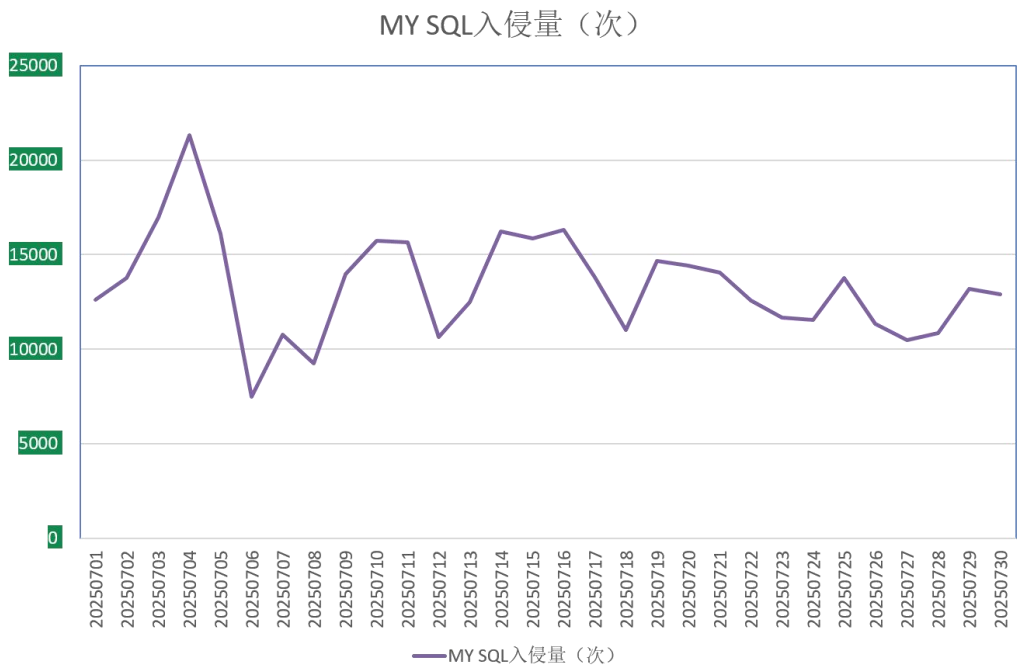


图 9. 2025 年 7 月监控到的 MYSQL 入侵量

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：利用各类软件漏洞利用方式进行投毒，通过 powershell 加载攻击载荷并与安全软件进行内核对抗。
- ✧ wxx: 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。
- ✧ bruk: 属于 Beast 勒索软件家族，该家族支持多个操作系统平台传播。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。
- ✧ 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。
- ✧ 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。
- ✧ weaxor: 同 roxaew。
- ✧ wstop: 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。

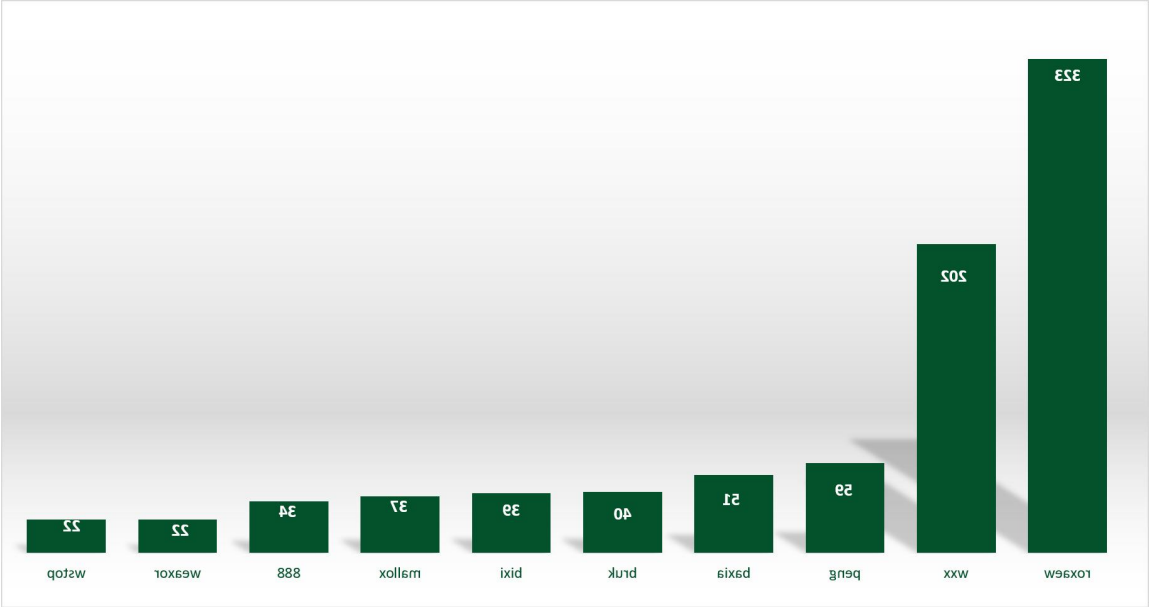


图 10 2025 年 7 月反病毒搜索引擎关键词搜索排名

解密大师

从解密大师本月解密数据看，解密量最大的是 CrandCrabV5 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。

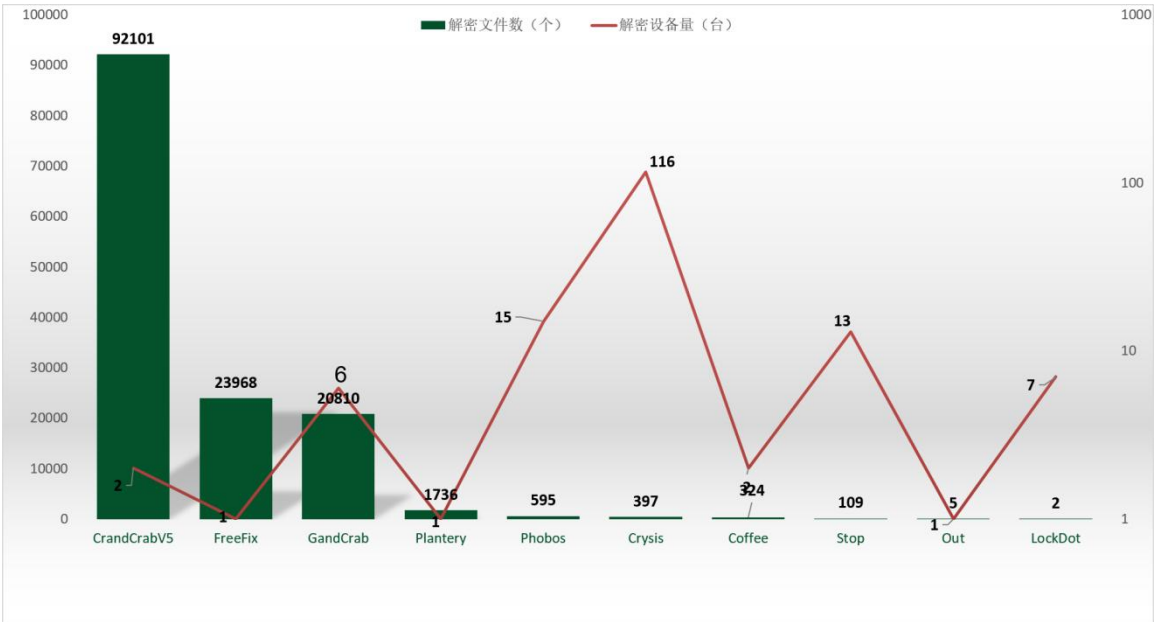


图 11. 2025 年 7 月解密大师解密文件数及设备数排名