

勒索软件流行态势分析

2025 年 4 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，勒索金额从数百万到上亿美元的勒索案件不断出现。勒索软件对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监测与防御，为需要帮助用户提供 360 反勒索服务。

2025 年 4 月，全球新增的双重勒索软件有 Devman、Gunra、Silent 等多个新增家族。传统勒索软件家族 Kann 再度活跃，360 成功破解。

近期，360 反病毒团队在监测过程中发现了一款勒索软件开始活跃，其变种名为“.kann”与“xmldata”。该勒索软件采用了较为复杂的混合加密策略，利用 RC4 与 AES 算法对受害者文件进行加密，并通过 RSA 算法对上述密钥再次进行加密，以此进一步提升了数据解密的难度。最后，勒索软件会将加密后的文件统一添加“.kann”扩展名。

而值得注意的是，虽然该勒索组织自认为在密钥管理上非常稳妥，但实际上存在一定设计缺陷。故此，研究人员通过对加密流程的逆向分析与算法优化，发现可以尝试利用当前 GPU 或高性能 CPU 的算力，对加密文件进行密钥暴力破解，从而在较短时间内实现文件解密。这一发现为受害者带来了一线希望，也为防御和应对类似勒索攻击提供了有价值的参考经验。受该勒索软件攻击的用户，也可以联系 360 反勒索服务进行解密。

以下是本月值得关注的部分热点：

- 1** Interlock 勒索软件团伙在 ClickFix 攻击中推送虚假 IT 工具
- 2** 西雅图港表示勒索软件泄露影响了 90000 人
- 3** 德克萨斯律师协会在 INC 勒索软件发布攻击声明后确认数据泄露

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，赎金范围在 8 千到 1.5 万元人民币之间。

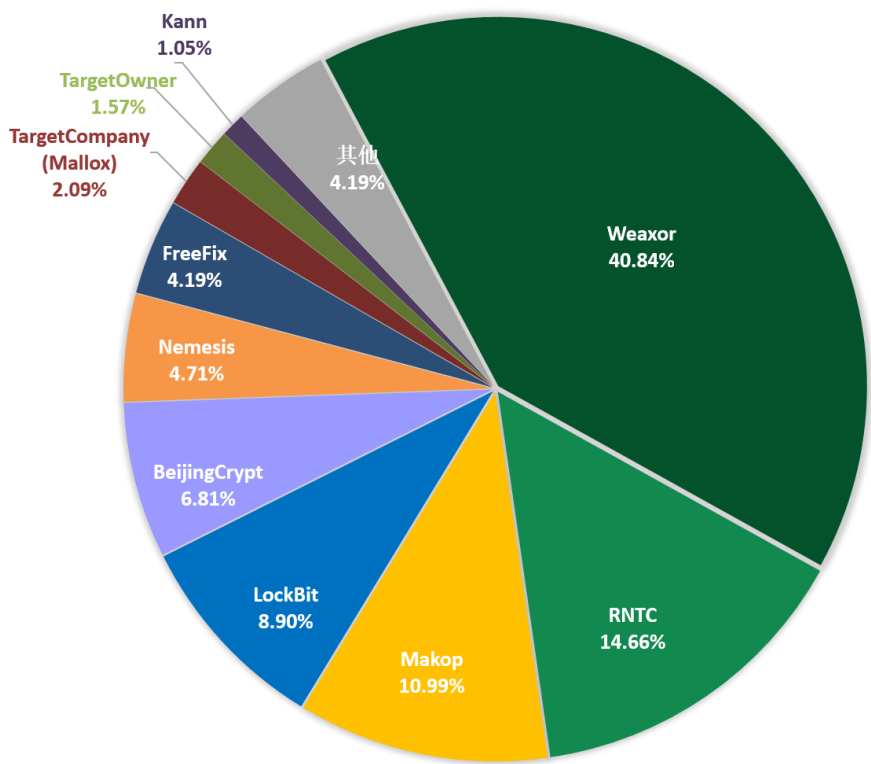


图 1. 2025 年 4 月勒索软件家族占比

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。

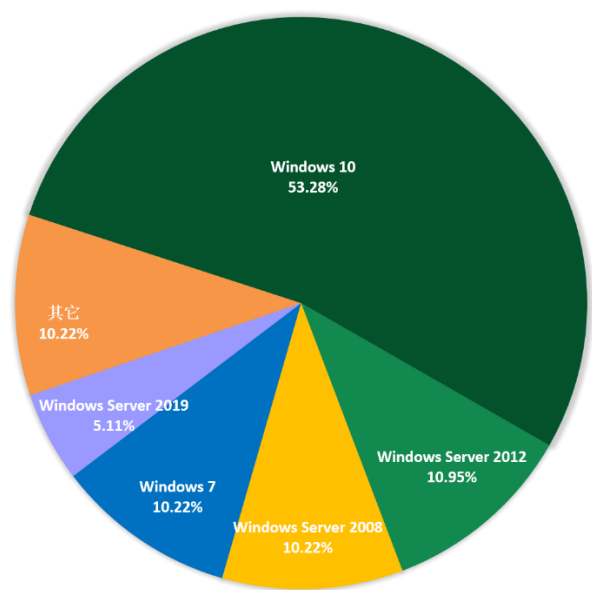


图 2. 2025 年 4 月勒索软件入侵操作系统占比

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 。

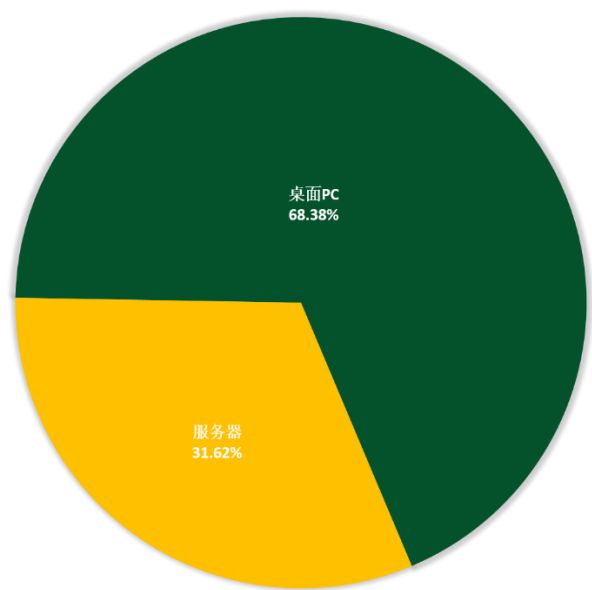


图 3. 2025 年 4 月勒索软件入侵操作系统类型占比

勒索软件热点事件

Interlock 勒索软件团伙在 ClickFix 攻击中推送虚假 IT 工具

Interlock 勒索软件团伙现在使用 ClickFix 攻击，此类攻击会依靠伪造的 IT 工具来破坏公司网络并在设备上部署文件加密恶意软件。ClickFix 是一种社会工程策略，受害者被诱骗在其系统上执行危险的 PowerShell 命令以修复错误或验证自己，从而导致安装恶意软件。虽然这不是 ClickFix 第一次与勒索软件感染相关联，但对 Interlock 的确认表明，利用该策略的这类威胁行为呈增加趋势。

过去，Interlock 利用虚假的浏览器和 VPN 客户端更新来安装恶意软件并破坏网络。据研究人员称，Interlock 勒索软件团伙于 2025 年 1 月开始使用 ClickFix 攻击。Interlock 至少使用四个 URL 来托管虚假的 CAPTCHA 提示，告诉访问者在他们的计算机上执行命令以验证自己并下载推广的工具。研究人员在四个不同的站点上检测到了恶意验证码，这些验证码模仿了 Microsoft 或 Advanced IP Scanner 门户：

- `microsoft-msteams[.]com/additional-check.html`
- `microstteams[.]com/additional-check.html`
- `ecologilives[.]com/additional-check.html`
- `advanceipscanner[.]com/additional-check.html`

不过，只有冒充 Advanced IP Scanner 的网站会引导下载恶意安装程序。

研究人员在分析恶意载荷时发现样本中具有 C2 域名以及各种有效载荷响应，包括 LummaStealer、BerserkStealer、键盘记录器和 Interlock RAT。后者是一种简单的木马，可以动态配置，支持文件泄露、shell 命令执行和运行恶意 DLL。

在最初的入侵和 RAT 部署完成后，Interlock 运营商使用被盗的凭据，通过 RDP 进行横向移动。此外，研究人员还发现了 PuTTY、AnyDesk 和 LogMeIn 均被用于发动相关攻击。

勒索软件执行前的最后一步是数据泄露，将被盗文件上传到攻击者控制的 Azure 存

储池中。

西雅图港表示勒索软件泄露影响了 90000 人

美国西雅图港于 2024 年 8 月 24 日披露了带有数据窃取的勒索攻击，称由此导致的 IT 中断影响了多项服务和系统，包括预订值机系统、乘客显示屏、西雅图港网站、flySEA 应用程序，并导致西雅图-塔科马国际机场的航班延误。在首次披露三周后，港口确认 Rhysida 勒索软件是本次攻击事件的幕后黑手。事件发生后，港口还决定不屈服于网络犯罪分子支付解密器费用的要求，即使他们威胁要在其暗网泄露网站上发布被盗数据。

2025 年 4 月 3 日，该港口宣布它现在将向受由此产生的数据泄露影响且拥有邮寄地址的个人发送大约 90000 封通知信。据该机构称，受此次数据泄露影响的人中约有 71000 人来自华盛顿州。泄露的通知信显示，攻击者以各种手段窃取了员工、承包商和停车数据，包括姓名、出生日期、社会安全号码、驾驶执照或其他政府身份证号码以及一些医疗信息。

此外，该港口还表示它存储的机场或海上乘客信息“非常少”，其支付处理系统没有受到攻击的影响。

德克萨斯律师协会在 INC 勒索软件发布攻击声明后确认数据泄露

美国德克萨斯州律师协会警告说，在 INC 勒索软件团伙声称已入侵该组织并开始泄露被盗数据样本后，他们确认了数据泄露的事实。在发送给受影响成员的通知信中，该协会表示它是在 2025 年 1 月 28 日至 2 月 9 日期间遭受了漏洞攻击，但本次攻击直到 2 月 12 日才被发现。攻击者从其网络中窃取的信息包括其成员的全名和其他数据，这些数据已提交给了当地的总检察长办公室的公共数据泄露处理部门。

该通知没有提供有关此次泄露的黑客组织的更多信息，但 INC 勒索软件团伙于 2025

年 3 月 9 日将该组织添加到其暗网勒索页面，声称对德克萨斯州律师协会发起了攻击。攻击者已经泄露了据称被盗的文件样本，包括法律案件文件。目前无法验证 INC 所泄露的数据是否来自该组织的网络，以及它们是私人信息还是公开信息。到目前为止，德克萨斯州律师协会也未做出相关的回应和声明。

但协会发出的数据泄露警告通知中，告知受害者可通过 Experian 获得免费的信用和身份盗窃监控服务。此外，建议他们考虑激活信用冻结或在其信用档案上放置欺诈警报，以减轻因数据泄露而产生的风险。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

decryptsystem@onionmail.org	ambulance@cock.li	recoverhelp2020@thesecure.biz
odblokujmujsystem@proton.me	ambulance@onionmail.org	payforrepair@tuta.io
Prestige.ranusomeware@Proton.me	sc0rpio@mailfence.com	payforrepair@mailum.com
dharkonsk@gmail.com	scorpi0@mailfence.com	support1@contonta.com
night.spire.team@gmail.com	JefferyData@dnmx.su	support2@cavopo.com
night.spire.team@onionmail.org	Devicdata@mailum.com	backtonormal@foxmail.com
night.spire.team@proton.me	Devicdata@onionmail.org	RestoreMyData@protonmail.com
BlackSpyro@tutanota.com	ineszafimi@web.de	7n9045b54789h@firemail.cc
ransombiz@tutamail.com	katrinnonaxo@web.de	babylon4367@proton.me
Maximsru@tutamail.com	antjepamuta@web.de	decryptmepleas@onionmail.org
nullhexxx@gmail.com	darkmystic@onionmail.com	gnsyihong@mailum.com
carnelyy@tutamail.com	darkmystic@tutamail.com	ferguson@mailum.com
carnelyy@cyberfear.com	realunlocker@india.com	ferguson@firemail.de
MassAttack@cock.lu	realunlocker@cock.li	kawsexpress@yahoo.com
CactusProInfo@cock.li	bannedlands@msgsafe.io	tanzaniya@onionmail.com
xmrdata@tutanota.com	xtralords@dnmx.org	carnelyy@tuta.io
xiaoba_666@163.com	ferrari@msgsafe.io	babuckransom@tutanota.com
Dizaster.cool@list.ru	helpdecrypt01@gmail.com	tormented.soul@tuta.io
decsupp24@tuta.io	elons1890@Cyberfear.com	absolutezero666@protonmail.com
decsupp247@outlook.com	helprecover@foxmail.com	jpermar12@protonmail.com

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）。

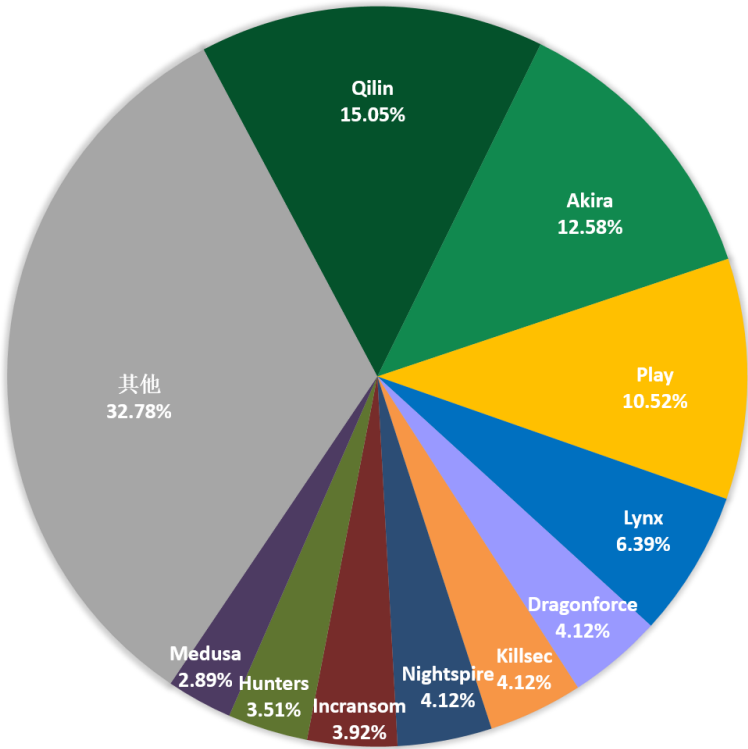


图 4. 2025 年 4 月通过数据泄露获利的勒索软件家族占比

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 485 个组织/企业遭遇勒索攻击，其中包含中国 9 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 5 个组织/企业未被标明，因此不在以下表格中。

SIMCO Electronics	Toppan Next	Bangkok Electronics Co., Ltd
Telco Intercontinental	Global Media Group	Simms Sigal Linwood Inc.
Matrix New World Engineering	Hayward Quartz Technology	Hotell Euroopa
FCC	Isthealthinc.com	Dinaksa Pesaje
Watkins Steel	Wilmington Personal Injury Lawyer - DPLAW	Sasszemklinika

Digestive Specialists	Compliance Consulting Group	MHT Partners
Southwood Financial, SWF FUNDING LLC, EduCap Inc.	Mid-America POOL RENOVATION, Inc	Consonic
mossyoak.com	Sally B Gold	ccso2014.local(sheriffs)
dlcid.com	accessmt.com	Yozgat City Hospital
bostonconveyorandautomation.com	HOPi	physiciansmedicalbilling.net
nuovadfl.it	Enflame Technology	gramoll.com
rfsdl3.org	universalwindow.com	farmerbros.com
Gorham Sand & Gravel	bertie.k12.nc.us	Taxplan
Cooper Global Chauffeured	yankeetrails.com	Mochtar Karuwin Komar: Indonesian law firm - MKK
Ushio	TRALFO Srl Trasporti e Spedizioni	technoforte software pvt ltd
BOLL Logistik	Schultz Industries Inc.	International Busines Service
Coop UQAM	Manchester Credit Union	Iris Neofinanciera
National Steel City	Ju Percussion Group	RFMS, Inc.
PermaCold Engineering	Kaye Lifestyle Homes	Pulse Urgent Care
Missouri Pipe Fittings	VIÑUELAS ABOGADOS	Bridgebank Limited
southernagllc.com	EVERTECH INSTRUMENTAL CO., LTD	National Association for Stock Car Auto Racing
SoloVue	aqhch.com.cn	Coulter & Tateoka
SJERP	itec-gmbh.com	https://www.thirdave.com
Hpital Glengarry Memorial Hospital (clglen.local)	heinrich-steinhardt.de	www.gchd.org
David Mills CPA, LLC	hurst-schroeder.de	averasia
w8textil	helixtools.co.uk	crystal-d.com
csspv	heilbronn.de	Gruppo C.R.S.p.a
Melco Capital Pte. Ltd.	getriebetech.de	FKS Group
Kramer Green Zuckerman Greene and Buchsbaum	kirkel.de	Bauer-Walser AG
Tolerance Masters	extremefire.com.au	The Fullerton Hotelsand Resorts
LaBella Associates	foerster-schwanau.de	Coop57
CCHC Healthcare	eichele-bau.de	Thiekon Constructie
nccer.org	frapack.de	shengyusteel.com
Dermatologists of Birmingham	Koninklijke Ahold Delhaize N.V.	Andretti Indoor Karting & Games
www.latouchechildrens.com	www.nelson.edu	CVTE
govcz	jackpotjunction.com	American Air Conditioning & Heating
MALAYSIA AIRPORTS HOLDINGS BERHAD	Feldman & Lopez	Dhoot Transmission
Bioprofarma Bagó S.A	Hyalogic	Cambridge Fluid Systems
Whitley Law Firm	niemann.de	The Komec
Minnesota Lawyers Mutual Insurance	Bio-Clima Service	Spring Creek Golf & Country Club
RC Manubhai	Red Chamber	JKC Australia LNG
Haas & Associates	d-line-it.com	Galesburg Area Chamber of Commerce
FMT Consultants	ende.bo	TIME Group

Mantel Machine Products	aeamg.org.br	St Edmund's College
Crawford Door Sales	Lamberti Group	Hewsco.com
Scientel Solutions	Seneca Gaming & Entertainment	Wertex Group
www.southlandscs.com	Dale Partners Architects	Metal Sales Manufacturing Corporation
liftsolutionsinc.net	Anfarm Hellas	sunbayhotel.com
Penderels Trust	D'Granel	Dalincoln
Matthews Law	McElwee Firm	Flo Components
Phelps United	govonisabbiatrici	ASOLO DOLCE SAS
Conditioned Air Corporation	semex.com	Telecontrol
Appalachian Regional Commission	KraftKisarna	Baucenter.it
Linney	Pryor Morrow	SMYK
KLINGER Italy	Pratt Homes	[DISCLOSED]Cell C
DIALOG company	Setpoint Systems	Phil Smith Automotive Group
Sisnet, Costa Rica	iblinfo.de	Dermatology Solutions
MDB	a-lfreeman	National Electronic Transit (N.E.T)
Stadtwerke Schwerte GmbH	Astra Products	Altara
shgcpa.com	Lake HVAC	IACC Holdings
corporateflight.com	www.clubcar.com	Texla Energy Management
Kenworth Del Sur	nevadareadymix.com	asiapacificex.com
DYNAMIS Insurance	toolsign.com	Dubai Company
M'AR De AR Hotels	spscompanies.com	Texas Construction Firm
Kasb Bank - K-Trade	ARRCO LSM	Optimax Technology
J. SCHNEEBERGER Maschinen AG	iescomm.com	doumen.fr
Penn Emblem (penn.local)	Heierli	Hofmann Fördertechnik GmbH
Santa Cruz Properties	Bolivar Insulation	IDS Infotech
Cohn Lifland Pearlman Herrmann and Knopf	King Industries Inc.	grupotersa.com.mx
DaVita	PEÑA BRIONES MCDANIEL & CO.	graphiquedefrance.com
Madison School District Schools	Inductors Inc.	Groupe Delcourt
EU victim	NewHotel cloud company	Swiss Capitals Group
Advanced Simulation Technology inc. (ASTi)	trocaire.edu	National Ticket Company
impactcanada.com	Oregon Department of Environmental Quality	Bosshard-Farben AG
buildingmaterialspecialties.com	Destination Toronto	caschile.cl
friscochamber.com	Pawnee Heights Unified School District	Eagle Distilleries
greatplainstransport.com	Cortez Resources	Csm Engineering
pay4freight.com	NL Olson & Associates	Optimax Technology
Pacific Metallurgical	CDI	Baltimore Steel Erectors
The Fortune Society	Waller	Hawk Technology
end2endtechnologies	Miller Boskus Lack Architects	ABITL Finishing

Dress To	Merri-Makers	TEDOM
Oversea Casing	O'Brien & Ryan	HighWire Press
Fogelman Management Group	Voigt-Abernathy Company	Asseco
Vicarage Court Solicitors	James & Sons Fine Jewelers	Racami
Fleet Canada	Comport Technology Solutions	LeoVegas AB
arkansasprimarycare.com	Al-Hejailan Group	Nexia Poyiadjis IT
HELUKABEL company	Caputo	Apex Logistics International
MFR CULTIVONS LES REUSSITES, France	Orthopaedic Specialists of Connecticut	FUJIFILM
Farmo Res	Agricola Da Quinta De Corona	Blackmon Mooring
The Derby High School	Calmont Group	Industrial Corona de México
rawafid company	STUMPF MÜLLER Biberach	Latronica Law Firm, P.C
tecnologias.mspz2.gob.ec	Oklahoma Steel & Wire	Massachusetts Municipal Wholesale Electric
Rayle Electric Membership Corporation	MENTAL HEALTH	Royal Glass
coloradopulmonary.com	REFFINDO-PT Pupk Indonesia	Fraser Trebilcock
Two Kings Casino Resort	FEELFOUR	Drive Products
Milicic	Med institute	Doman
RRS Foodservice	Tawasol	amourgis.com
Varela Hermanos	CALTON.COM	DELOPT
Dar Al Teb	InterLOGIC Inc	Source Photonics
Shinko Shoji	Secretaria de Educacion de Veracruz, SEV	AWM Alliance Real Estate Group Ltd.
ESP Associates	Nicera	RORZE Technology Inc.
Versa Networks	Emotrans Chile	Sansone Group
lemi-group	Zaphira Uniformes	yuagam
www.unitedcaps.com	Audit Accounting Advisory Taxes	Parker Fabrication, Inc
N8XT	intelliloan.com	Henna Chevrolet
Mafi	Condista	National Sign corp
Jet Ice	Precision Textiles	raymurray.com
Springer & Steinberg	Miller & Caggiano	dgr.at
Independent Financial Services	Service Trade SpA	yumaspazio.com
M-POWER Information, Taiwan	Harris Steel	The ToolShed
promenade-village-dental, Canada	Ossman Consultants Limited	Woodmen Valley Chapel
Diedrich Coffee	McFarland Commercial Insurance Services	Cherokee County School District
NESCTC	Fall River Public Schools	Gem-Dandy Accessories
The Human Bean	FEELFOUR	Fuller Metric Parts
Lantronix	Chickenshed	Fulfillment Plus
Suburban Carting	visionproducts.llc	Doumen
All Book Covers	acimfunds.com	Krypton Solutions

Asesor í a Bieito	MS SUPPLY CHAIN SOLUTIONS (MALAYSIA) SDN. BHD	FS Tool Corporation
Natilait	Mapaex	Alton Steel
Amazon Transportes	CMC Corperation	Hop Industries
amethystgroup.co.uk	Dimension Composite	Lifebreath
franklin nursing home	bilbie.com.au	Parvin-Clauss Sign Company
Bacton Transport Services	Bjørklund	OTA Management
R&N Manufacturing	C?l????t Group	Regionale Verkehrsbetriebe
parrishleasing.com	mbmdubai.com	Socarpor
Acos Favorit	Restaurant Associates	Naza TTDI Sdn Bhd
agromate company	Colmar Industrial Supplies	Mikado Publicis
C-Mec	Batesville Products, Inc.	Entech Sales & Service, LLC
Richmond CPA	Codinter	Prima Power
Dominion Lending Centres	Imagineering Finishing Technologies	Clarity Ventures
MASHBURN CONSTRUCTION	On IT	crownlaboratories.com
The law firm of Rochelle McCullough, L.L.P	Cane Creek Cycling Components	caliendarchitects.com
Bindi SpA	Sfrent.net	Br ü gger Architekten AG
TrussWorks International	The Study	Royal Saudi Air Force
Sinalisa Segurança Vi á ria Ltda	PAC Strapping Products	Collective Architecture
Pharma Force	New York Sports Club	IMA Global
tuttoperlufficio.eu	Noyen Construction	US BioTek Laboratories
The Michelson Organization	KER Custom Molders	DG2 Design
Accueil - Site Offciel de la commune d'Ardon	Bonick Landscaping	STORT
Premier Meats South Africa	hasbco	The Loretto Hospital
Singapour Victim	TMA Group of Companies	Bamar Plastics, Inc.
Honk Kong Victim	ModulusGroup,Ludi-SFM	Mercury Integrated Manufacturing
China Harbour Engeneiring Company	inspec-international.com	Alora Pharmaceuticals, LLC
FAKO-M Getränke	Algas Engineering Pte Ltd - Algas Engineering	747 Studios
MRC de Maskinong é - district	SeproTec Multilingual Solutions	BenefitElect
ChangShen Hospital, Taiwan	Harvest	Ocuco
bettininformatica - suporteon company	sk.com	Workers Inform á tica Ltda
dhsmithco.com	3P Corporation	Testima Engineering
The Tech Interactive	Potomac Financial Services	Brella
Independent Title Agency, LLC ("ITA") (USA)	finetech.de	Fancy Films
Agencia Browne y Espinoza	chesterfieldtpw.org	Lendco
Heinz Hammer Vertragswerkstatt (Mercedes-Benz car dealer)	silocaf.com	Nydegger + Finger AG

Lithium Americas Nevada	Dumont Telephone	intellioan.com
Iris ID	Správa služeb hlavního města Prahy	jackpotjunction.com
City of Grove	SPEEDFAM	Dorel Home
www.monaghan.eu	Blink Photo	Hexicor
farma	North Platte Natural Resources District	AAPG
Hubbard, McIlwain, & Brakefield, P.C.	Galvatech	Hanna Global Solutions
Tänzer GmbH	Helitek Company Ltd.	Flagship Press Flagship Press

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。

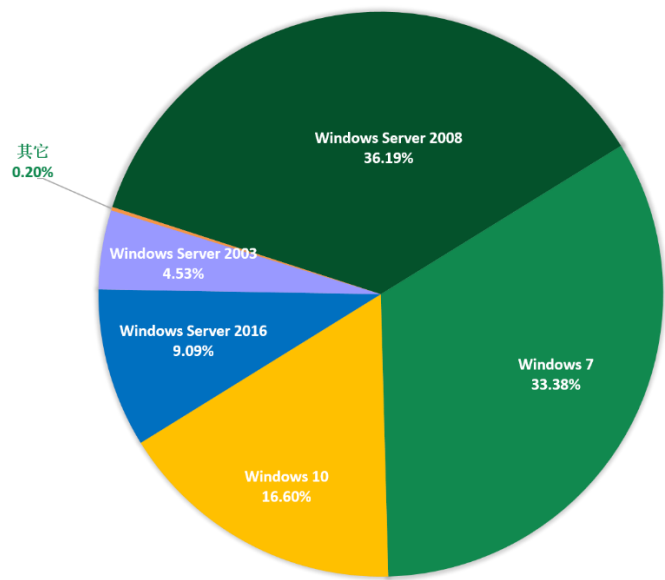


图 5 2025 年 4 月受攻击系统占比

对 2025 年 4 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被攻击的主要对象。

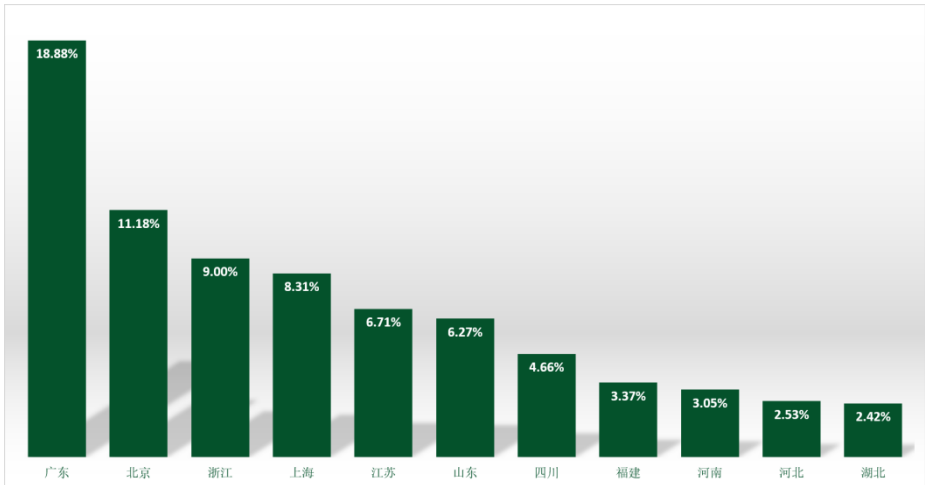


图 6. 2025 年 4 月国内受攻击地区占比排名

通过观察 2025 年 4 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。

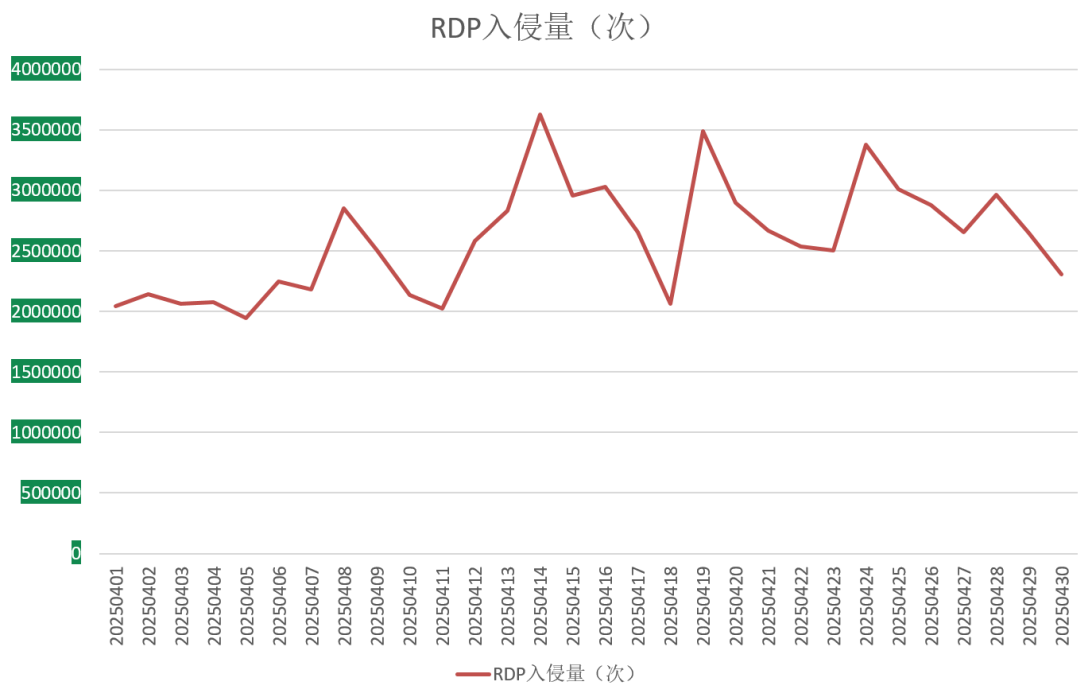


图 7. 2025 年 4 月监控到的 RDP 入侵量

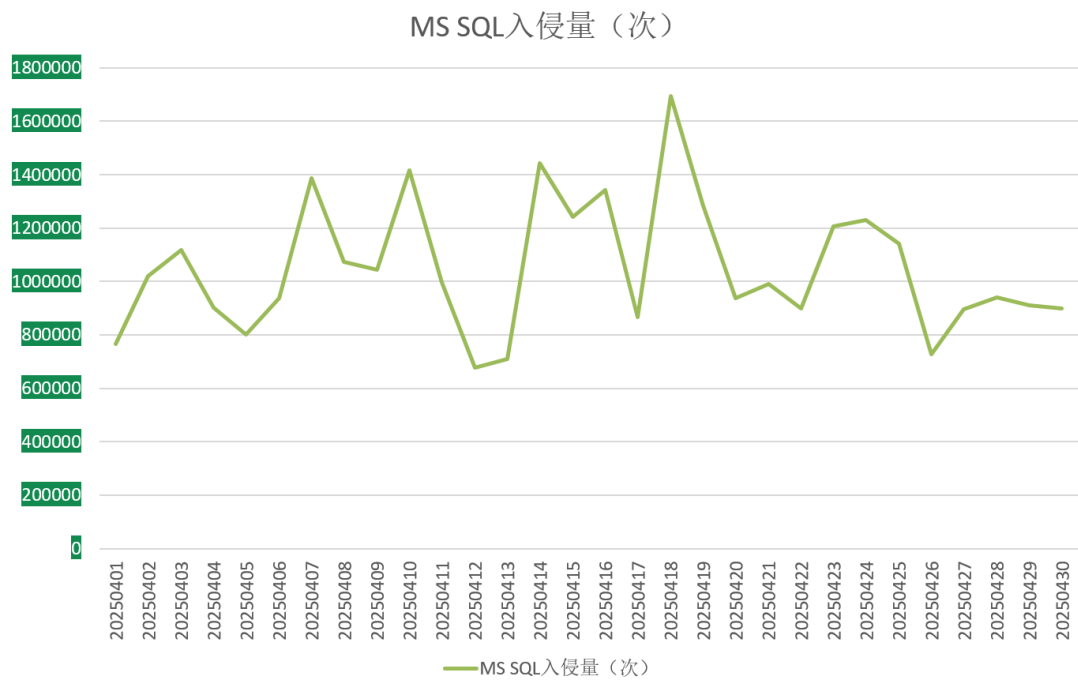


图 8. 2025 年 4 月监控到的 MS SQL 入侵量

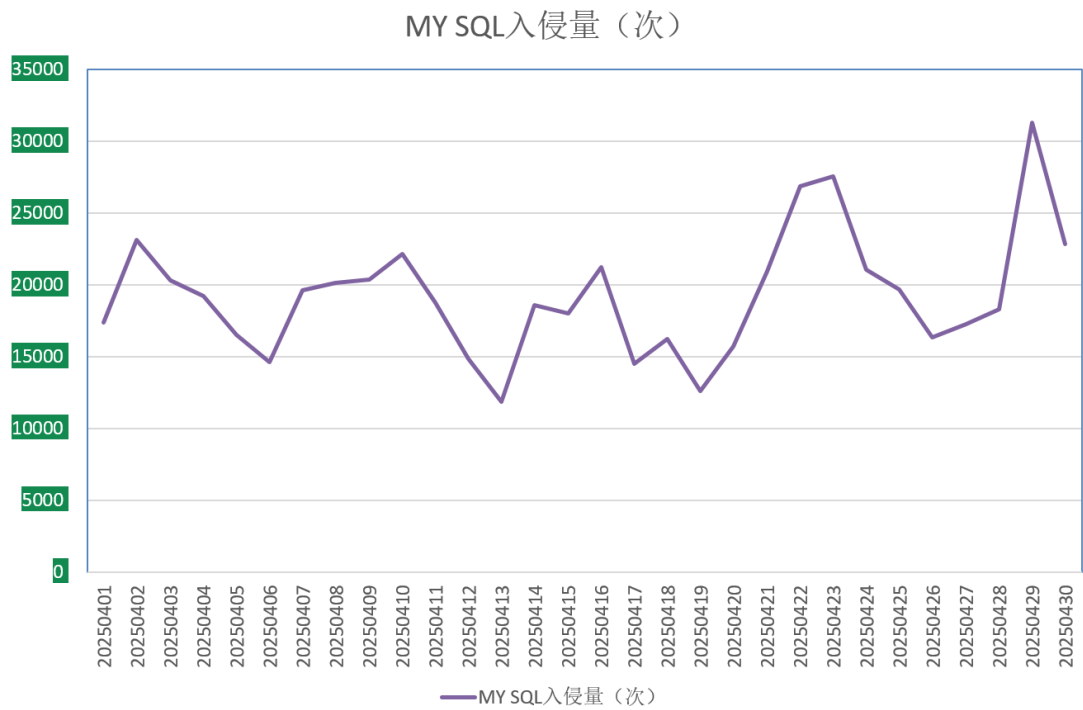


图 9. 2025 年 4 月监控到的 MY SQL 入侵量

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。
- ✧ **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。
- ✧ **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。
- ✧ **bixi**: 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。
- ✧ **baxia**: 同 bixi。
- ✧ **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，后来增加了利用漏洞的传播方式。此外，360 安全大脑监控到该家族样本曾通过匿影僵尸网络进行传播。
- ✧ **weax**: 同 wxx。
- ✧ **wxr**: 同 wxx。
- ✧ **sstop**: 同 wstop。

✧ 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。

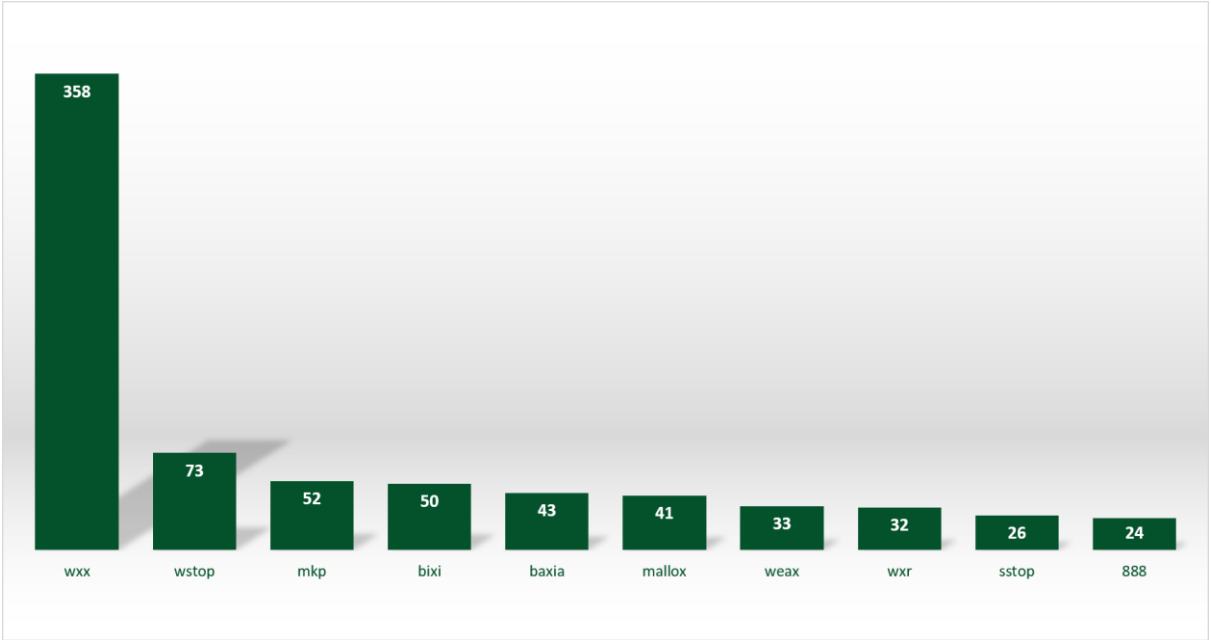


图 10 2025 年 4 月反病毒搜索引擎关键词搜索排名

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 Loki。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。

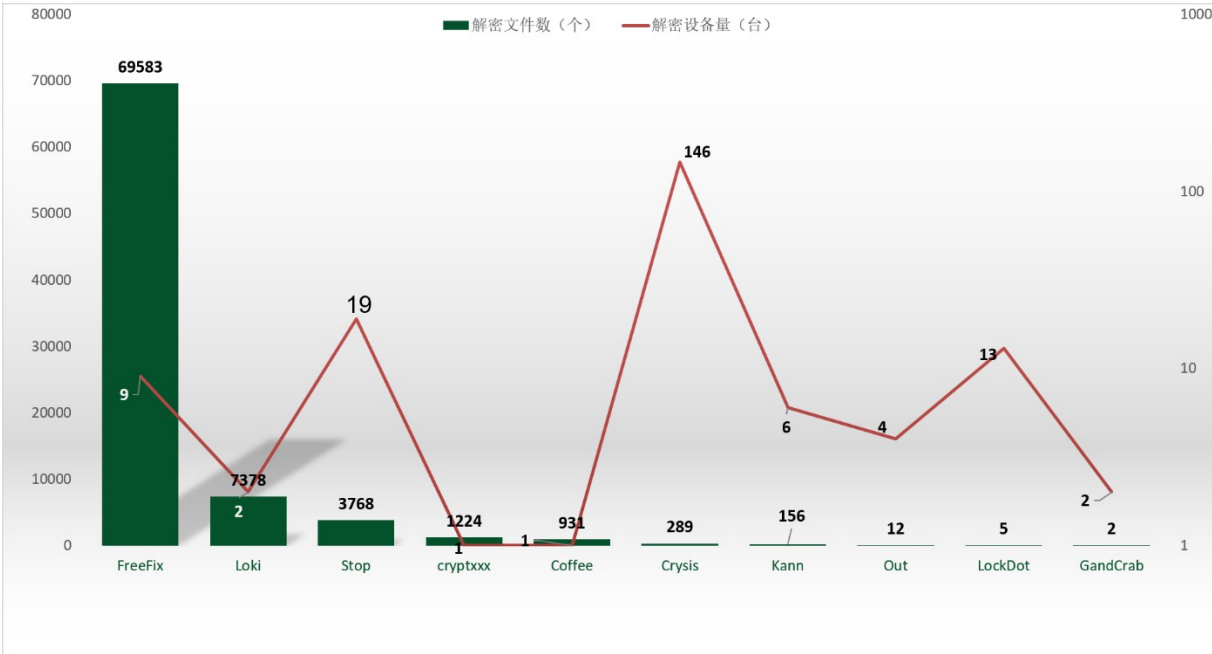


图 11. 2025 年 4 月解密大师解密文件数及设备数排名