

勒索软件流行态势分析

2025 年 3 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，为需要帮助用户提供 360 反勒索服务。

2025 年 3 月，全球新增的双重勒索软件家族有 Babuk2、Crazyhunter、Nightspire、Ralord、VanHelsing、Weyhro、Skira、Secp0、Arkana 等。

其中 Babuk2 是 Babuk 勒索软件的后续变种，运营者对 Babuk 勒索家族进行了仿冒。主要针对 VMware ESXi 平台实施攻击，采用 AES+RSA 加密算法及双重勒索策略（加密文件并窃取数据），Babuk 代码因在暗网部分泄露而增强了传播威胁。

CrazyHunter 最早现身于 2025 年 2 月，其使用 Prince 家族泄露源码构建。利用污染的 USB 设备作为初始攻击载体。当前该家族攻击的 10 个目标全部为中国台湾企业，涉及教育、医疗、体育、科技等行业。

NightSpire 攻击主要利用 FortiOS 漏洞（CVE-2024-55591）获取管理员权限进行初始访问，随后进行横向移动攻击。喜好对受害者进行施压，要求 2 天内支付并公开拒绝付款企业信息以削弱受害企业声誉。

RALord 利用 Python/Rust 开发加密器，以 RC4+PRGA 算法加密文件（扩展名 .RALord），重点攻击 Fortinet、SonicWall、Cisco 等企业设备，并偏好暴力破解与 CVE 漏洞利用；该组织以高分成比例吸引附属机构，提供工具链与暗网服务，疑似关联已关闭的 RA World（曾用 Go 存储样本，与停运的 FunkSec 代码部分相似）。

VanHelsing 勒索家族采用 C++ 编写，支持 Windows、Linux、BSD、ARM、ESXi 系统，具备跨平台威胁能力。运营方要求加盟者禁止攻击独联体国家，并通过区块链验证的 5000 美元保证金准入（优质攻击者可豁免）。加盟者分成 80%，运营方抽取 20%。

以下是本月值得关注的部分热点：

- 1** CISA 称 Medusa 勒索软件攻击了 300 多个关键基础设施组织
- 2** EncryptHub 利用 Windows 的 Oday 漏洞部署勒索软件
- 3** 勒索软件从网络摄像头对网络进行加密以绕过 EDR

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 35.97%居首位，第二的是 RNTC 占比 22.30%的，Makop 家族以 15.51%位居第三。

其中：Weaxor 家族最早出现于 2024 年 11 月，是 Mallox 家族的变种版本。该团伙重点攻击国内的用友 NC、亿赛通、蓝凌、明源、智邦、灵当、致远 OA、SQLServer 等 Web 应用和数据库，针对部分机器投递 CobaltStrike 进行远程控制，针对部分机器投递勒索病毒。

自 2025 年 1 月起此家族持续霸榜 Top1，赎金范围从 8 千到 1.5 万人民币间波动。

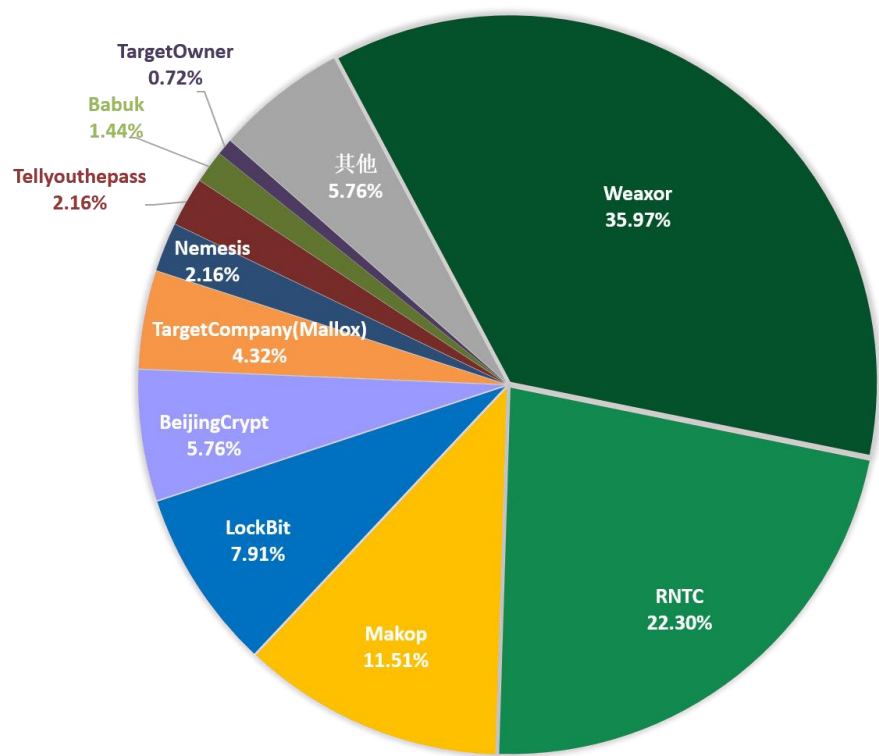


图 1. 2025 年 3 月勒索软件家族占比

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 7 以及 Windows Server 2012。

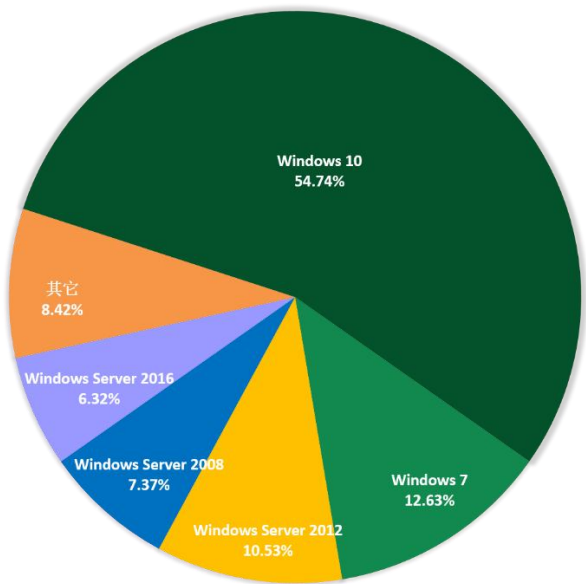


图 2. 2025 年 3 月勒索软件入侵操作系统占比

2025 年 3 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，NAS 平台以内网 SMB 共享加密为主。

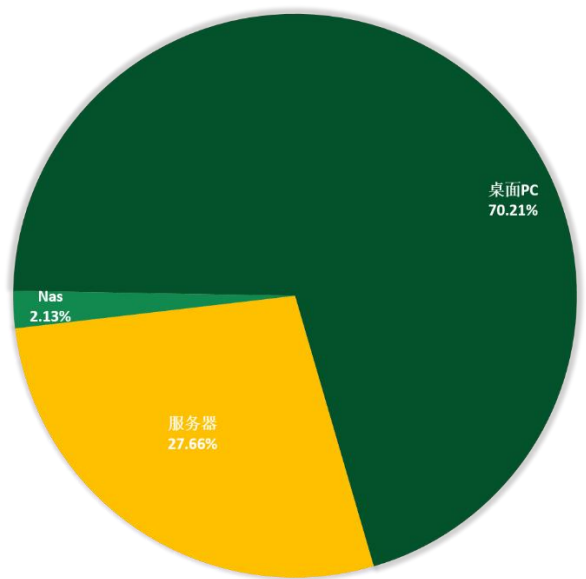


图 3. 2025 年 3 月勒索软件入侵操作系统类型占比

勒索软件热点事件

CISA 称 Medusa 勒索软件攻击了 300 多个关键基础设施组织

美国网络安全和基础设施安全局（CISA）表示，截至上个月，Medusa 勒索软件攻击行动已影响到美国关键基础设施领域的 300 多家机构。这一情况是在 CISA 与美国联邦调查局（FBI）以及多州信息共享与分析中心（MS-ISAC）近日联合发布的一份公告中披露的。

CISA、FBI 和 MS-ISAC 在 3 月 11 日发出警告称：“截至 2025 年 2 月，Medusa 勒索软件的开发者及其关联方已影响到来自多个关键基础设施领域的 300 多个受害者，受影响的行业包括医疗、教育、法律、保险、科技和制造业。”……“FBI、CISA 和 MS-ISAC 鼓励各机构实施本公告‘缓解措施’部分中的建议，以降低 Medusa 勒索软件事件发生的可能性并减轻其影响。”

正如公告所解释的，为防范 Medusa 勒索软件攻击，建议防御者采取以下措施：

- 修复已知的安全漏洞，确保操作系统、软件和固件在合理时间内完成补丁更新。
- 对网络进行分段，限制受感染设备与机构内其他设备之间的横向移动。
- 过滤网络流量，阻止来自未知或不可信源对内部系统远程服务的访问。

Medusa 勒索软件大约在四年前，即 2021 年 1 月首次出现。但该犯罪团伙的活动直到两年后的 2023 年才开始增多。当时，他们推出了 Medusa Blog 数据泄露网站，以被盗数据为筹码施压受害者支付赎金。自出现以来，该团伙声称在全球有 400 多个受害者。2023 年 3 月，在宣称对明尼阿波利斯公立学校区（MPS）发动攻击并分享被盗数据视频后，该团伙引起了媒体的关注。2023 年 11 月，丰田汽车公司旗下的丰田金融服务公司拒绝支付 800 万美元的赎金要求并通知客户数据泄露后，该团伙还在其暗网勒索门户上泄露了据称从该公司窃取的文件。

EncryptHub 利用 Windows 的 Oday 漏洞部署勒索软件

名为 EncryptHub 的攻击组织与利用本月修补的 Microsoft 管理控制台漏洞的 Windows 系统 Oday 攻击有关。

研究人员发现，此安全功能绕过（CVE-2025-26633）存在于易受攻击设备上的 MSC 文件处理方式中。攻击者可以利用该漏洞来规避 Windows 文件信誉保护并执行代码，因为在未修补的设备上加载意外的 MSC 文件之前，用户不会收到警告。

研究人员在向 Microsoft 报告漏洞之前发现的攻击中，EncryptHub（也称为 Water Gamayun 或 Larva-208）使用编号为 CVE-2025-26633 的 Oday 漏洞来执行恶意代码并从受感染的系统中提取数据。在整个攻击活动中，攻击组织部署了多个与之前的 EncryptHub 攻击相关的恶意负载，包括 EncryptHub 窃取程序、DarkWisp 后门、SilentPrism 后门、Stealc、Rhadamanthys 窃取程序和基于 PowerShell 的 MSC EvilTwin 木马加载程序。

此外，EncryptHub 还会部署勒索软件载荷，其主要合作的勒索组织为 RansomHub 和 BlackSuit。

值得一提的是，EncryptHub 攻击组织在广泛进行各类攻击活动外，还以“SkorikARI”名义向微软提交漏洞（如 CVE-2025-24071、CVE-2025-24061），并获得了微软官方致谢。

勒索软件从网络摄像头对网络进行加密以绕过 EDR

有人发现 Akira 勒索软件团伙利用一台未受保护的摄像头对受害者的网络发动加密攻击，成功绕过了原本在 Windows 系统中阻止加密程序的端点检测与响应（EDR）系统。

值得注意的是，Akira 团伙最初试图在 Windows 系统上部署加密程序，但被受害者的 EDR 解决方案拦截，之后才转而利用摄像头发动攻击。这些攻击者最初是通过目

标公司暴露在外的远程访问解决方案进入企业网络的，很可能是利用了被盗的凭证或通过暴力破解密码得逞。进入网络后，他们部署了合法的远程访问工具“AnyDesk”，窃取了该公司的数据，用于实施双重勒索攻击。接着，Akira 团伙使用远程桌面协议（RDP）进行横向移动，在部署勒索软件有效负载之前，尽可能地将其控制范围扩展到更多系统。最终，攻击者投放了一个受密码保护的 ZIP 文件（win.zip），其中包含勒索软件有效载荷（win.exe），但受害者的 EDR 工具检测到并隔离了该文件，基本上阻止了这次攻击。

此次攻击失败后，Akira 团伙开始探寻其他攻击途径，他们对网络进行扫描，寻找可用于加密文件的其他设备，结果发现了一台网络摄像头和指纹扫描仪。攻击者选择网络摄像头是因为它容易受到远程 shell 访问攻击，并且其视频流可以被未经授权查看。此外，该摄像头运行的是基于 Linux 的操作系统，与 Akira 的 Linux 加密程序兼容，而且它没有安装 EDR 代理，因此是远程加密网络共享文件的理想设备。

安全分析团队证实，攻击者利用网络摄像头的 Linux 操作系统挂载了该公司其他设备的 Windows SMB 网络共享。然后，他们在网络摄像头上启动了 Linux 加密程序，并通过 SMB 协议对网络共享进行加密，成功绕过了网络上的 EDR 软件。

这个案例表明，EDR 防护并非万能的安全解决方案，企业不应仅仅依赖它来防范攻击。此外，物联网设备不像计算机那样受到密切监控和维护，但仍然构成重大风险。因此，这类设备应与生产服务器和 workstation 等更为敏感的网络隔离开来。同样重要的是，所有设备（包括物联网设备）都应定期更新固件以修复可能在攻击中被利用的已知漏洞。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

Decoding@qbmmail.biz	lockhelp1998@skiff.com	adresspower@tutanota.com
Cost1BTC@protonmail.com	summerkiller@mailfence.com	data_guram@tutamail.com
bitcoin@email.tg	genesis1337@tutanota.com	guram24@onionmail.org
onioncrypt@aol.com	ghost1998@tutamail.com	b10694a2d90e3a69@mail2tor.com
onion@nigge.rs	webroothooks@tutanota.com	zsszyy@mailum.com
3998181090@qq.com	boramae@mailum.com	cypt@tuta.com
info@cloudminerapp.com	mr.jokerpalfinger1984@gmail.com	backuprestore@mail.ee
fortisram@zohomail.eu	supersupp@mailum.com	restorelocki@my.com
alexpetrov11094@gmail.com	supersupp@startmail.com	Anubis@mailum.com
alexanderpetrov20200@gmail.com	Bluecrap8@gmail.com	Anubis20@firemail.de
bitlocker@foxmail.com	Bluecrap@my.com	npomocit02@surakshaguardian.com
asauribe@tutanota.com	solodiner@seznam.cz	636231621397832@cock.li
ghostbackup@skiff.com	xinoz@cock.li	693132169321893@tutamail.com
cringghost@skiff.com	louisblanc@mailum.com	Resp0nse1999@tutanota.com
retryit1998@mailfence.com	louisblanc@firemail.de	Resp0nse1999@tutanota.com
crptbackup@skiff.com	pasmunder@zohomail.eu	data.revival@onionmail.org
retryit1998@tutamail.com	famerun@email.tg	m0sc0vlum@tutanota.com
d3crypt@onionmail.org	worldofdonkeys@protonmail.com	astralocker2@tutanota.com
rsacrpthelp@skiff.com	worldofdonkeys@xmpp.jp	metro777@messagesafe.io
d3svc@tuta.io	xueyuanjie@onionmail.org	Elons1890@mailum.com
rsahelp@protonmail.com	xueyuanjie@mail2tor.com	MattVenom@proton.me
eternalnightmare@tutanota.com	xueyuanjie@exploit.im	Redemption1441@gmail.com
just4money@tutanota.com	schipkealfred@gmail.com	whatswrongscareddd@gmail.com
sdghost@onionmail.org	tianrui@mailum.com	brain.support@cyberfear.com
evilcorp@skiff.com	MedusaSupport@cock.li	woodpecker@onionmail.org
kellyreiff@tutanota.com	mds.svt.breach@protonmail.com	fluxsocy@cock.li
fileunlock@onionmail.org	medusasupport@cock.li	king_size_banana@freemail.hu
kevlnt@tuta.io	bones800@protonmail.com	king_size_banana@tutanota.com
shadowghosts@tutanota.com	h3llr4ns@onionmail.com	edgypsin@proton.me
fortihooks@protonmail.com	zphc@cock.li	

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)。

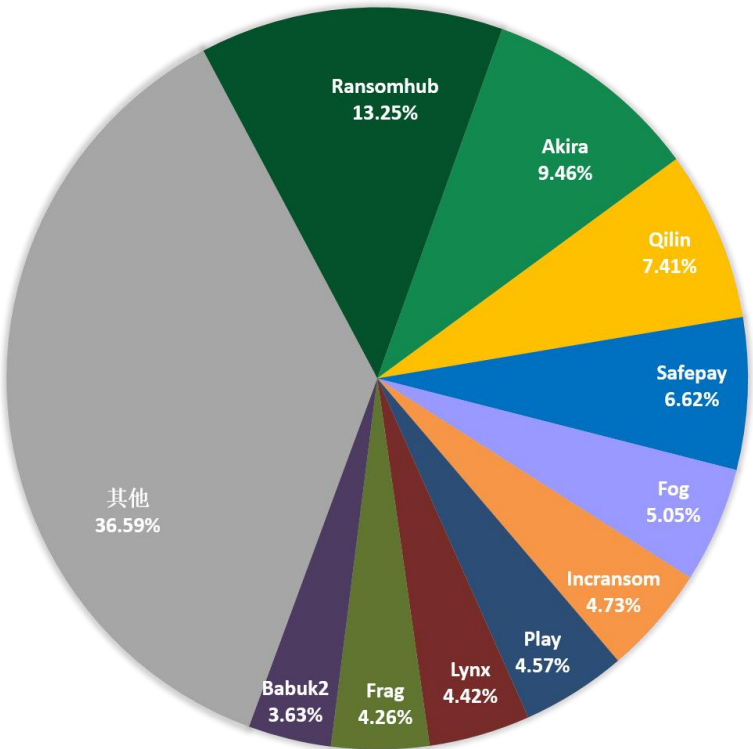


图 4. 2025 年 3 月通过数据泄露获利的勒索软件家族占比

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 634 个组织/企业遭遇勒索攻击，其中包含中国 16 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 2 个组织/企业未被标明，因此不在以下表格中。

Groupe Sinari	PMA	Skyward Specialty Insurance
Bunger Steel	Precision Accounting Intl	Trymata
goosehead.com	Ambleside	Gaines County, Texas
Pak Technologies	abeyor.fr	Springfield Water and Sewer Commission
Evans Distribution Systems	architekturbuero-heller.de	Longue Vue Club
Transcore	AutoCanada	ciscientific.com.au
pln.co.id - PLN INDONESIA	Doumen	SIRIUS S. R. L.
moh. gov. rw	Zaveta Custom Homes	Suder&Suder
Lee & Sakahara Architects	Goshen Medical Center	WAUGH & GOODWIN, LLP

Kyocera Document Solutions Europe	REOC San Antonio	wmk-hvb.de
Design Design	Yadea Group Holdings Ltd	Veristat
CMC Technology Group	Colemanmaterials	All4Labels – Global Packaging Group
Meridian Senior	Advance Tapes International	Essex County OB/GYN Associates
Saunders and Saunders	MinebeaMitsumi Inc	Edesur Dominicana
Sonrisas Dental Health	SPARSH Hospital	Princeton Hydro
Hartmann Stanyak Bürosysteme	Innovative Surfaces	fnde.gov.br brazilian government
REPROHAUS Corp	jp-property.com	lexmark.com Company
Virserius Studio	Aztec Municipal School District	Wilkinson Rogers (wilkinsonrogers.com)
Ste Group Key Corp	compassionhealthcare.org	forvismazars.com.fr (mazars.fr) By Babuk Locker 2.0
AKTO	gbsn.com.br	fredsalvuccicorp.com
Élan Sportif Nantes	www.avalonapparel.com	Magnolia Manor (magnoliamanor.com)
Ihara company	armetal.com	dccsagroup.com&csahome.com
Zuni Data	www.scpautomation.com	Mandarin.com.br By Babuk Locker 2.0
Analog Integrations Corporation	www.gestionquintessence.com	GARANIMALS.COM
Formosa Chang	www.engines.man.eu	Callico Distributors, Inc.
Netronix Inc	www.abmenviro.ca	Pacific Honda Company
TEPAS	www.accessfinanceonline.com	Arcusin
creativeunited.org.uk	www.ahmadiyya.ca	Safe-Strap Company, LLC
brightonaustralia.com.au	www.elizajennings.org	www.hexosys.com
tieraerzte-warburg.de	www.sinkdirect.com	Fickling & Company
system-toolsgmbh.de	www.broadmoormethodist.org	The Loretto Hospital
vinylvisions.com	www.parklandmanufacturing.com	GPS 909
estilointeriors.co.uk	www.oneupinnovations.com	Dacas Argentina
swr.school	www.solinst.com	Asia University
albrecht-partner-steuerberatung.de	www.allstarhealthcaresolutions.com	ACTi Corporation
alpsteel.com	www.njcalwe.com	Cotswold Fayre
blunk-gmbh.de	www.gcsnet.com	Vercoe Insurance Brokers
cjs-buerodienstleistungen.de	www.core-1.com	Steel Dynamics UK
beaudry.ca	www.esquirebrands.com	E Leet Woodworking
bohrerhof.de	Cayman National Bank	Customer Management Systems
metallogicinspection.com	bellendorf.de	CPI Books
comfort.de	CS Plastics	emperors.edu
vcvitanzasons.com	Officio Medical	wog-kaiserbaeder.de
tramann.de	Subsurfco LLC	BerksBar.org
schuhbode.de	yano.tokyo	williampevear.com
norson.com	www.mslglobalexp.com	baldaufarchitekten.de
fd-friedrich.com	L&S Mechanical	Clawson Honda
westwarwickwelding.com	Whittaker & Company	prelco.ca
prestigeer.com	www.georgehay.co.uk	KH OneStop
ecconstructors.com	www.janvier-labs.com	Salemerode.com

wrm. org	Land Planners	State Bar of Texas (www. texasbar. com)
retycol. com	Auren	Greenwood Village South GVS
marcom-inc. ca	Oag. state. va. us	Buckley BalaWilson Mew
adolphelawgroup. com	Wr-recht. de	Jerue Companies
wagner-transporte. com	Baltimorecityschools	Syma-System
children-ne. org. uk	Obra Play	Compound Solutions
mayaassurance. com	interiseworld. com	T J Machine & Tool
importantsteps. com	Instituto de Ojos	Gevril
National Defense Corp	National Safety Council	Peak Season
www. assisi. nl	Augusta Industrial Services, Inc.	Yorke & Curtis
bahnlog. com	Champions Group	Holiday Comfort
dapope. com	J McCann & Co Ltd	Dectron
Town of Orangeville	Big Horn County School District #4	Nor Arc
O'Shea Builders	ZB ZIMMERMANN UND BECKER GmbH	British virgin islands London Office
Thaon-les-Vosges	Newtown Friends School (newtownfriends. org)	Insider Technologies Limited
hardmanjohnston. com	woqod. com	Changhua Christian Hospital
charlesjones. ca	Cargills Bank	Huacheng Electric
blue-hive. com	Luff Industries	Mackay Hospital
derianhouse. co. uk	Megacentro	www. dcarosolutions. com
bedfordma. gov	www. kvhealth. net	mittchellmcnutt. com
frazierllp. com	controlledair. com	www. jpwindustries. com
mmmbbs. net	Q railing	Tech NH
Geass	www. medsr. com	Allworx
Transsion Holdings	Los Madroños Hospital	Island Realty
solaroptimum. com	The Ely Company, Inc.	Minnesota Orthodontics
Forrest City School District	Machu Picchu Foods	REYCOTEL
phaus. us&phakr. com&phabodysystems. com	LINC Systems	Hancock Public School
Martin Mechanical (martin. local)	VEST LLC	total-ps. com
AJF Inspections & Engineering ()	Palomino Petroleum	lofotenseafood. com
Commercial Concrete Systems	warmsworth. doncaster. sch. uk	ADDA (adda. io)
augustssons. se	alphaoil. ca	www. cdg. us
pereclaver. org	CD	Swift Haulage Berhad
www. bassi. it	newhollandwood. com	bayvillage. org
Superior Forge & Steel	Coopertruni	Aj Taylor Electrical Contractors Ltd
S. S. White	THX Transport	ACDC Express
unired. uz	Kiribati Government	Sittab INC
Kaspar Companies	Gloria Cales	wheats. com
agakam	Atos-racks. com	srmg. com. au
UNITED OPTICS GmbH	Ted Hosmer Enterprises	City government office in Van (Turkey) - van. bel. tr
entandallergy. com	AMICIO	RFA Decor

wieso-cert	5ltalk.com	Central Electropolishing Company, Inc.
acm	PTS Group	Resnick & Caffrey, PC
Lupin Limited	JAMEL CONTAINERS LLC	Avantune Corporation
Wildeck Inc	expertdata.com.au	MBI International, Inc.
www.allmilmo.com	Cleveland Municipal Court	Fragola S.p.A
ihara.com.br	airtelligence.com	Tugwell Pump & Supply
brattenelectricn.com	SAGETRA INC.	www.portlandschools.org
amatechinc.com	gaertnerhof-jeutter.de	www.hinton.ca
Manning Materials Corp.	sp.tnitelecom.com	agi.net
City of Fort St. John (city.cityfsj.local)	Harcourts Prime Properties	www.centersheetmetal.com
NAI Earle Furman	Bridgewater Retirement Community	www.convention.qc.ca
Senior Support Services	assaabloy.com	hickorylaw.com
REIMERS FURNITURE MFG INC	kyb.com	Dynamic Closures
NEW JERSEY CPA	Electronics For Imaging	Adval Tech
Ebassi.com (E.B. Archbald and Associates)	Lepant Law Office	lovesac.com
heras.co.uk	Worldlawn Power Equipment	WJCC Public Schools (wjccschools.org)
alliedwoundcare.com	Diode Technologies	Connektd, Inc.
crimgroup.com	www.baxterlaboratories.com	Ministry of Foreign Affairs of Ukraine
aman-iraq.com	ccktech.com	Naples Heritage Golf & Country Club
www.fkm-elemente.de	terrell.k12.ga.us	Oberlin Cable Co-op (oberlin.net)
Hansa Solutions	oneill.com	1X Internet
TOGA	www.jhayber.com	Bizcode
Helbor	Solist	Manning Publications Co.
Monette Barakett	RAE (Real Academia Española) (rae.es)	Engikam
compumedics.com.au AND neuromedicalsupplies.com	CableVision	FHNW
www.hongthongrice.com	www.cityofbellville.com	Aeonsparx
conterra.com	PIBOR ISO SA	CIE
TriCity Family Services	SMC Corporation	Flightsim studio
Oregon Surveillance Network - OSN!	KIU System Solutions	Neopoly
Austring Fairman & Fekete	KD Panels	Kr3m
R&K Drysdales	Kairav Chemofarbe Industries	InfoReach
Roshan Packages	consultoria-consultores.es	Euranova
Initiative Var	ROBONG-WINMINI	Inelmatic
Benkin Sheet Metal 2008 Ltd	Lake Psychological Services	Kotliva
Elmos	CANAM Realty Group	Inet
The PNST	CNS	Blue Planet

www.DSelectrical.com	la-z-boy	Eumetsat
tomioingenieria.com.ar	sitro.com.au	Melexis
ec-nantes.fr	SRP Companies (Second lock! + Company scam!)	USGS
Direct Traffic Control	Coldwell Banker D' Ann Harper, REALTORS	Law Diary (USA)
saiedu.fi	Kleen-Pak Products	Carruth Compliance Consulting
kalesavunma.com - KALE SAVUNMA.	Moncaro	CCL Products India
Kimco Steel	DTS -services	Krisala Developer (India)
B&C Industries	Dane Court Grammar School	Pervedant
usCalibration	www.ameda.com	willms-fleisch.de
gettys.com	Courageous Home Care	LIPPERTENT.COM
Primary Flow Signal: Flow Meters Flow Measurement	Tanaka Electronics Taiwan Co.,LTD	SCOLARO FETTER GRIZANTI & McGOUGH, P.C. (scolaro.com)
Curtain Bluff	Fireplace Warehouse	www.black-star.fr
I. A. T. S. E. Local 667/669	Waihong Environmental Services Limited	Adrenalina
Plaza Brasília Hotéis	Wilson Re Limited	Cyncly Company
AAYLEX ONE S.A.	MESS sales srl	City Plumbing & Electric Supply Co
fepasa.com.ar	Ascom Holding AG	www.sunsweet.com
bioclimaservice.it	Ricardo Rodriguez	www.japanrebuilt.jp
www.carolinaac.com	Casale Del Giglio	www.cda.be
www.garbinc.com	yeanshalle.de	Schmiedetechnik Plettenberg GmbH & Co KG
www.mododoc.com	Fulcrum Lifting	Chicago Doorways, LLC
www.argentosc.com	Perrigo Company	Best Collateral, Inc.
www.ripplejunction.com	argusdatainsights.de	365labs - Security Corp
www.creativelogisticservices.com	Domina Entrega Total	Phoenix
www.afnigc.ca	Unicorr Packaging Group	PFS Grupo - Plan de igualdad, Sostenibilidad
www.cormidom.com.do	ideconstruction.com	dsrny.com
www.lions-online.org	jennyoo.com	Pampili (pampili.com.br)
ossc.com.mx	Bancroft Wines	Keystone Pacific Property Management LLC
Primex Farms LLC	Tryon	Mosley Glick O' Brien, Inc.
Wide Open West - WOW!	Indiv Usa	FANTIN group
Okeene Elementary School	Portland Street Honda	Ray Fogg Corporate Properties
6ixty8ight	Karen S Pouliot	Grupo Baston Aerossol (baston.com.br)
Sanyo Special Steel India Pvt. Ltd.	mdm-insurance.com	Seabank Group
KHAZMODAN STUDIOS	Cothron's Security Professionals	rockhillwc.com
MISR AL MAHABA HOSPITAL	nuclep.gov.br. Nuclep Brazil	bpmmicro.com
McMillan James Equipment Company (MJEC)	Terralogic	peruzzi.com

Montgomery Little & Soran, PC	rixos.com	goencon.com
texascompressionservices.com	dtrglaw.com	Tata Technologies
Omnitracs	SL Tennessee Information	Wendy Wu Tours
Grupo Santillana	Harrells.com	IOVATE.COM
allbiz.com	Best Cheer Stone	Legal Aid Society of Salt Lake
www.solidworld.it	fstlogistics.com	Ewald Consulting
www.s3s.com	Backes	Netcom-World
www.rivaldt.com	World Wide Fittings	InternetWay
OMLTD.CO.JP	www.raymond.in	Sunnking SustainableSolutions
technicare.com	University Diagnostic Medical Imaging, PC (udmi.net)	drvitenas.com
cisd.org	El Camino Real Academy (elcaminorealacademy)	quigleyeye.com
Family Health Services, Inc	Milano	familychc.com
mmn.hu	Far East Consortium International Limited	andreyevengineering.com
Business Software Solutions	baillie.com\$130.5MUSA52GB<1% DISCLOSED	usarice.com
TMT Clam Dredger	tempe1.com	LINKGROUP
iberdrola.com (Spain energy)	thermoid.com\$183.2MUSA199GB<1% DISCLOSED	Openreso
studiodclvallone.it	rocketstores.com\$738.9MUSA3.2TB<1% DISCLOSED	Itapeseg
Wheels and Deals	urban1.com	logic insectes
AmeriKen Die Supply, Inc	Raja Ferry Port Public Company Limited	RJ IT Solutions
Andrew Davidson & Co., Inc.	Business Ledger Limited	Grafitec
AeroWorx	Tohpe Corporation	synaptic.co.tz
Bunting Capital Management Inc	Baily International of Atlanta	ICO
California Gasket and Rubber Corporation	Hydro-Vacuum S.A.	Utsunomiya Central Clinic
Community Management, Inc.	Ascoma Group	La Uni ó n
Ellis Glass and Mirror Ltd	TUV India Pvt. Ltd.	ceratec.com
Texas Fifth Wall Roofing Systems	marinabaysands.com - Singapore Hotel (Internal Server)	Central McGowan (centralmcgowan.com)
FRANKLIN PRODUCTS	Yushin America, Inc	Klesk Metal Stamping Co (kleskmetalstamping.com)
Kontane Logistics, Inc.	PACOMARTINEZ	Forstenlechner Installationstechnik
Lake Beverage Corp.	SMG Bahamas	Ganong Bros
Maine Highlands Federal Credit Union	CAHOKIA CUSD 187 SCHOOL DISTRICT	Couri Insurance Agency
Red Credit solution, LLC	Best Telecom Laos	Pre Con Industries
Moody Homes	Industrial Acceptance Corporation	IT-IQ Botswana
iTEK Services, Inc.	CNQC	North American Fire Hose

Komoto Healthcare	Peerless Food Equipment	M&n Management
Nelson Law Firm	Helmut Hölbling Spedition GmbH	Optometrics
Opulent	India's telecommunication network	International Process Plants
Rahnama Law	www.visualisation.one	gruppocogesl.org
QUILTcraft	HOST Software Entwicklung und Consulting GmbH	Bell Ambulance
Salvi, Schostok & Pritchard P.C.	HYPONAMIRU	Workforce Group
Southwest Inspection and Testing	HYPERNOVA TELECOM	FM. GOB. AR
STATEWIDE ENTERPRISES	Baykar Turkish defense company C4I and artificial intelligence By Babuk Locker 2.0	neatem.fr
Stuwarooij	airexplore.aero Company	germancentre.sg
Superior Technology, Inc.	wapda.gov.pk By Babuk Locker 2.0	breakawayconcretecutting.com
Woodbine Hospitality	tradingacademy.com	Kable Product Services
SEAQUEST SEAFOOD	ultimateclasslimo.com	City of Aurora
www.exemplar.com	havenresorts.com	APTEAN.COM
www.solventacentroamerica.com	lgipr.com	JEFFREYCOURT.COM
Johnson Fitness	jockeysalud.com.pe	GS Floor Designs
Groupe des Industries Métallurgiques	motomecanica.com	Newton & Associates, Inc
General Formulations	cali.losolivos.co	

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。

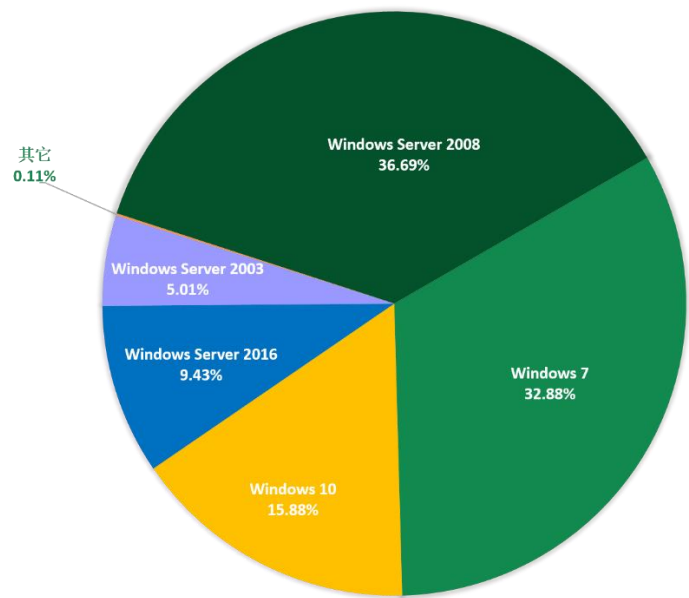


图 5 2025 年 3 月受攻击系统占比

对 2025 年 3 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。

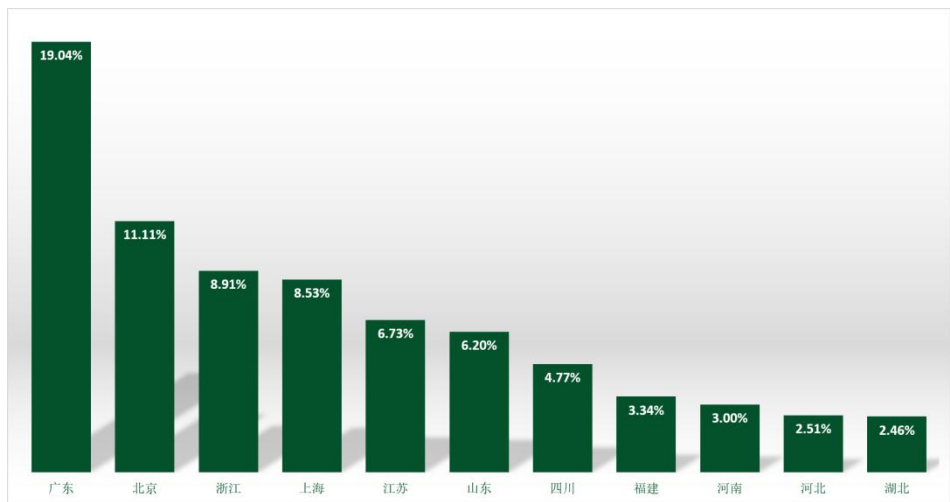


图 6. 2025 年 3 月国内受攻击地区占比排名

通过观察 2025 年 3 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。

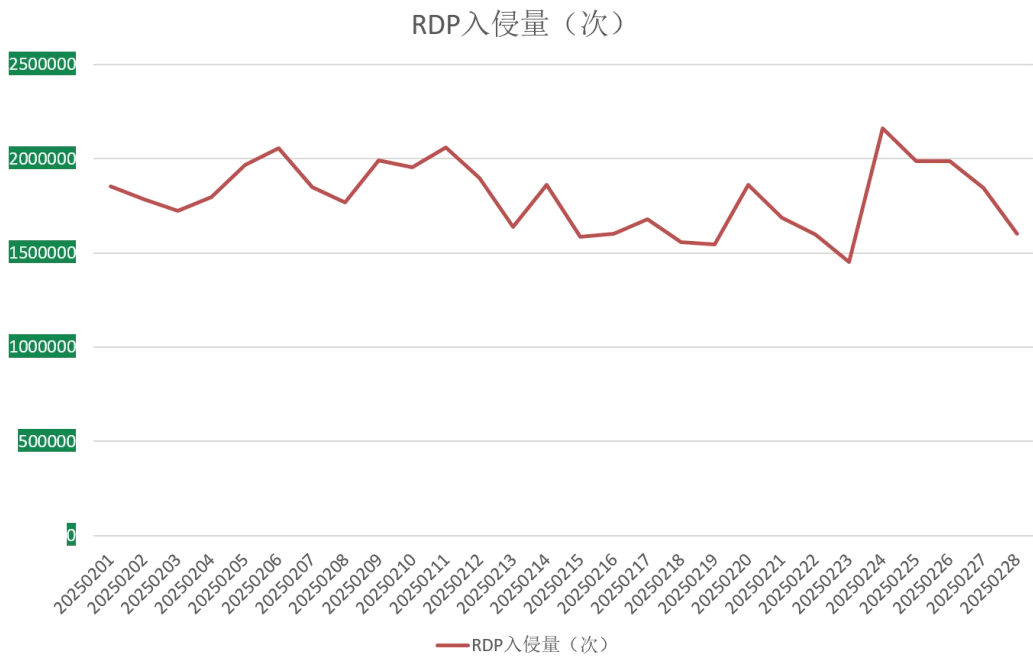


图 7. 2025 年 3 月监控到的 RDP 入侵量

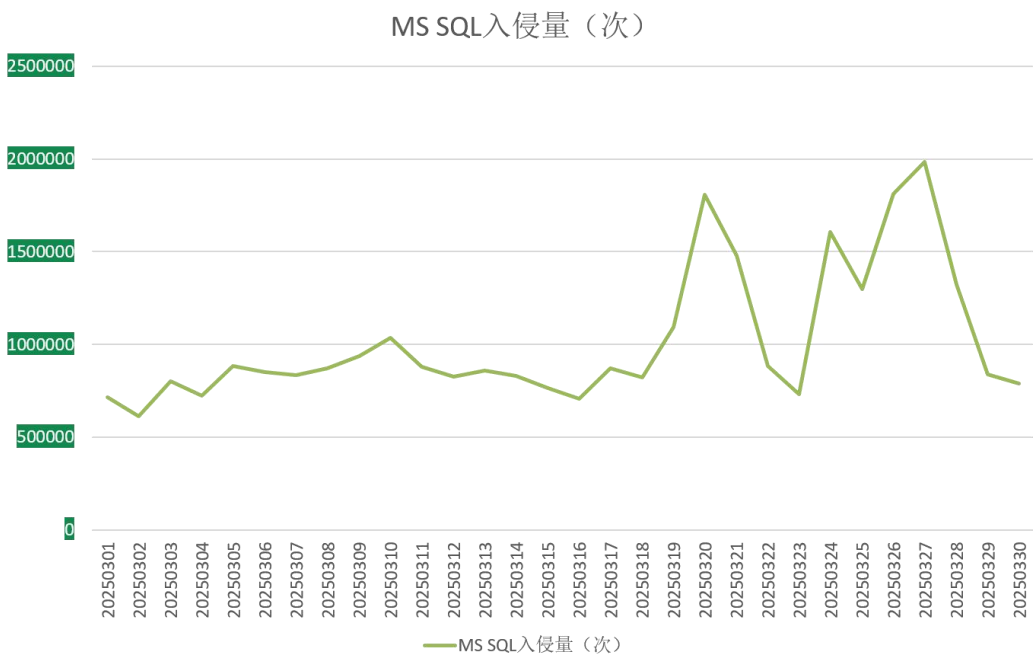


图 8. 2025 年 3 月监控到的 MS SQL 入侵量

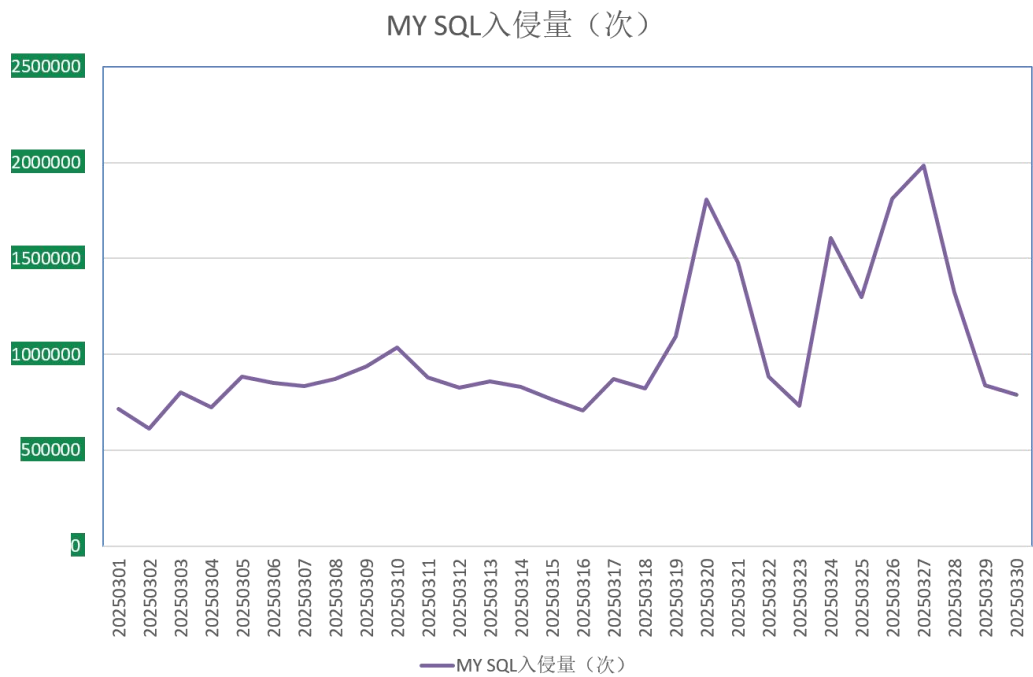


图 9. 2025 年 3 月监控到的 MYSQL 入侵量

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，该家族目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。
- ✧ sstop: 同 wstop。
- ✧ baxia: 同 bixi。
- ✧ 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。
- ✧ wex: 同 wxr。
- ✧ wxx: 同 wxr。

✧ devicdata: 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。该分支主要通过暴力破解远程桌面口令成功后手动投毒。

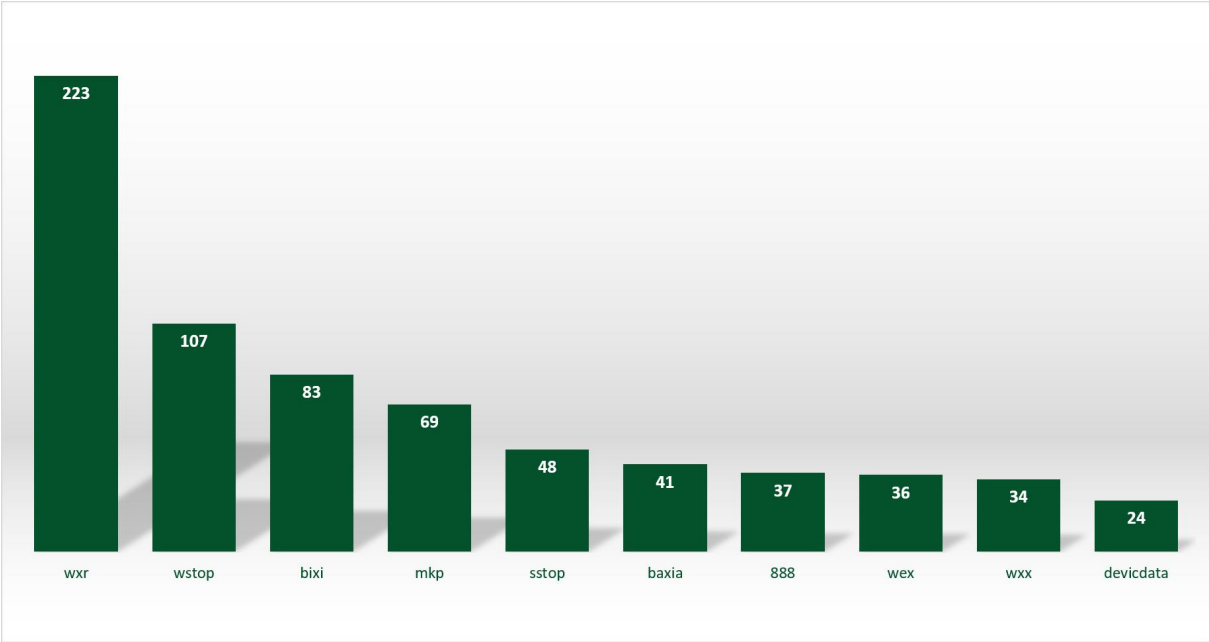


图 10 2025 年 3 月反病毒搜索引擎关键词搜索排名

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 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。

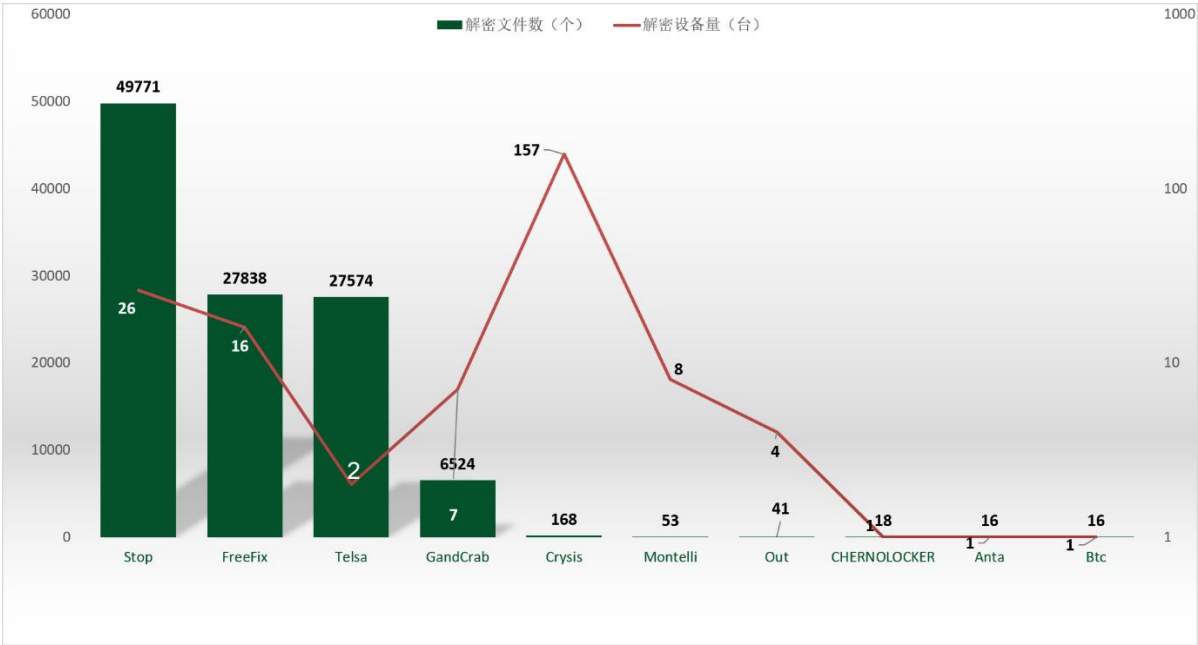


图 11. 2025 年 3 月解密大师解密文件数及设备数排名