勒索软件流行态势分析

2025 年 2 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 2 月，全球新增的双重勒索软件家族包有 Anubis 和 RunSomeWares，前者具备跨平台的勒索能力并主要以数据窃取为主。老牌双重勒索软件 Clop 勒索软件利用软件漏洞（疑似 Craft CMS CVE-2025-23209 与 Palo Alto Networks PAN-OS CVE-2025-0111）在 2 月份纪录式地入侵了 335 个受害者，以北美为地区主。

以下是本月值得关注的部分热点：

1. **黑客利用 SimpleHelp RMM 漏洞部署 Sliver 恶意软件**
2. **CISA 和 FBI 表示 Ghost 勒索软件入侵了 70 个国家或地区的组织**
3. **新的 NailaoLocker 勒索软件被用于攻击欧盟的医保组织**

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 24.42%居首位，第二的是 RNTC 占比 16.28%的，Makop 家族以 15.12%位居第三。

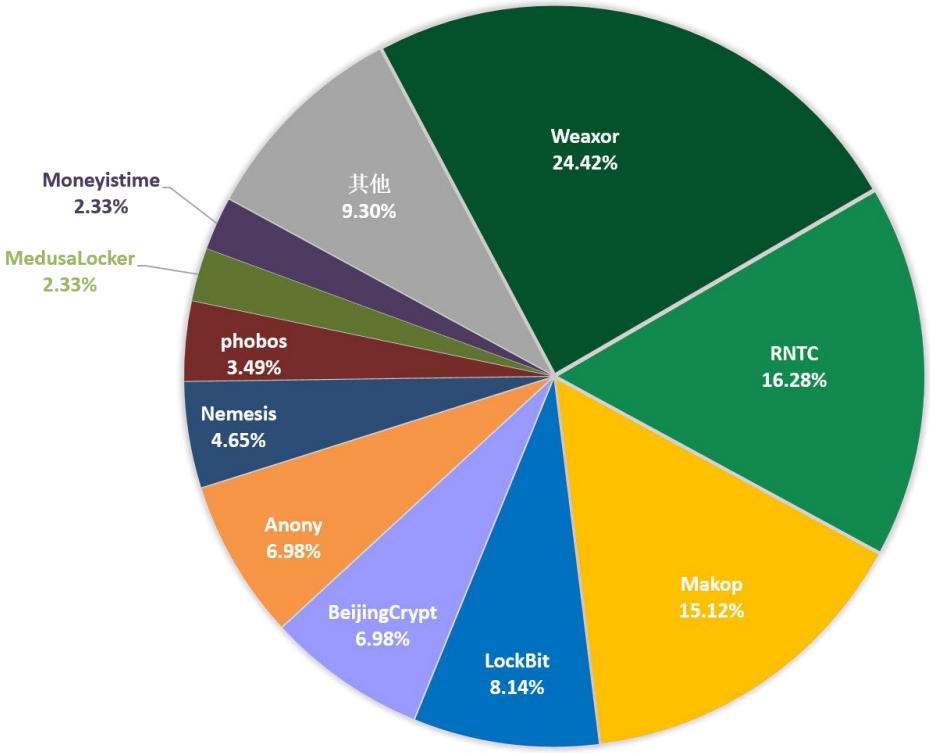

图 1. 2025 年 2 月勒索软件家族占比

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 2016。

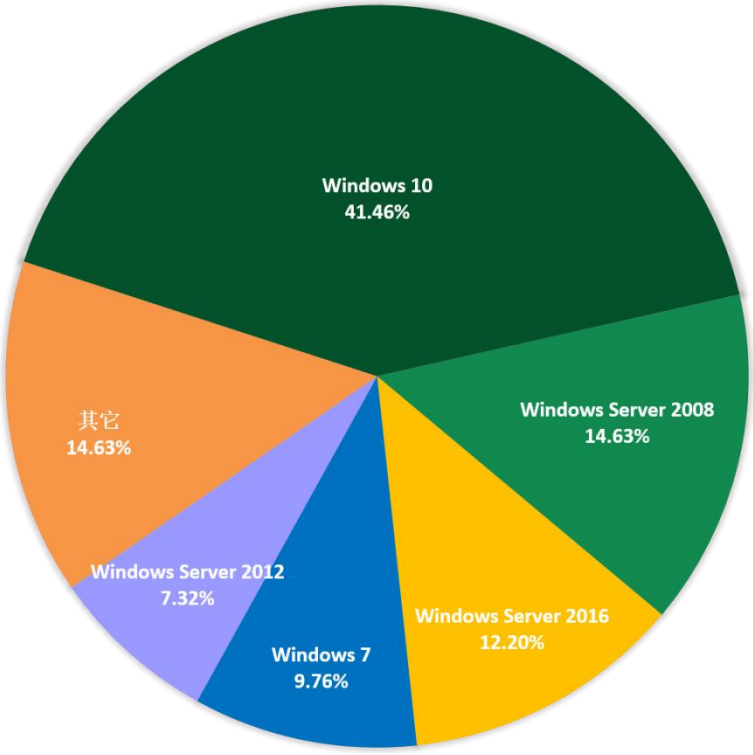

图 2. 2025 年 2 月勒索软件入侵操作系统占比

2025 年 2 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 与服务器平台较为接近，NAS 平台以内网 SMB 共享加密为主。

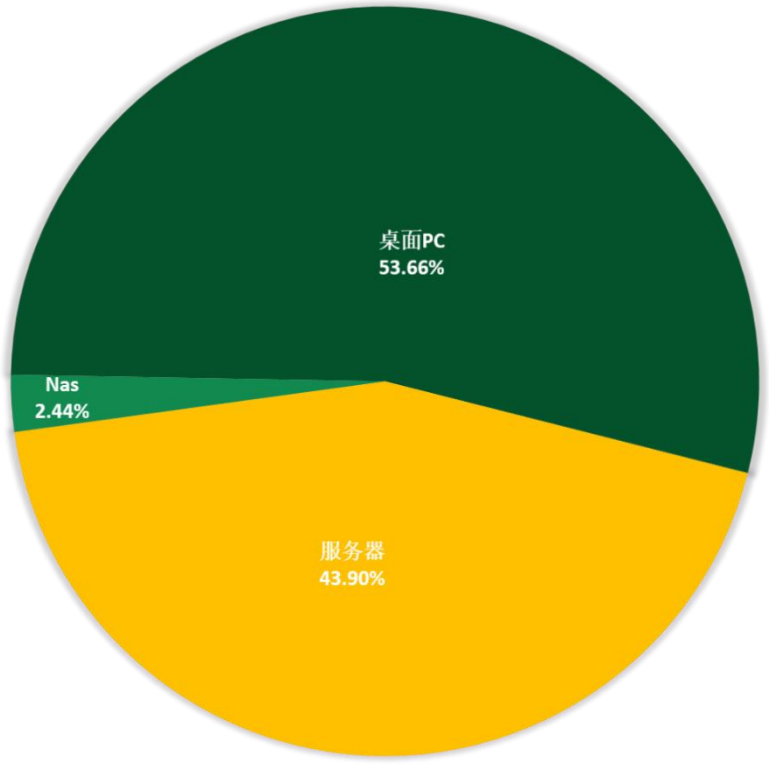

图 3. 2025 年 2 月勒索软件入侵操作系统类型占比

勒索软件热点事件

黑客利用 SimpleHelp RMM 漏洞部署 Sliver 恶意软件

黑客以存在漏洞的 SimpleHelp RMM 客户端为目标，创建管理员帐户、放置后门并可能为勒索软件攻击奠定基础。被利用的漏洞编号为 CVE-2024-57726、CVE-2024-57727 和 CVE-2024-57728。上周有报告称这些漏洞可能被 Arctic Wolf 利用，但尚未找到确切证据。此外，网络安全研究人员还观察到的活动有 Akira 勒索软件攻击的迹象，不过目前没有足够的证据来进一步印证勒索攻击与漏洞利用的必然联系。

本轮攻击始于攻击者利用 SimpleHelp RMM 客户端中的漏洞建立与目标端点的未经授权的连接。已观察到的攻击事件中，攻击者连接到爱沙尼亚 IP 的服务器

194.76.227.171 的 80 端口上运行的 SimpleHelp 实例。通过 RMM 连接后，攻击者会快速执行一系列发现命令以了解有关目标环境的更多信息，这包括系统和网络详细信息、用户和权限、计划任务和服务以及域控制器信息。此外，安全人员还发现受害机器中存在 CrowdStrike Falcon 安全套件的命令，可能是攻击者尝试利用该命令绕过机器中的权限控制。

之后，攻击者利用他们的访问权限继续创建了一个名为“sqladmin”的新管理员帐户来维护对环境的访问，并安装 Sliver 利用框架（agent.exe）。在过去几年中，Sliver 一直是作为 Cobalt Strike 的替代方案，该工具的使用量有所增加，而 Cobalt Strike 则因越来越容易被安全软件检测到而被逐渐抛弃。部署 Sliver 后，攻击者则通过命令链接到控制服务器以打开反向 Shell 或等待命令在受感染的主机上执行。

在攻击中观察到的 Sliver 信标被配置为连接到荷兰的 C2。此外，研究人员还发现受害机器中被启用了远程桌面协议（RDP）的备份功能。建立持久性链接后，攻击者通过使用相同的 SimpleHelp RMM 客户端破坏域控制器（DC）并创建另一个管理员帐户“fpmhlttech”来进一步深入整个系统的内部网络中。目前未发现攻击者安装后门，而是安装了伪装成 svchost.exe 的 Cloudflare Tunnel 以保持隐蔽访问并绕过安全控制和防火墙。

CISA 和 FBI 表示 Ghost 勒索软件入侵了 70 个国家或地区的组织

美国网络安全与基础设施安全局（CISA）和联邦调查局（FBI）表示，部署 Ghost 勒索软件的攻击者已入侵了来自 70 多个国家多个行业领域的受害者，其中包括关键基础设施组织。其他受影响的行业包括医疗保健、政府、教育、科技、制造业，以及众多中小企业。

CISA、FBI 和多州信息共享与分析中心（MS-ISAC）在周三发布的联合公告中称：“从 2021 年初开始，Ghost 勒索软件的攻击者就开始攻击那些面向互联网的服务运行着过时软件和固件版本的受害者。”……“这种对存在漏洞网络的随意攻击，已导致 70 多个国

家的组织受到侵害。”

Ghost 勒索软件的运营者经常更换恶意软件的可执行文件,更改加密文件的扩展名,修改勒索信的内容,并使用多个电子邮件地址进行赎金交易沟通,这使得对该组织的追踪归属随着时间推移而不断变化。与该组织有关的名称包括 Ghost、Cring、Crypt3r、Phantom、Strike、Hello、Wickrme、HsHarada 和 Rapture,其攻击中使用的勒索软件样本包括 Cring.exe、Ghost.exe、ElysiumO.exe 和 Locker.exe。

这个以获取经济利益为目的的勒索软件组织利用公开可得的代码,利用易受攻击的服务器中的安全漏洞。他们瞄准的是 Fortinet（CVE-2018-13379）、ColdFusion（CVE-2010-2861、CVE-2009-3960）和 Exchange（CVE-2021-34473、CVE-2021-34523、CVE-2021-31207）中未修复的漏洞。

新的 NailaoLocker 勒索软件被用于攻击欧盟的医保组织

2024 年 6 月至 10 月期间,在针对欧洲医疗保健组织的攻击中发现了一款新出现的“NailaoLocker”勒索软件。此次攻击利用了 Check Point 安全网关的一个漏洞（CVE-2024-24919）来入侵目标网络,并部署了“ShadowPad”和“PlugX”恶意软件。

法国电信旗下网络安全公司 Orange 的计算机应急响应小组认为“NailaoLocker”是一种相当基础的勒索软件,原因在于它不会终止安全进程或正在运行的服务,缺乏反调试和逃避沙盒检测的机制,也不会扫描网络共享。

该恶意软件通过动态链接库加载（sensapi.dll）的方式部署到目标系统上,并利用了一个合法且经过签名的可执行文件（usysdiag.exe）进行掩护。恶意软件加载器（NailaoLoader）通过进行内存地址检查来验证环境,然后解密主有效负载（usysdiag.exe.dat）并将其加载到内存中。接着,NailaoLocker 使用 AES-256-CTR 加密方案对文件进行加密,在加密后的文件后面添加“.locked”扩展名。加密完成后,勒索软件会留下一个 HTML 格式的勒索通知,文件名异常长,为:

unlock_please_view_this_file_unlock_please_view_this_file_unlock_please_view_this_file_unlock_please_view_this_file_unlock_please_view_this_file_unlock_please_view_this_file_unlock_please.html

Orange 进一步调查后表示该勒索软件可能与 Kodex Softwares（前身为 Evil Extractor）的网络犯罪组织出售的勒索软件有相似之处，但并没有直接证据。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

rudolfbrendlinkof1982@tutamail.com	evilant.ransomware@gmail.com	coomingproject@onionmail.org
brendangirhin@proton.me	barboza40@yahoo.com	spiderparadise@proton.me
Filesupport@airmail.cc	Linersmik@naver.com	bettercallarmin1@gmail.com
insomrans@outlook.com	Jinnyg@tutanota.com	germanmax26@outlook.com
zimmer1488@proton.me	Yourencrypt@tutanota.com	vgod@ro.ru
pzimmer1488@mailfence.com	Files4463@tuta.io	haxcn@proton.me
zimmer1488@2mail.co	RestorFile@tutanota.com	Kryptran@gmail.com
evilcorp_simulation@evilcorp.com	Vfemacry@mail-on.us	Krypt@onionmail.org
innokentiy@mailum.com	Bitmine8@tutanota.com	secretuser@tuta.io
innokentiy@onionmail.org	Barboza40@yahoo.com	secretuser@mailum.com
password2@tutamail.com	linersmik@naver.com	paul_letterman@zohomailcloud.ca
attack-tw1337@proton.me	jinnyg@tutanota.com	thomas_went@gmx.com
pwn3d@keemail.me	poluz@tutanota.com	wehavesolution@onionmail.org
coronaviryz@gmail.com	RestoreFile@qq.com	nsolution247days@outlook.com
korona@bestkoronavirus.com	oken@tutanota.com	systemfail@mailum.com
coronavirus@exploit.im	vfemacry@mail-on.us	nfortisram@zohomail.eu
corecrypt@hotmail.com	d3336666@tutanota.com	johncollinsy@proton.me
vijurytos@tuta.io	matrix9643@yahoo.com	robertokarlosonewtggg@outlook.com
vijurytos@cyberfear.com	redtablet9643@yahoo.com	Ghost_Kir4@proton.me
sspdlk00036@cock.li	bluetablet9643@yahoo.com	adver@mailum.com
taylorpaycrypto@onionmail.org	decodedecode@yandex.ru	anjelikaa733@gmail.com
taylorbtcpay@tutamail.com	decodedecode@tutanota.com	gretikola@outlook.com
bitcoin@2mail.co	askhelp@protonmail.com	hfghrebjr88@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）。

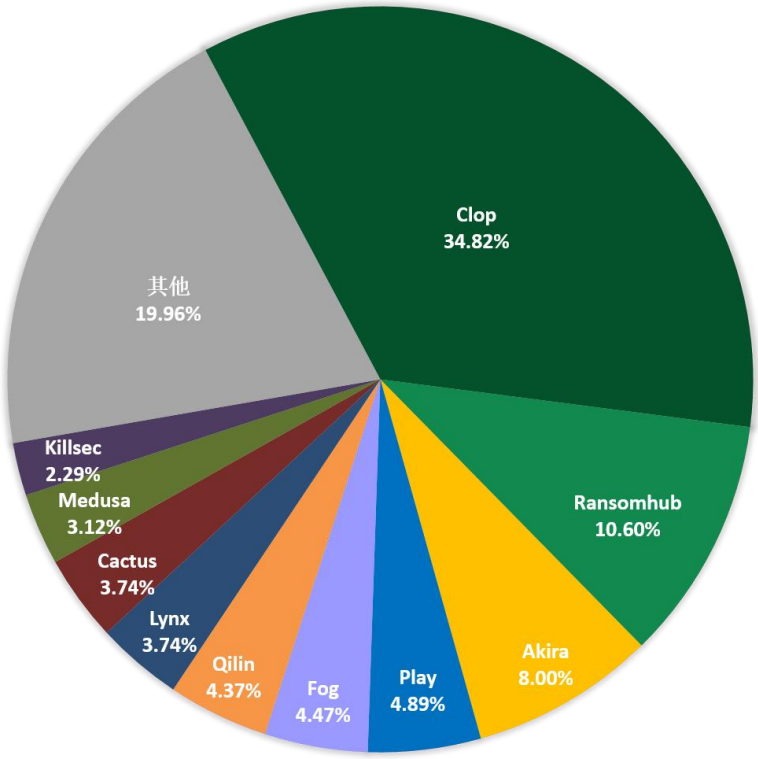

图 4. 2025 年 2 月通过数据泄露获利的勒索软件家族占比

以下是本月被双重勒索软件家族攻击的企业或个人。若未发现被数据存在泄露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 962 个组织/企业遭遇勒索攻击，其中包含中国 11 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 11 个组织/企业未被标明，因此不在以下表格中。

www.journeyoilfield.net	HANSONFASO.COM	Wakefield & Associates
www.casinoessentials.com	HANSONCOLDSTORAGE.COM	Prime Trust Financial
plasseramerican.com	HALGAND.COM	sehma.com
Engineering Mechanics	GARAN MANUFACTURING	Hammond Trucking & Excavation
Inversiones Clinica Del Meta SA	GARDNERHEALTHSERVICES.ORG	Rogers
ctpomd	GALATECHNOLOGY.CO.UK	I.B.G SPA
Houston Symphony	GREATPLAINSDISTRIBUTORS.COM	ldi-trucking-inc

sublettecountywy.gov	GULFSTATESCS.COM	Wisper Reimer Ingenieure GmbH
FORTFORWARDING.COM	GTIMPORTS.NET	Unimicron
www.townofbourne.com	GSMETALL.COM	Logix Corporate Solutions
Meta E2 F	Navien, Inc.	sole technology
Praxis Eins	FOODIMPORTGROUP.COM	TMC
CMCOLDSTORES.COMCODAGAMI.COM	FINLEYBEER.COM	primesourcestaffing.com
GOURMETTRADING.NET	FFL-GROUP.COM	The Children's Center Of Hamden
GNSWORLD.COM	FERNGROUP.COM	Old National Events Plaza
GIBSONHOMEWARES.COM	FAUSTDISTRIBUTING.COM	www.jsp.com
GHENT.COM	EMETER.COM	komline.com
GETGARVEYS.COM	EMDOMAIN4.LOCAL	bazcooil.com
GERSONANDGERSON.COM	EARLE.LOCAL	sdfab.com
GBBEV.COM	EXPORTPACKERS.COM	kaplanstahler.com
GATE7LLC.COM	EQLOGISTICS.US	EKONOM.COM
GAIAM.COM	EZUP.COM	EDITEL.EU
FASHION.PRI	EXCELLED.COM	DERRYTRANSPORT.COM
FLORENCECORPORATION.COM	ESSEXPOWERLINES.CA	DANA-CO.COM
FUN-WORLD.NET	ESBERBEVERAGE.COM	DESIGNDESIGNINC.COM
FOTE.COM	ENTERATEK.MX	DAATAGROUP.COM
FORDSTORAGE.COM	ENCHANTEACCESSORIES.COM	DUNNRITEPRODUCTS.COM
Lee Enterprises	THERMOTRAFFIC.COM	D2GO.IO
Mercury Paper Inc	UNITEDLEGWEAR.COM	DYNASTYFOOTWEAR.COM
teamwass.com	PHONONET.DE	DXC.COM
www.nasonptc.com	DZL	DUNDASJAFINE.COM
Donna G. Rogers, CPA, P.A.	Advantage Home Construction Insurance	DREXEL.CA
Thai Metal Aluminium Co., Ltd	Cronos Europa	DONLEN.COM
F&V Capital Management, LLC (FVCM)	Thornton EngineeringAustralia Pty Ltd	DLFNA.COM
Gilbert	denbyco.co.uk	DIRECTEX.NET
Sterling BMW	Metro Supply Chain Group.	DIAZFOODS.COM
jtu.com.br	amalgamatedsugar.com	DETECNO.COM
Autohaus Kießling	Planet One	DELTAENTERPRISE.COM
Soco systems	Johnson's Nursery	DELTACHILDREN.COM
Biogena GmbH & Co KG	Goldstein Law Group, S.C.	DECRESCENTE.COM
OneDealer	Northern Management	DBETANCES.COM
Finck Cigar	The Northwestern Illinois Association	DATAPAKSERVICES.COM
caltrol.com	www.famcomachine.com	COGLANS.COM
holtcat.com$1BUSA868GB<1% DISCLOSED	Bayteq	CYCLE.LOCAL
alphabaking.com$421.9MUSA1TB<1% DISCLOSED	WDNA	CASSINFO.COM
3cBSI	Naphix	CLAW.LOCAL

www.envirolabsinc.com	Digital Technology Co., Ltd.	CGDC.COTTONG.LOCAL
www.kppm.com	Shaghalni	CPS.K12.IL.US
Gitlabs: Synelixis Solutions, INGV, VMO Holdings	BluAgent Technologies, Inc	CONBRACO.COM
Story Environmental	Novi Community School District	CLEARON.COM
Muller Insurance	G&M Direct Hire	CRESTMILLS.COM
Nationz Technologies Inc.	ondaralogistica.com	CRANEBSU.COM
www.newburghhealthcarecenter.com	Afa Systems Ltd.	COVECTRA.COM
Kendall Auto Group	SPEED Co	CONNEXION-INFORMATIQUE.FR
www.obrienavocats.qc.ca	CCOO Servicios	COMPASSHEALTHBRANDS.COM
www.cmsg.cl	Al Bawani	COLLECTIONXIIX.COM
www.amerasphalt.com	Tristram European	COGHLANS.COM
www.emeryair.net	Martin Energy Group Services	CODAGAMI.COM
Chimu Agropecuaria S.A.	G&S Electric LLC	CMCOLDSTORES.COM
Omni United	Benton Police Department	CLASSICACCESSORIES.COM
Sound Ideas	Peter Glenn Ski Sport	CINEMA1.CA
powelltool.com	Excel Security	CHEROKEEDISTRIBUTING.COM
ITU AbsorbTech	evergreenpnw.com	CHEMSTARCORP.COM
Surface 678	alleghenybradford.com	CHALLENGER.COM
Fairhaven Shipyard Companies	teamsters175.org	CESARCASTILLO.COM
bluedge.com$104.5MUSA994GB<1% DISCLOSED	www.witheyaddison.com	CEDARSFOODS.COM
London Belgravia	Vvf Ilinois Services	CATHAYHOME.COM
National Legal Service	Siegel Group	CATCHUPLOGISTICS.COM
Rooks Rider Solicitors	(kc2) geokon.com	CASTLEWOODAPPAREL.COM
Arcandco	www.nola-law.com	CARLSONDISTRIBUTING.COM
Genea	www.electro-fusion.com	Enfin
Convert Solar	www.midwestvascular.net	D-7 Roofing
welcompanies.com	megamtls.com	Recievership Specialists
Radco Industries	planetone-asia.com	abcapital.com.ph
Island Realty	headcount.com	Allen & Pinnix
First Federal Savings & Loan	jindalgroup.com	Atlas Commodities
Benjamin Consulting Services	Luminus Management	The Pawn
Groupe Renault	Insyst GmbH	Adler Shine LLP
ALCOTT HR GROUP	guadeloupeformation.com	SimonMed Imaging
Vermeer Mexico	Paratus	PAD Aviation Technics GmbH
Friendship House	Barhite & Holzinger Inc.	Serenity Salon & Spa
www.avalon-hotel.com	statesideseattle.com	Michael’s Hair Body Mind
www.rgb.com	l.warsemann.fr	Greenwich Medical Spa
www.wpisd.com	www.fla-esq.com	Brockway Hair Design
www.ateliermonarque.com	www.elecgalapagos.com.ec	True World Foods
www.confabca.com	Crossroads Trading Company, Inc	MEDES College
hgmlegal.com	www.saracenproperties.com	Capital Cell Global (CCG)

lifting.com	palauhealth	ASRAM Medical College and Hospita
Merkanti Bank Ltd	newhorizonsbaking.com$163MUSA455GB<1% DISCLOSED	Polstermöbel Oelsa GmbH
tni.mil.id	gilcar.co	Marshall Motor Holdings
MNJ Technologies Direct	Medical File	Albright Institute
Mundelein Park & Recreation District	www.okddsi.net	WhoHire
South Georgia Accounting Services	conduent.com	Upstate Glass Tempering
Dinizulu Law Group LTD	eaglepost.com	Saied Music
essenzamovies.com.br	Andover Family Medicine	CAPITALFINEMEATS.COM
unila.edu.mx	Nebraska Irrigation	CALIFORNIARAINLA.COM
PPS Services Group	Mac Jee	CAINEWAREHOUSING.COM
ossc.mx	Waggonereng.com	BARCOMADE.COM
tequaly.com	www.selt-sistemi.com	BEINOGLOU.GR
Pulmonary Physicians of South Florida Clinics | Data security breach!	Minaris Medical America	BIAGIBROS.COM
Nichino Ryokka Co Ltd	californiaclingpeaches.com	BSIEDI.COM
Pound Road Medical Centre	Access2Jobs	BOZICKDIST.COM
Summit Home Health, INC.	www.phdental.com	BOWANDARROWPET.COM
Comercializadora S&E Perú	Berg Engineering Consultants, Ltd.	BOSSCHAIR.COM
First Defense Fire Protection	www.pransystems.com	BISSELL.COM (CLEO)
acmefan.com	M-1 TOOLWORKS	BESTBRANDSINC.COM
Executive Agenda	www.riverdale.edu	BERKSHIREINC.COM
Birdsall Muller LLC	ehdd.com	BENSONMILLS.COM
pacresmortgage.com	Ligentia	BENBECKER.EU
Xepa Soul	Supreme Administrative Court of Bulgaria	BAYSIDENH.COM
EMSON.COM	Ondunova	BARRETTDISTRIBUTION.COM
everelgroup.com$259MItaly440GB<1% DISCLOSED	Südkabel GmbH	BACKYARDDISCOVERY.COM
regulvar.com$253.5MCanada3.6TB<1% DISCLOSED	ziese.net	ALEGACY.COM
chfindustries.com	rwrhine.com	AURORAIMPORTING.COM
aiibeauty.com	foyernotredamedepaix.be	ARLAN.NL
formanmills.com	fastrans.com	ARKIEJIGS.COM
stuermer-maschinen.de	Hochschule	APOLLOCORP.COM
electrocraft.com	VISEO	AOL.COM AJ MISSERT INC
associatedasset.com	Vector Engineering, Inc	ANNABELLECANDY.COM
grede.com	Hall Law Group LLP	ANDROSNA.COM
branchgroup.com	Next TI	ANDREWSDISTRIBUTING.COM
pace-usa.com	Alabama Ophthalmology Associates	AMSINO.COM
steelwarehouse.com	DR.Claims FL LLC	AMERICANLIGHTING.COM
stanleyconsultants.com$190.5MUSA388GB<1% DISCLOSED	EzyLegal	ALPADVANTAGE.COM

compactmould.com	DBK	ALLTECH.COM
Aurora Boardworks	haleycomfort.com	ALLIANCEMERCANTILE.COM
Heartland Health Center	traffic-advertising-llc	AIRLIQUIDE.COM
Laurens School District 56	dr-elizabeth-bjornson	AGILITYAUTOPARTS.COM
WKKELLOGG.COM	Haggin Oaks Golf (hagginoaks.com)	AFFINITYCANADA.COM
WHEELS.COM	Eservices.gov.zm	ACTIAN.COM
WERTEX.COM	lake-washington-vascular	ACPIDEAS.COM
WENDOVERART.COM	h2o.ai	ACCEM.COM
WELCOMEIND.COM	BeniPlus	ABCOPRODUCTS.COM
VANDALE.COM	Brolly	3PLSOFTWARE.COM
VSSTRANSPORTATIONGROUP.COM	Revi	3FINITY.NET
VSSLOGISTICS.COM	Help Me Grow Yolo	1888MILLS.COM
VPGLOBAL.COM	NimuSoft	CXTSOFTWARE.COM
VLCDISTRIBUTION.COM	uniekinc.com	Israel Police Hacked
VIKINGWEAR.COM	midwayimporting.com	Kitty cookies
VIDAGROUP.COM	revitalash.com	www.cisco.com
VERSANTTECHNOLOGIES.COM	ranhillbersekutu.com.my	www.cdprojekt.com
VERSAILLES-INC.COM	bestbrands.com$25.5MUSA659GB<1% DISCLOSED	www.mgl.law
VALLEYDIST.COM	HCRG Care Group	www.fudpucker.com
UNIEK.INTERNAL	autogedal.ro	ctntelco.com
UNIVERSALWAREHOUSES.COM	www.mwmechanicalinc.com	Leading Edge Specialized Dentistry
USM-INC.COM	www.alphamedctr.com	iRidge Inc.
UPPERLAKESFOODS.COM	www.ccttechnologies.com	Maxvy Technologies Pvt
UNITERS.COM	www.copleystoughton.com	Universitatea Politehnica din Bucuresti
TITESI.LOCAL	www.macmed.com	Makesworth Accountants
TILLSONBURGHYDRO.CA	Decore-Ative Specialties	wwcsd.net
TWINSTARHOME.COM	Daniels Homes	Spectrum Solutions
TESISQUARE.COM	PREMIER HOUSEWARES LIMITED	Hpisd.org
TIMKEN.COM	lavi.co.il	Substitute Teacher Service
TWTDIST.COM	pyasolutions.com	SAKAI SOUKEN Co.
TRIPLE8.CA	Buanderie Centrale de Montreal	cmr24
TUXTON.COM	Bushmans	3SS
TUCKERCO.COM	kinseysinc.com	Fligno
TRIMACO.COM	steelerubber.com	Chalmers tekniska högskola
TRIBORO.COM	almostfamousclothing.com	teamues.com
TRENDSPOTINC.COM	HRS_IDEA_Expertises	Tropical Foods Company Inc
TPGXML.COM	Bulldog Oilfield Services	sautech.edu
TOTALWINE.COM	www.macter.com	nldappraisals.com
THENORTHWEST.COM	Cuna Supply	renmarkfinancial.com
THEMEZZSHOPPE.COM	Inland Empire Distribution Systems, Inc.	SmithDunn&Co

TERINICHOLS.COM	Wylie Steel Fabricators	northernresponse.com$17.4MCanada366GB<1% DISCLOSED
TARATOY.COM	Oxford Companies	savoiesfoods.com$18.2MUSA95GB<1% DISCLOSED
TALLTAILSDOG.COM	Stage 3 Separation	harcoboe.net
SAMSCLU.COM	Transkid	lowernazareth.com
SCHAWK.COM	Rheinischer Sch	zsattorneys.com
SJI.LOCAL	Startek Peglar & Calcagni	UNIEKINC.COM
STAR.LOCAL	Weed Man Canada	NG-BLU Networks
SCOPEIMPORTS.LOCAL	Robinson Family Dentistry	Presence From Innovation (PFI)
SDITECH.COM	Crager LaBorde	Lexington Electric
SUPPLYON.COM	The Townsley Law Firm Information	Robertshaw
SEA-DELIGHT.CA	danecourt.kent.sch.uk	HARADA
SUN-RICH.COM	toitoiusa.com	SmithDunn&Co
SENAO.COM.TW	lekiaviation.com	DIEM
STUDIODESIGNS.COM	bisindustries.com	Top Systems
STILACOSMETICS.COM	teamwass.com	eConceptions
STEVENSONBEERDISTRIBUTING.COM	hamton	McCORMICK TAYLOR
STEPHENJOSEPHGIFTS.COM	Hisingstads Bleck	www.iecsolutions.com
STELLARPACK.COM	Leadership Strategies	corehandf.com
STARMARKETINGCANADA.COM	Thong Sia	Dash Business
STANLEYCREATIONS.COM	ssmcoop.com$22.5MUSA26GB<1% DISCLOSED	Hall Chadwick
SPARTANLOGISTICS.COM	Autoschade Pippel	NESCTC Security Services
SOBELATHOME.COM	Pedensia Graphics Distribution	STORKCRAFT.COM
SLTRANS.COM	Winbas	Shinsung Delta Tech
SIMPLEHUMAN.COM	LINTEC & LINNHOFF Holdings	Banfi Vintners
SHIPGFS.COM	Swissmem	rablighting.com
SGKINC.COM	Woman's Athletic Club of Chicago	boostheat.com
SGEMESA.COM	Greencastle-Antrim Senior High School (gcasd.org)	annegrady.org
SEA-JET.COM	Allied Tenesis	Rural Health Services
SAUNDERSMIDWEST.COM	Bulverde Glass, Inc.	Mid-State Machine & Fabricating Corp
SATCO.COM	P.N. Sakkoulas	Toshapp.com
SANTAFENYSHOP.COM	DA Capital	A2b-cargo.com
SALTEDAWG.COM	COSMED	casperstruck.com
SALSON.COM	Persante Health Care	medicalreportsltd.com
SAKAR.COM	annegrady.org	mgainnovation.com
REVITALASH.COM	Pamrya.de	cornwelltools.com
REDCLAYGOURMET.COM	QBurst	rashtiandrashti.com
ROYALLEMKES.NL	Acqua development	Town Counsel Law & Litigation
ROUNDHOUSEGROUP.COM	Gpstech2007.com	Professional Computer Co., Ltd.
REV.DE	Mervis.info	LUA Coffee

REMAFOODS.COM	Realtime.tw	GFZ Helmholtz Centre for Geosciences
REGENCY-RIB.COM	saulttribe.com/kewadin.com	PT. ITPRENEUR INDONESIA TECHNOLOGY
REESEPHARMACEUTICAL.COM	www.310tempering.com	Devlion
REESECHEMICAL.COM	www.colacouronnelocations.com	SOLEIL
REDDYICE.COM	www.rowetactical.com	hemio.de
RDSGAMING.COM	www.transcend-info.com	Madia
RAYTIK.COM	www.naga.ae	X-lab group
RANDSTRUCKING.COM	www.cityoftarrant.com	Bolin Centre for Climate Research
RADLEY.COM	www.imgenterprises.com	escada.com
RACKSPACE.COM	www.solardatasystems.com	mielectric.com.br
QBTRANSPORTATION.COM	City of McKinney	engineeredequip.com
PTIDOM.LOCAL	Fortune Electric Co Ltd	emin.cl
PUROLATORINTERNATIONAL.COM	Northeast Delta Human Services Authority	alphascriptrx.com
PTCOUPLING.COM	halex.com	premierop.com
PRIMELINE.NET	(M)Empire-home-center	acesaz.com
PRESPERSE.COM	Heritage South Credit Union	mipa.com.br
PITSCO.COM	Castle Rock Construction Company	usm-americas.com
PIPERSYSTEMS.COM	Window World of Raleigh	feheq.com
PHYSICALDISTRIBUTIONSERVICES.COM	Hydronic & Steam Equipment	stewartautosales.com
PETMATE.COM	Ratioparts	milleraa.com
PERRONEANDSONS.COM	CST Corp	jsfrental.com
PEMAMERICA.COM	F.TECH R&D NORTH AMERICA INC.	summitmovinghouston.com
PELLONPROJECTS.COM	Primaveras	dwgp.com
PDSITE.COM	Nelson & Townsend, CPA's	easycom.com
PARTNER.RO	Genus	alfa.com.co
PANEUROFOODS.COM	www.calspa.it	westernwoodsinc.com
PAIGEDENIM.COM	brockbanks.co.uk	viscira.com
PAIGE.COM	Go Strictly	elitt-sas.fr
PACIFIC-TEXTILE.COM	Bethany Lutheran Church	cfctech.com
OUTSOURCELOGISTICS.COM	GANRO	armellini.com
OBJECTIF-EMBALLAGES.FR	Regency Media	mbacomputer.com
OREGONFRUIT.COM	The Agency	directex.net
OUTERSTUFF.COM	Shields Facilities Maintenance	360energy.com.ar
ONWBEER.COM	ADULLACT	saludsa.com.ec
OLDSPRODUCTS.COM	Ayomi	intercomp.com.mt
OFFICEBASICS.COM	Omydoo	sportadmin.se
O2COOL.COM	Aspire Rural Health System	C & R Molds Inc
NEBRASKAWAREHOUSE.LOCAL	leonardo.com - ROTORSIM-CAE	Commercial Solutions
NRESPONSE.COM	Mozo Grau (mozo-grau.com)	kksp.com
NORTHWIRE.COM	CoMo-Industrial Engineering	www.aymcdonald.com
NYCALLIANCE.COM	enventuregt.com	capstoneins.ca
NPLUS1TECHNOLOGIES.COM	snoqualmietribe.us	clarkfreightways.com

NMR.CO.UK	Nash Brothers Construction	mistralsolutions.com
NETPLUSTMS.COM	Nippon Steel USA	alojaimi.com
NATURESWEET.COM	Financial Services of America, Inc.	www.aswgr.com
MAPLELEAFFARMS.COM	Layfield & Borel CPA's L.L.C	heartlandrvs.com
MAGTARSALES.CA	Dain, Torpy, Le Ray, Wiest & Garner, P.C.	gaheritagefcu.org
MDS.LOCAL	vadatech.com	ITSS
MMSUPPLY.COM	Elite Advanced LaserCorporation	C2S Technologies Inc.
MCCUBBIN.COM	Dan Eckman CPA	SSMC
MAE.LOCAL	http://thermaseal.net	Rivers Casino and Rush Street Gaming
MCWILLIAMSMOVING.COM	curtisint.com	Asterra Properties
MYSTICAPPAREL.COM	britannicahome.com	Caliente Construction
MAINFREIGHT.COM	uniquehd.com	brewsterfiredepartment.org
MAHARTOOL.COM	Obex Medical	derrimon.com
MERCERLOGISTICS.COM	Cache Valley ENT	globexusa.com
METALANDWIRE.COM	JP Express	Dickerson & Nieman Realtors
MUXIE.COM	Central District Health Department	Sheridan Nurseries
MUNDI.COM	MORRISGROUP.CO	The Hill Brush
MORET.COM	stjerome.org	Woodway USA
MONARCHBRANDS.COM	Therma Seal Insulation Systems	Daniel Island Club
MGAINNOVATION.COM	Quality Home Health Care	KWS
MGAE.COM	Vicky Foods	DPC Development
METOOSHOES.COM	Squeezer-software	QGS Development
MERIDIANGROUPREM.COM	Spacemanic	gruppozaccaria.it
MERANGUE.COM	INGV	Glow Medi Spa
MEGATOYS.COM	alderconstruction.com	Grail Springs Retreat
MEDCODATA.COM	steveallcorn.remax.com	Karadeniz Holding (karadenizholding.com)
MCARDLESKEATH.COM	bergconst.com	Lakeshore Title Agency
MARELLI.COM	burdickpainting.com	Denton Regional Suicide Prevention Coalition
MAJORLABELGROUP.COM	columbiacabinets.com	www.origene.com
LOLLYTOGS.COM	ekvallbyrne.com	www.wongfleming.com
LAWSONROANOKE.COM	krmcustomhomes.com	smithmidland.com
LYNNS.COM	laderalending.com	GOVirtual-it.com (VIRTUAL IT)
LOSCABOSMEXICANFOODS.COM	minnesotaexteriors.com	coel.com.mx
LOSCAB.COM	rogerspetro.com	Ponte16 Hotel & Casino
LNFDISTRIBUTORS.COM	sundanceliving.com	Alford Walden Law
LITTLEARTH.COM	thejdkgroup.com	Pasco Systems
LENMAX.COM	twncomm.com	MPP Group of Companies
LEGALTRACKER.COM	Hess (hess-gmbh.de)	Elslaw.com
LEADINGLADY.COM	TJKM	DRI Title & Escrow
LAPOLICEGEAR.COM	askgs.ma	DPA Auctions

KEELEWL.COM	slchc.edu	Altair Travel
KWIKGOAL.COM	weathersa.co.za	Civil Design, Inc
KURTADLER.COM	Erie Management Group, LLC	The Gatesworth Senior Living St. Louis
KOLCRAFT.COM	tomsmithindustries.com	realtaxcanada.com
KOCHLOGISTICS.COM	Heartcentre	Tosaf
KNFILTERS.COM	North American Spares	usuhs.edu
KIRCHNERBEER.COM	EAC Consulting	Four Eye Clinics
KIKKERLAND.COM	MICRO MANUFACTRING	jpcgroupinc.com
KEELEWAREHOUSING.COM	Cold Storage Manufacturing	turbomp
JDADELIVERS.COM	The Brown & Hurley Group	Cyrious Software
JPWEST.COM	Societatea Energetica Electrica S.A.	Medical Associates of Brevard
JOHNPAULRICHARD.COM	Tie Down Engineering	Civic Committee
JOBAR.COM	Monroe Transportation Services Inc	Ayres Law Firm
JENNE.COM	Kensington Glass Arts	Growth Acceleration Partners
JAYAAPPARELGROUP.COM	Jildor Shoes	CHAMPIONHOMES.COM
JAGGEDPEAK.COM	Mainline Information Systems	Zamzow's
IDPE.CO	Fastighetsservice AB	DATACONSULTANTS.COM
IUSA.MX	Baltimore Country Club	CIERANT.COM
ID-GP.COM	CESI	DATATRAC.COM
INNOVADOR.COM.MX	Shinn Fu Company of America	Nano Health
thefireplacewarehouse.co.uk	ROCK SOLID Stabilization & Reclamation	My New Jersey Dentist
INTERFACTURA.COM	Neaton Auto Products Manufacturing	St. Nicholas School
INTERCHARGE.DE	O&S Associates	Héron
INTELEKTECHNOLOGIES.COM	Accelerator	Tan Teck Seng Electric (Co) Pte Ltd
INNOVSYS.COM	Saint George's College (saintgeorge.cl)	High Learn Ltd
HOMEDEPOT.COM.MX	Aurora Public Schools (aurorak12.org)	CAMRIDGEPORT
HPE.COM	Natures Organics	Wireless Solutions (Morris.Domain)
HP.COM	Paignton Zoo	Falcon Gaming
HOLLANDIADAIRY.COM	SRP Companies	Eascon
HIGHBARTRADING.COM	Braum's	Utilissimo Transportes
HENRYKA.COM	LACOLD.COM	GATTELLI SpA
HENDERSONSTAMPING.COM	The University of Notre Dame Australia (nd.edu.au)	Technico

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。

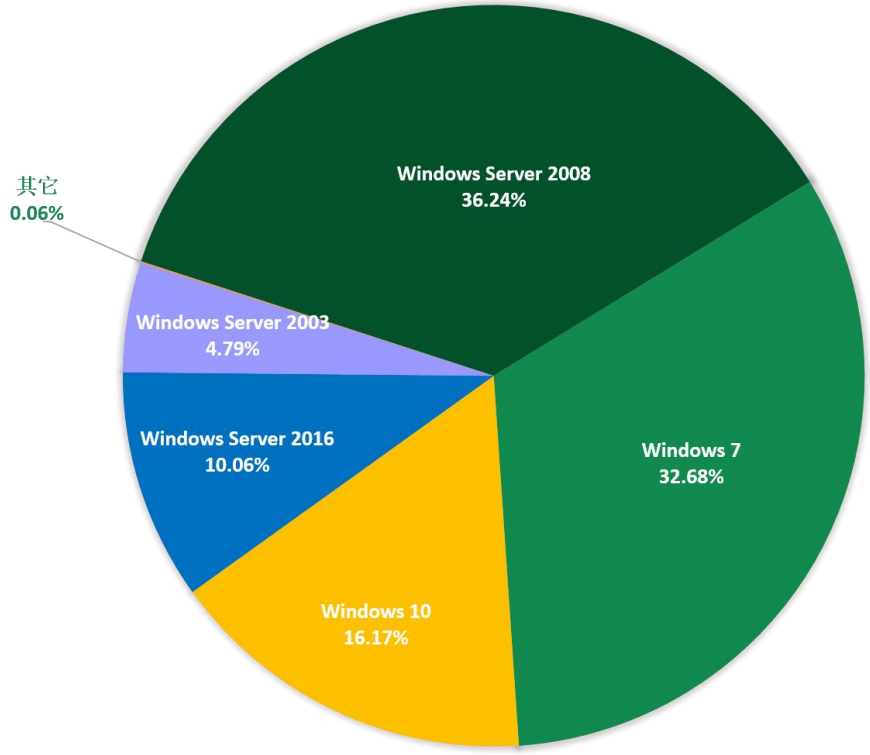

图 5 2025 年 2 月受攻击系统占比

对 2025 年 2 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。

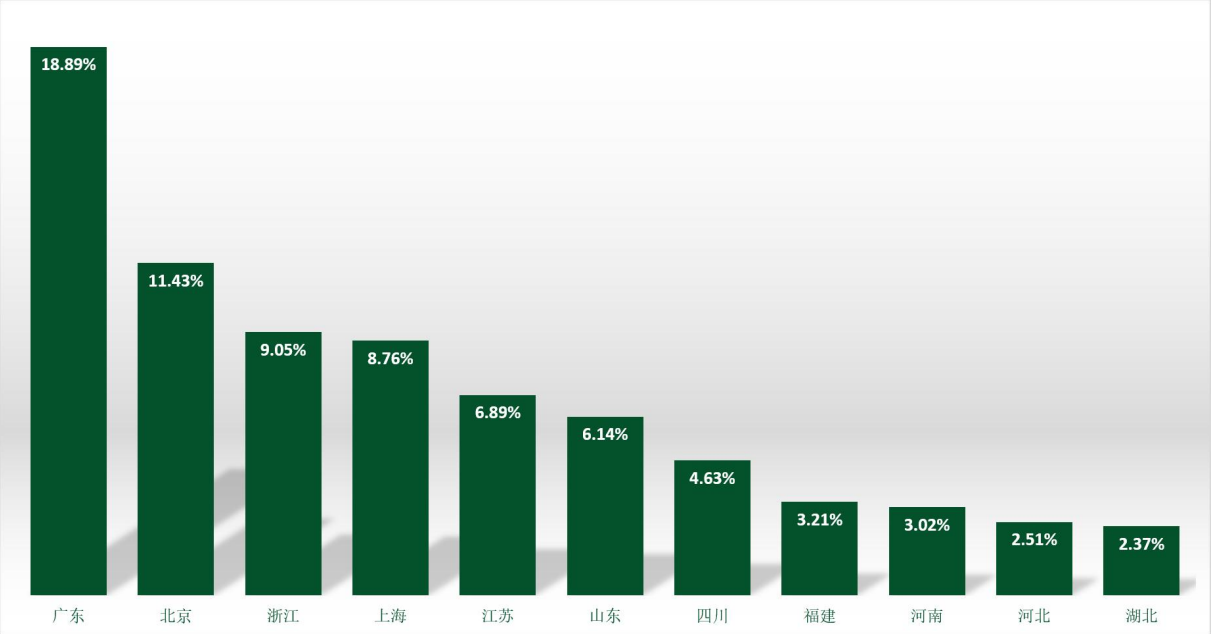

图 6. 2025 年 2 月国内受攻击地区占比排名

通过观察 2025 年 2 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。

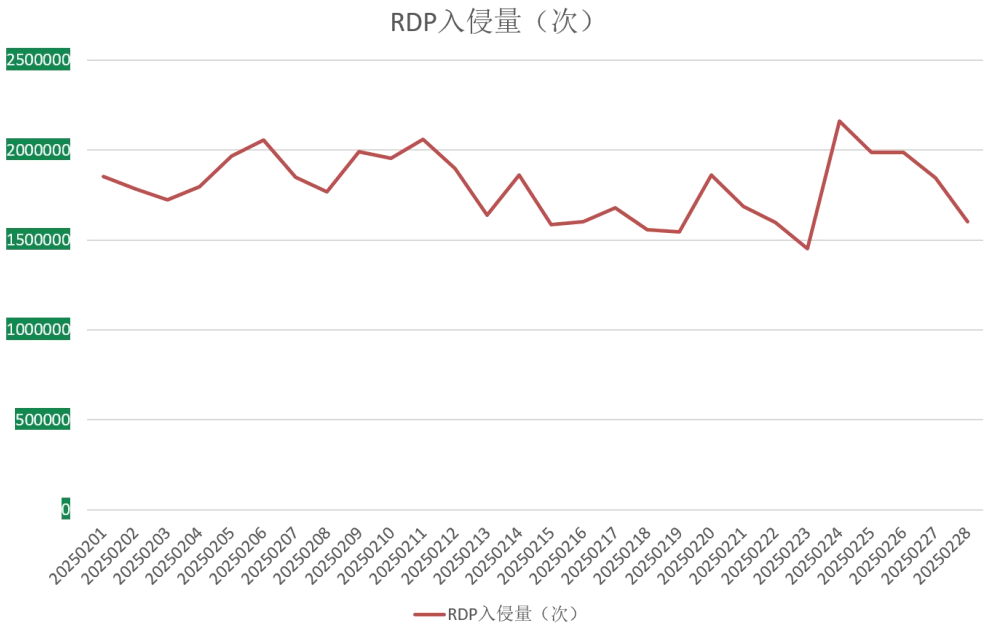

图 7. 2025 年 2 月监控到的 RDP 入侵量

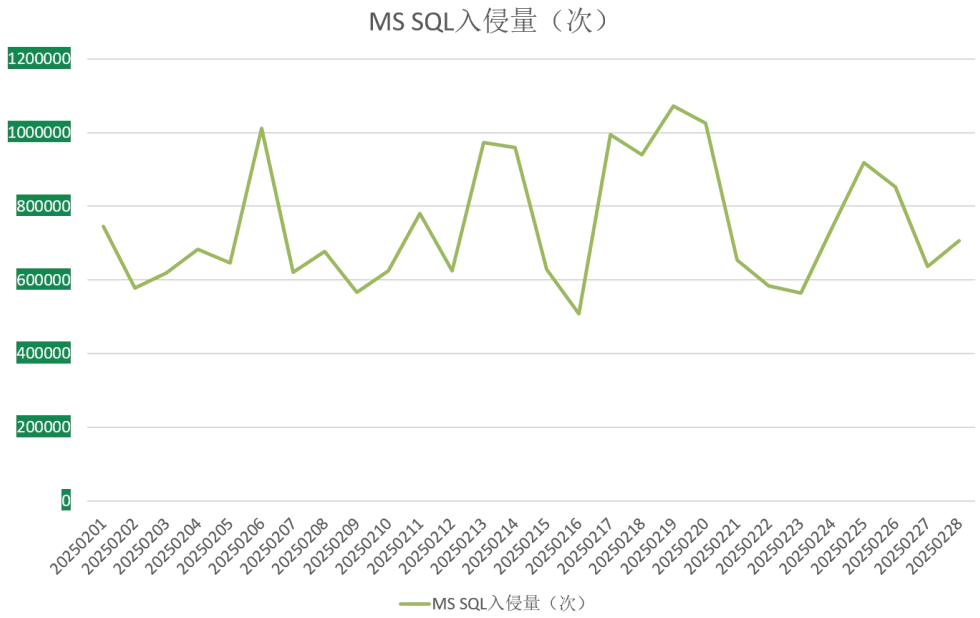

图 8. 2025 年 2 月监控到的 MS SQL 入侵量

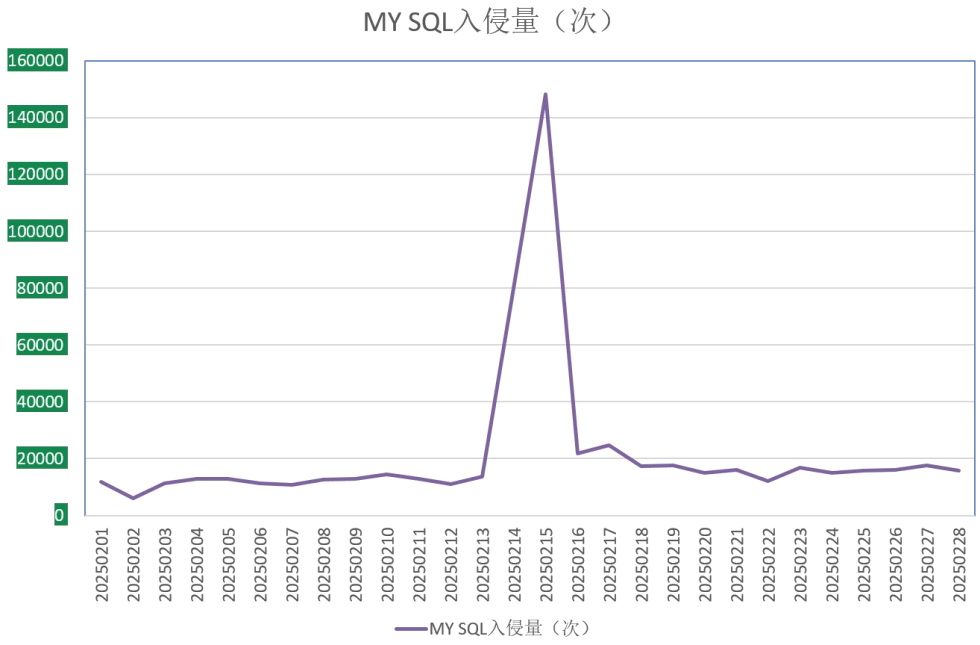

图 9. 2025 年 2 月监控到的 MYSQL 入侵量

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。

✧ wxr：属于 Weaxor 勒索软件家族，该家族之前的主要传播方式为：通过暴力破解远程桌面口令成功后手动投毒，以及类软件漏洞利用方式进行投毒。

- 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。
- 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。
- 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。
- baxia：同 bixi。
- wex：同 wxr。
- resback：同 mkp。
- sstop：同 wstop。m
- 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成功后手动投毒。devicdata:同 hmallox。

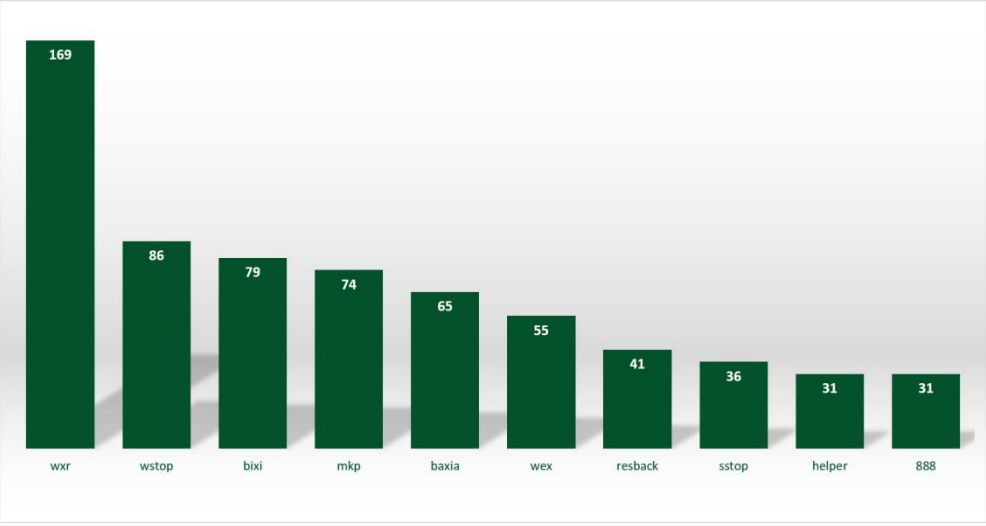

图 10 2025 年 2 月反病毒搜索引擎关键词搜索排名

解密大师

从解密大师本月解密数据看，解密量最大的是 Stop 其次是 Crysis。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。

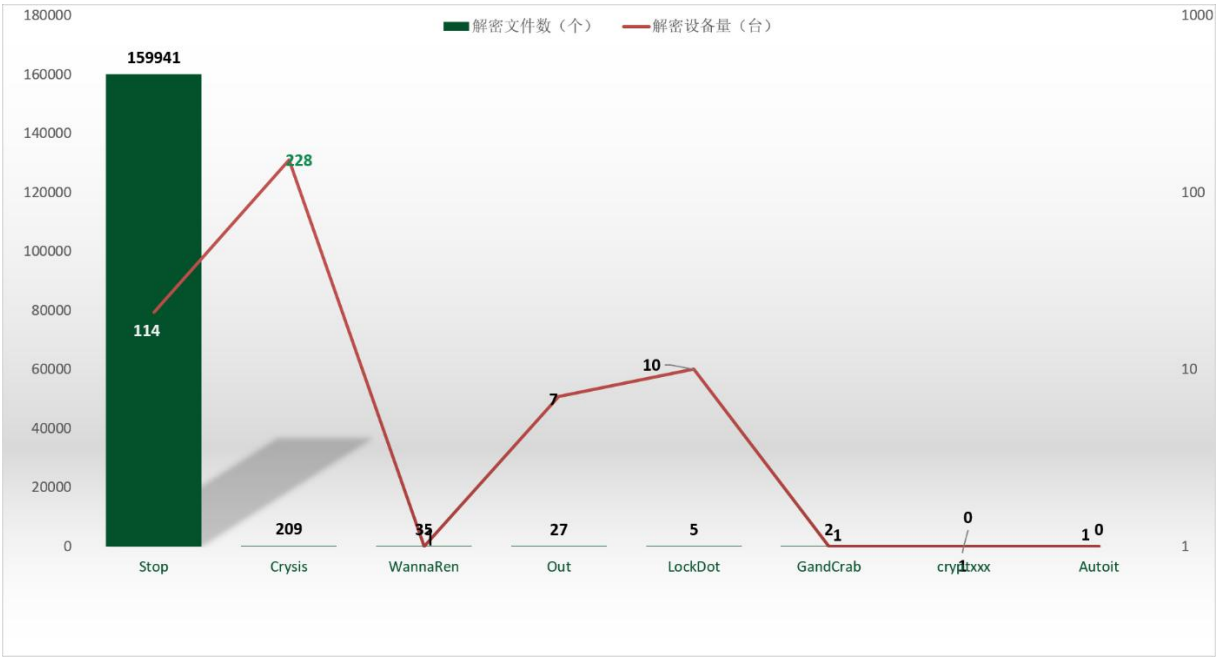

图 11. 2025 年 2 月解密大师解密文件数及设备数排名