勒索软件流行态势分析

2025 年 6 月

三六零数字安全科技集团 | 高级威胁研究分析中心

勒索软件传播至今，360 反勒索服务已累计收到数万次勒索软件感染求助。随着新型勒索软件的快速蔓延，企业数据泄漏风险不断上升，勒索金额在数百万到近亿美元的勒索案件不断出现，勒索软件对企业和个人的影响和危害也越来越大。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 6 月，全球新增的双重勒索软件有 WarLock、Kawa4096、TeamXXX 等多个家族，传统勒索软件新增 UraLocker、SafeLocker 等家族。

本月 360 反勒索服务团队接到大量 Weaxor 勒索家族的反馈，经技术人员分析排查发现该家族勒索软件主要是利用企业 OA 系统漏洞进入到内部网络的。我们也针对性的发布了相关分析报告和解决方案。

以下是本月值得关注的部分热点：

1. **Anubis 勒索软件添加了擦除器来阻止文件恢复**
2. **Krispy Kreme 表示，去年 11 月的数据泄露影响了超过 16 万人**
3. **迈凯伦医保表示，数据泄露影响了 74.3 万名患者**

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 52.24%居首位，第二的是 RNTC、占比 11.94%，BeijingCrypt 家族以 7.46%的占比位居第三。

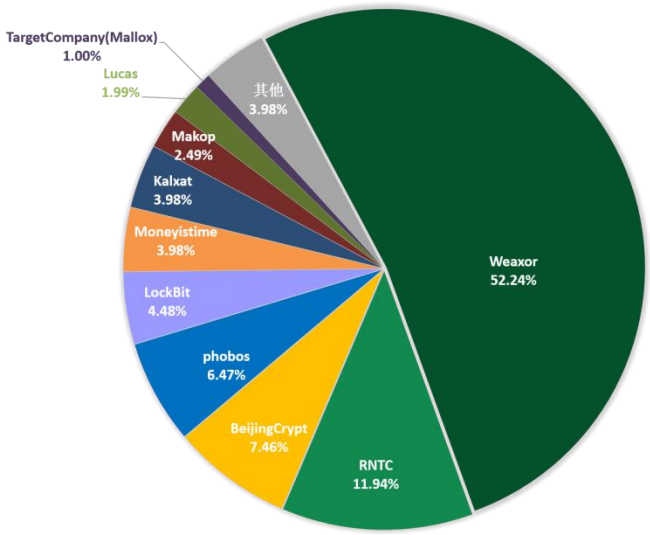

图 1. 2025 年 6 月勒索软件家族占比

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 7。

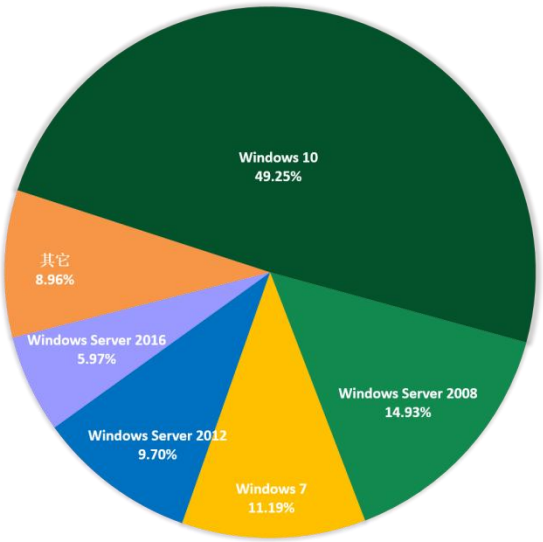

图 2. 2025 年 6 月勒索软件入侵操作系统占比

2025 年 6 月被感染的操作系统占比显示，受攻击的系统类型中，桌面 PC 系统大幅领先服务器系统。

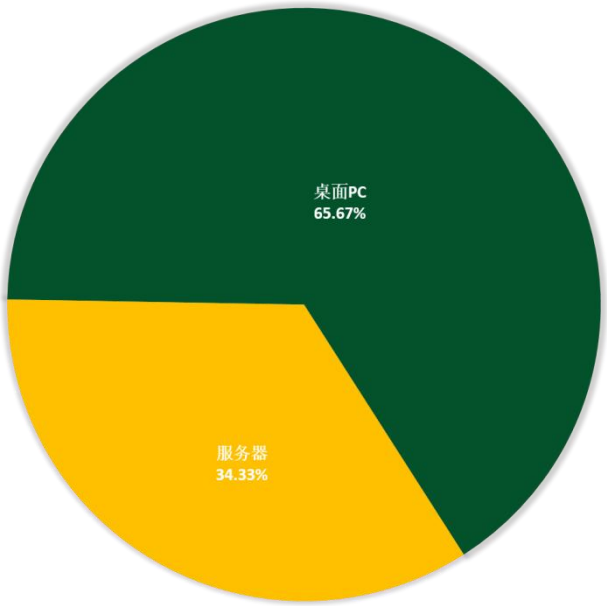

图 3. 2025 年 6 月勒索软件入侵操作系统类型占比

勒索软件热点事件

Anubis 勒索软件添加了擦除器来阻止文件恢复

近期，我们发现 Anubis 勒索软件在文件加密工具中，添加了一个擦除器模块。该模块会销毁目标文件，即使支付了赎金也无法恢复。目前，Anubis 在暗网上的勒索页面只列出了 8 名受害者。

6 月 13 日，一份安全研究机构的报告显示，Anubis 团伙在代码中添加了一些新功能，其中也包含了文件擦除功能。研究人员通过分析最新 Anubis 样本，发现了擦除器功能，认为该功能是为了让受害者在压力之下付款。其代码会识别命令行参数“/WIPEMODE”激活破坏性行为，该参数需要发出基于密钥的身份验证。激活后，擦除器会擦除所有文件内容，将其大小减小到 0KB，同时保持文件名和结构不变。受害者仍能看到预期目录中的所有文件，但其内容已销毁且无法恢复。

相关机构的分析显示，Anubis 在启动时支持多个命令，包括用于权限提升、目录排除和目标路径加密的命令。默认情况下，重要的 system 和 program 目录被排除在外，以避免导致系统完全不可用。勒索软件还会删除卷影副本，并终止可能干扰加密过程的进程和服务。

该勒索软件加密代码使用了 ECIES 算法，并在加密文件后附加“.anubis”扩展名。完成加密后，在加密目录中放置了 HTML 赎金记录，并且尝试更改桌面壁纸。

Krispy Kreme 表示，去年 11 月的数据泄露影响了超过 16 万人

美国甜甜圈连锁店 Krispy Kreme 证实，攻击者在 2024 年 11 月的一次网络攻击中，窃取了超过 16 万人的个人信息。

Krispy Kreme 透露，在今年 6 月下旬提交缅因州总检察长办公室的一份文件中，其在去年 11 月遭遇的数据泄露已影响 161676 人。虽然该公司没有透露事件中暴露了哪些

数据，但提交马萨诸塞州总检察长的另一份文件显示，被盗文件包含受影响个人的社会安全号码、金融账户信息和驾驶执照信息。

Krispy Kreme 于 2024 年 11 月 29 日在其 IT 系统上检测到未经授权的活动，并在 12 月 11 日提交美国证券交易委员会的文件中，披露了该事件及其在线订购中断的情况。该公司还采取措施遏制漏洞，并聘请了外部网络安全专家来评估攻击对其运营的全面影响。

虽然 Krispy Kreme 始终尚未公布有关 11 月数据泄露事件的更多细节，但 Play 勒索软件团伙在去年 12 月下旬声称对此次攻击负责，称他们还从该公司网络中窃取了数据。

Play 勒索软件声称，其窃取到的文件包含：

- 个人机密数据
- 客户文件
- 预算
- 工资单
- 会计账单
- 合同
- 税务缴纳 ID
- 财务信息

最终，Play 勒索软件团伙在与该公司谈判失败后，于 12 月 21 日在其暗网泄露网站上发布了多个档案，其中包含数百 GB 文件。

迈凯伦医保表示数据泄露影响了 74.3 万名患者

迈凯伦医保组织警告 74.3 万名患者，2024 年 7 月发生的 INC 勒索软件攻击，导致其卫生系统发生数据泄露。虽然攻击是在 2024 年 8 月 5 日被发现的，但确定攻击影响的司法调查直到 2025 年 5 月 5 日才完成，相关通知直到 6 月 20 日才发布。

2024 年 8 月初，迈凯伦医保组织遭遇 IT 和电话系统中断，促使其进行调查。据报道，患者数据库受到影响，人们在访问迈凯伦医院时，被要求携带有关预约和药物的信息。尽管该组织没有具体说明攻击者情况，但迈凯伦位于密歇根州贝城的一家医院的一名员工在网上发布了 INC 的勒索信息，这些勒索信息会通过医院的打印机自动打印。

在发送给受影响个人的通知中，迈凯伦医保组织承认该事件涉及勒索软件攻击，但仍未提及 INC。本次调查确认，攻击者在 2024 年 7 月 17 日至 2024 年 8 月 3 日期间，拥有迈凯伦和 Karmanos 系统的访问权限。

在提交给美国当局的迈凯伦数据泄露样本中确认患者姓名信息已泄露，并增加了其他已泄露的数据类型。因此，数据泄露的整体情况仍不清楚。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

c0mrade@cyberfear.com	Delavencei@tutanota.com	forinquiries@cock.li
Lucas2000@firemail.de	File_acce@tuta.io	recov_supp@firemail.de
Lucas2000@cyberfear.com	zelenskyy.net@mailum.com	Watkins@firemail.cc
g6o0e9@sina.com	spiderweb@cock.li	Ruiz@firemail.cc
bender@nigge.rs	taller@2mail.co	fdid@tutamail.com
Mikhopui@mailfence.com	taller@cyberfear.com	bondbond1@protonmail.com
basta2025@onionmail.com	JQWOFIoiQWF@fogmail.cc	williamh@tuta.com
chesterblonde@outlook.com	blackandwhite@cock.li	dinhvanhie@bk.ru
uncrypt-official@outlook.com	openpgp@foxmail.com	dinhvanhieuhd88@gmail.com
dendrogaster_88095@protonmail.com	lissykemiki@tutamail.com	decryptcore@gmail.com
programroo@cock.li	sandrasimontrigov@outlook.com	decransom@gmail.com
SkFJwbEhwmZjdEhw@mailum.com	alessandro1967@onionmail.org	titan@laboo.boo
TheHiBroHi@proton.me	theomassalini2002@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，勒索软件也让数据泄露风险越来越大。以下是本月通过数据泄露获利的勒索软件家族占比，该数据仅包含未第一时间缴纳赎金或拒缴纳赎金的部分企业或个人（已经支付赎金的企业或个人，可能不会出现在这个清单中）。

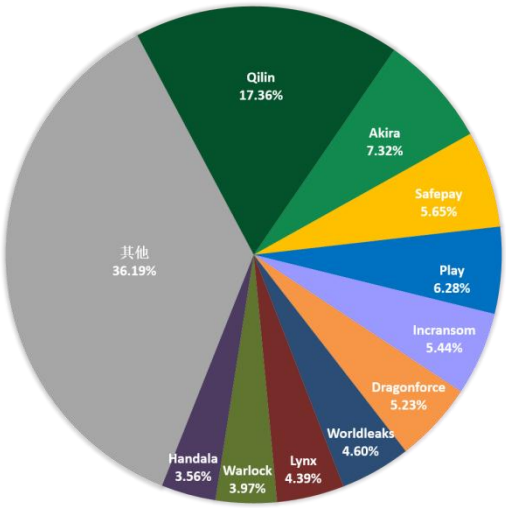

图 4. 2025 年 6 月通过数据泄露获利的勒索软件家族占比

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 478 个组织/企业遭遇双重勒索/多重勒索攻击，其中，中国 6 个组织/企业遭受双重勒索/多重勒索，另有 8 个组织/企业未被标明，因此不在以下表格中。

simmons-Boardman Publishing, Inc	AFECC - Hospital Santa Rita de Cássia	JELGAVAS TIPOGRAFIJA
Portel Logistic Technologies	RADIX	peterpauper
semco-tech.com	varico Poland	interiorsgroup.ie
www.nuphoton.com	Feng Chia University	narvikhavn.no
www.malonebailey.com	THAIRUNG GROUP	event-medical.com
oandg.com.au	GB Group	nationwidecare.org
Hotam EC	nipro.com	webberrestaurantgroup.com
entab.se	gmaxequine.com	belkorpAg.com
Murex Petroleum	fiestafranchise.com	Parkway Construction LLC
HRConnects, LLC	realityfinance.com	K.M. Packaging Co., Ltd
Meleam S.p.A.	nardinifire.com	Medifarma
Budget Electric	hparchitecture.com	Health-Insights
Epcatalogs Company	kontek.com	Mount Rogers Community Services
ClockWorkAdmin	mileschristi.org	rotaryeng.com.sg
Landscape Hawaii	accu-search.com	wow pictures
Tiscali SPA ⚠ Target errato	spacebridge.com	infraestructures.cat
ONGC Petro Additions Limited	New Jersey Association on Correction	rmzoilfield.com
Four Quarters	Coreix	palawancoop hospital
Dynamic Netsoft	Agura B.C LTD Hacked	Petroquim Chile
NK Customer Solutions	Mor-logistics	education.gouv.fr
Welthungerhilfe	Weizmann Institute of Science Hacked	S5 Agency World
www.ultrarapit.net	West Texas Oral and Facial Surgery	SHUKAKU-INC
www.humac.dk	Huesman Schmid Insurance Agency	Homestead Gardens
www.prival.com	Pressure Dynamics International	electro-seal.com
www.skcounsel.com	Trackside Services	Community Choice Credit Union
www.continental.aero	Clayton Construction	Bumfords
www.sanmarti.es	Strait Steel	Hartwig Mechanical Inc
www.anubis-cosmetics.com	membersourcecu.org	San Jose Country Club
www.floralimited.com	Alaffia	girv
Tech Mahindra	TSE Industries & WHK Biosystems	dugoni
elpasoglass.com	TN CPA	ecoter

greatcdltraining.com	Evans Pharmacy	NyN
broadleafgame.com	coBuilder	Al Tadawi Specialty Hospital
buffalomarine.com	Technology Consultants Group	EUC Sjlland
norsk.global	macedonia.oh.us	mytaac.com
artexmanagement.com	Bridgehead	mercercapital.com
Carter Manufacturing	Ess Brothers & Sons	triangleheatingcooling.com
Emtech Inc	Metropolis Country Club	https://www.personalservice.com.br/
View Zuellig Industrial	Equip'LaboFROID	Deakin Medical
Islington Golf Club	Durant City	ad-engineering.co.uk
Sunrise Springs Spa Resort	HYBRO Saatzucht GmbH& Co KG	Ascot Vale Health Group
CGP&H	Academic Urology & Urogynecology of Arizona	Hudson River Housing
Cartel Communication Systems	Lamina Dielectrics, United Kingdom	AntFarm
Associated Packaging	Sandhill View County School_UK	waiwhetu-medical-centre
SiloKing	gibGREINER	In'Tech Industries
Dickow Cyzak Tile	VERTEL	Ticketmaster
Morningsideservices	Tufton Capital Management	rinaldi.com.br
Woodtect	NF Stroth & Associates	Ingonyama Trust Board
PILOTTHOMAS.COM	Jasper Products	The Green Flame Gas Co.
Pensions.gov.lk	accountant falavinha.local	QuadMiners
The Kingdom of Tonga's Ministry of Health	Agaris	ACCS Le Groupe
Dealmed Medical Supplies	Cutcliffe Archetto &Santilli	TC Wilson
hubermanlaw.co.il	Ab Ovo	Optima Tax Relief
Tappoo Group of Companies	Clark Mechanical	Synopsys
melilla.es	CNPC USA	Homeyer Consulting Services, Inc
Martin Showers Smith& McDonald	Strafford County NH	Farmacisti Più Rinaldi S.p.A.
Imblum Law Offices	Freedman HealthCare	Nunez Dental
Johnstone Supply Dallas-Fort Worth	spg.net	Productionsaw.com
Antigo Construction	moserengineering.com	quenotedeporten
Merlin Industries	SecurU	lgipr
mcparlane.com	Rollex	Best Profil
MultiStone	Brett-Robinson	MTTEXPERTISES.COM
Studio Verna Società Professionale	bulentklise.com.tr	Kittery Police Department
Arbour Volkswagen	Project Partners	golf-schoenenberg.ch
Airedale Springs	Sacred Heart School	frylite.com
Ubon Ratchathani University	S&H Express	regen.com
Pay Tel Communications	NPD Products	regentscapital.com
QHR Ltd	codesco.com	cityofbelvedere.org
Habitat for Humanity of Greater Sioux Falls, Inc.	packagesteel.com	microman.com
Quaser Machine Tools, Inc	hohmannoilandplumbing.com	healthtrust.org

AEROBLOX	cs-groupllc.com	brucknertruck.com
JobPlace Ltd Hacked	pzsarchitects.com	britteninc.com
Wilsonville Toyota-Scion	welcometosedgebrook.com	accuvein.com
Positive Solutions	moffett-towers-club.com	appotech
Medical Center of Marin	liberty-township.com	Triumph Construction
Tecore	mcsl.de	Ebac
gudeco.de	rusindustries.com	Veethree
Cutcliffe Archetto & Santilli	theoverheaddoorco.com	LS Proline
Informatika A.D.	awo-giessen.org	Barnhartcrane.com
Pennant Park	realschule-karlstadt.org	Western Insurance Marketing Corporation
T.O. Brasil	bristolhose.com	HBI Canada
Fund for Reformed Companies (FONPER)	Repremundo.com.co	GRECA Asfaltos
CMI	Y.G. New Idan	Columbia TI
GMORS Co., Ltd	Aerodreams Hacked	Sturdevant's Auto Parts
Olivera Canarias	NewGen	Tien Tuan Pharmaceutical Machinery Co. Ltd
tdunhamcpa.com	StudentKare	Ryan Harvie McEnery
sbh	Central Point School District 6	AMS Paving
motorsport-de-la-capitale	faycom	RECYCLA
lurie-glass	Ajmanre.gov.ae	iscamen
www.covenanthealth.net	Eagle Builders	FORTÉ
VS Associates	isdl.org	American Hospital Dubai
Datrose	sgapl.com.au	Lts.com.vn
Integrity Mortgage	cypress	Groupe Devimco
Keystone Shipping	ramlaw.com	V² Development
hawaiiunified.com	Bowles Womack & Company, P.C	all-nations-health-center
The Lowell Hotel New York	Món Sant Benet	YIEH UNITED STEEL CORP
Inflite Engineering Services	Biogest	IoTechWorld
Access Financial	Frazier & Bowles	EPC Group
Seppeler Gruppe	550madison.com	Davies, Mcfarland & Carroll
Myrtue Medical Center Hospital	talismancivil.com	DALB
Lexington & Richland County School District Five	Sweeney	Kel Campbell
gouverneur.com	lakebook.com	Zeus Tecnología
Arlington Occupational Health and Wellness	upstartpower.com	J-Kraft
PeopleCheck	dcinvestors.com	cemeteries.local
Katz & Doorakian Law Firm, P.L.	biokplus.com	university of chile
Avantic Medical Lab	haydist.com	Funktel GmbH
Fishman, Larsen & Callister	wilsonappliance.com	Solar City Tyre Service
caldine	garmonandcompany.com	Kettering Health
hy-vee.com	skirball.org	Epworth-Hospital
mccn.org	Lake Region Healthcare	www.motorworldarc.co.uk
Scherzinger	Dyrham Park	FLOE International

Estes Forwarding Worldwide	Patron Insurance Services	Myer Auto
mlderm.com	nucamprv.com	ochsinc.org.com
Agganis Driving School	titantrailers.com	digitalwarroom.com
Hilliard Enterprises	McCracken Financial Solutions	Sorter Construction
Brown & Winters	alleray-labrouste	yahtec
Brown & Brown PC	lawyersmutual.com	Rochon
Israel Job Info Ltd Hacked	apollomd.com	VANTAGE
Ovalstrapping	Cryoviva	basakkent
Telcom Insurance Group	www.waveny.org	sky
Fisher59	Christian Brothers Academy	North American Lighting
Dairy Farmers of America	Lawton Partners	Dynamic Engineering
etoscapitalasia.com	www.kerrvilleisd.net	Observer Media Group
Ben Horin & Alexandrovitz Ltd	Asefa Insuarance	Sleepy Hollow Country Club
fecovita.com	bioalleva	Sandhills Medical Foundation
rhodar.co.uk	fasse.com	Navesink Rehab
Wisconsin Judicare	Chain IQ	Solar City
rioglass-solar	A&R Engineering	Lumenation
Zacharia Levi Ltd Hacked	Center for Clinical Research	WC Smith
OAK PARK & RIVER FOREST HIGH SCHOOL	Eastern Platinum Limited	FLOE Internationa
Collision & Classics	Rosewood Farm	Capital Trade
ALFA Testing Equipment	Morpeth Pharmacy	jerichofd.com
Levinzon CPA	Letry	Vinda Group
doradosoftware.com	Skyline Dubuque	Rechler Equity Partners
Disneyland Paris	Fenol Kimya	Family Health Specialists
Sivim IT	Capitol Taxes	Naper Grove Vision Care
AXT	currimjee	Diyar
Kibbutz Almog Hacked	via-optronics	Riverdell Construction
cisin.com	iberol	DHL THAILAND
powells.biz	eira-group	Jardin De Ville
diffazur.fr	KMMP	Kansas City Aviation Center
Comelesa	nipponindiaim	venezolanadepinturas.com
SUSTA-STAMPI	unilever	Pistolero
januschke.at	Ersar	valuestoreit
Vacation Myrtle Beach	NCVOO	Wilkie Sanderson
taoscounty.org	BTHK	Hospital Jos é Agurto Tello de Chosica
Place Homes	lactanet	Universidad T é cnica del Norte Ecuador
siamgas and petrochemicals public company ltd	ssi-mi	PPM Industries SpA
glwholesale.com	dad	Dcsdev.org
Highlands Oncology Group	astronika	daycohost.com
https://www.ilesfuneralhomes.com/	sras	nokotapackers.com
Haor Heavy Transport	icidesi	Bailey's
YHD Group	taos	Presort First Class

Saban Systems	carducci	RE/MAX
R&W Engineering	Arch-con	Town of North Providence Rhode Island corporate office
Sun Direct	Evasa	immobilia.hu
Morar Construtora e Incorporadora LTDA	AP Lettering	

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。

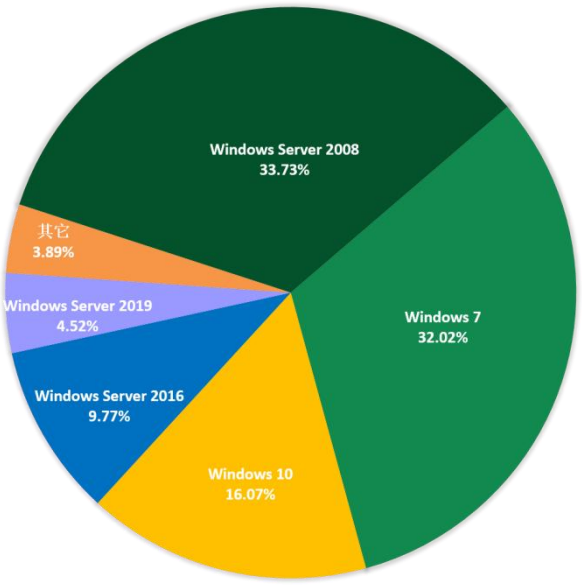

图 5 2025 年 6 月受攻击系统占比

对 2025 年 6 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相比，地区排名和占比变化均不大。数字经济发达地区仍是被攻击的主要对象。

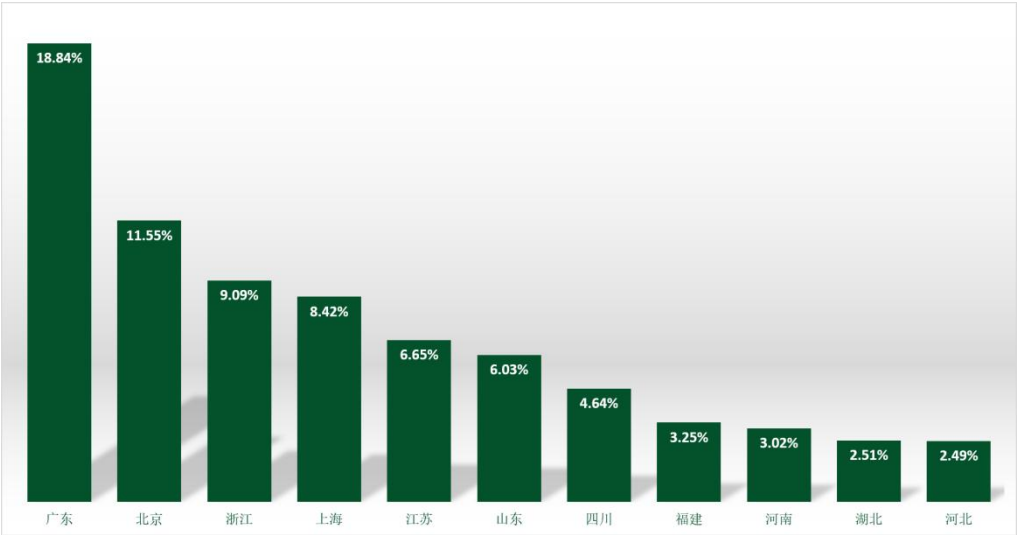

图 6. 2025 年 6 月国内受攻击地区占比排名

通过观察 2025 年 6 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。

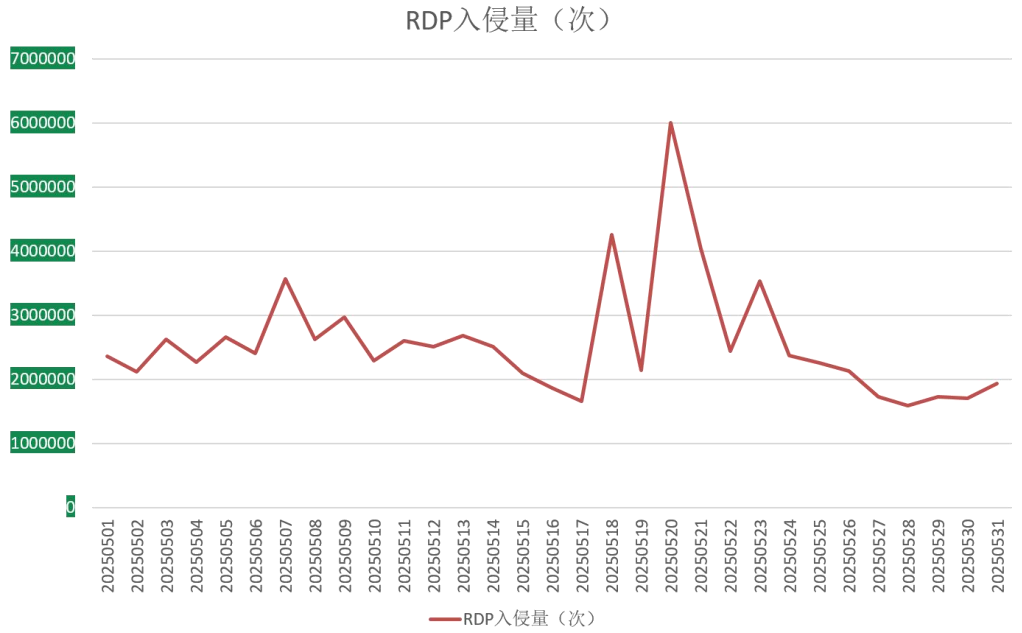

图 7. 2025 年 6 月监控到的 RDP 入侵量

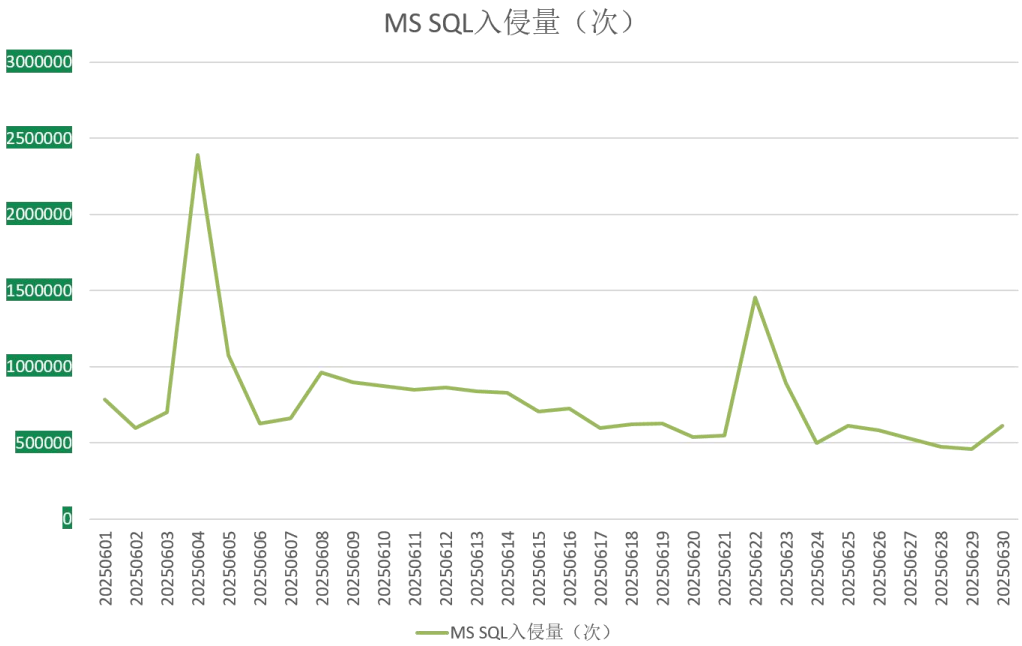

图 8. 2025 年 6 月监控到的 MS SQL 入侵量

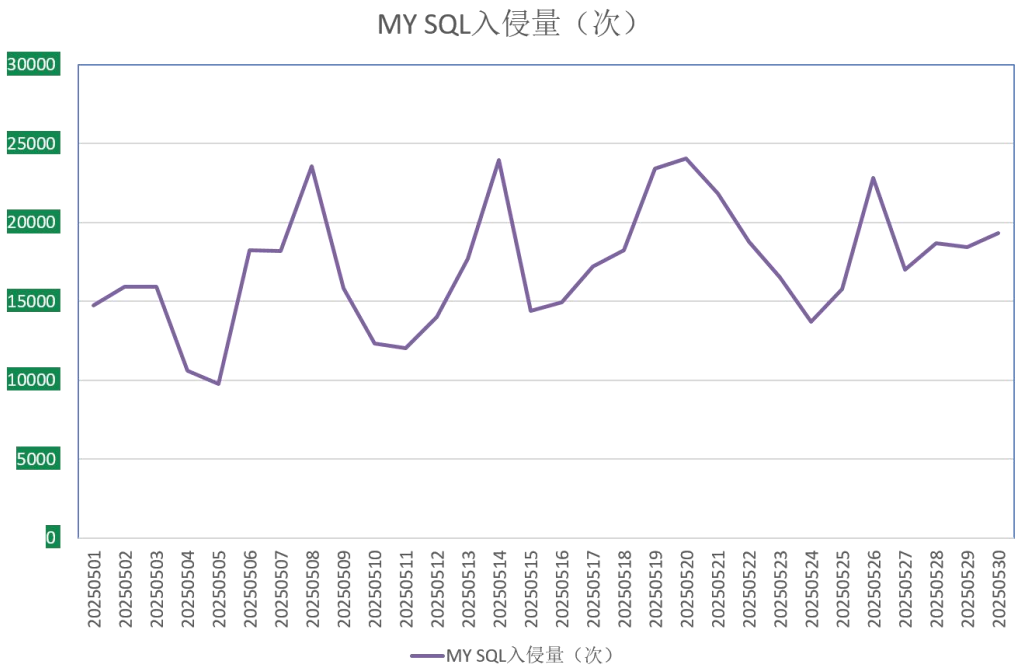

图 9. 2025 年 6 月监控到的 MYSQL 入侵量

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。

- wxx：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，以及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。
- 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：同 baxia。
- kalxat：属于 Kalxat 勒索软件家族，由于被加密文件后缀会被修改为 kalxat 而成为关键词。该家族主要的传播方式为：通过暴力破解或注入数据库成功后手动投毒。
- weaxor：同 wxx。
- 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，后增加利用漏洞的传播方式。此外,360 安全大脑监控到该家族曾通过匿影僵尸网络进行传播。
- mkp：属于 Makop 勒索软件家族，由于被加密文件后缀会被修改为 mkp 而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。
- peng：属于 phobos 家族，使用 Rust 语言进行编译的版本，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。

✧ backups：属于 LockBit 家族，以泄露的 LockBit 构建器代码创建。该家族的主要传播方式为：通过暴力破解远程桌面口令与数据库口令，成功后手动投毒。

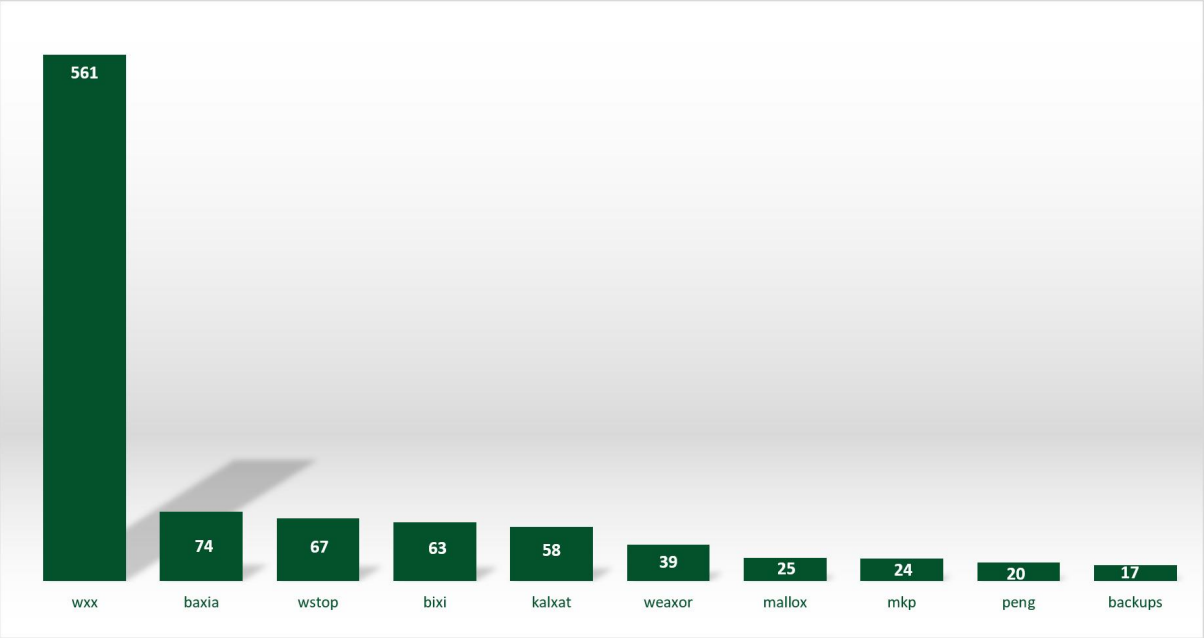

图 10 2025 年 6 月反病毒搜索引擎关键词搜索排名

解密大师

从解密大师本月解密数据看，解密量最大的是 FreeFix,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。

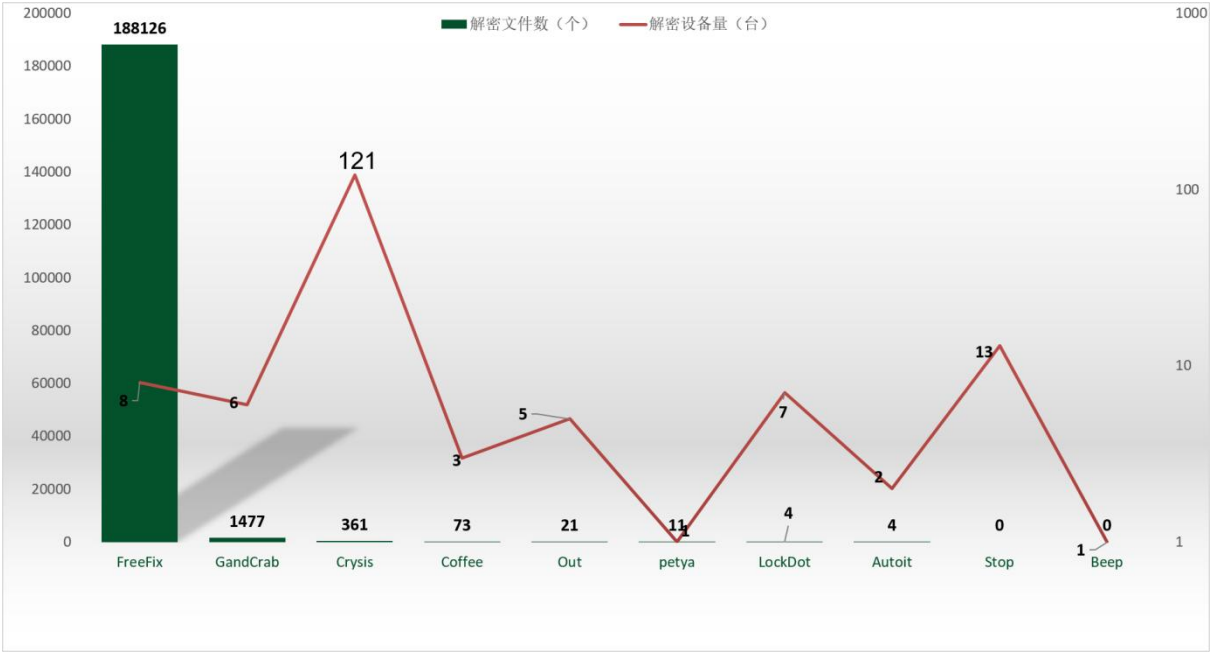

图 11. 2025 年 6 月解密大师解密文件数及设备数排名