2026 年 3 月

勒索软件

流行态势报告

三六零数字安全科技集团 | 安全能力中心反病毒部

勒索软件传播至今，360 反勒索服务已累计接收到数万例勒索软件感染求助。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。

2026 年 3 月，全球新增的双重勒索软件有 Insomnia、Exitium、Killada 家族，传统勒索软件家族新增 RedStar、SurfLocker、Uragan、PCLocker、IsoLens 等多个家族。

本月国内热门的勒索家族 Weaxor，新增了多个尚未分配编号的 Web 漏洞利用，并同步新增了多个 BYOVD 驱动利用，360 安全大模型已第一时间捕获并支持拦截。

以下是本月值得关注的部分热点：

① Sorry 后缀勒索软件利用 Web 漏洞大肆传播

② 医药巨头史赛克因与伊朗相关的擦除软件攻击而被迫离线

③ 勒索软件攻击扰乱西班牙主要渔港运营

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。

安全软件占比分析

360 提供反勒索服务已经超过十年，长期致力于全网勒索病毒攻击的响应、分析、处置、攻防、预警、解密工作。自 2026 年 1 月起，新增安全软件占比统计，主要用于评估当前复杂网络攻防态势下愈发严重的基线安全问题，为勒索相关的攻击事件提供接近真实维度的数据。

本月的勒索反馈中未安装安全软件的占比达到 62.50%，而未正常启用 360 安全软件的设备数量则占比 20.83%，安装了其他安全软件的设备则占比 16.67%。在溯源分析中发现，所有安装了 360 安全软件的反馈设备均未开启相关防护，尚未发现绕过 360 多维防御体系的勒索攻击。

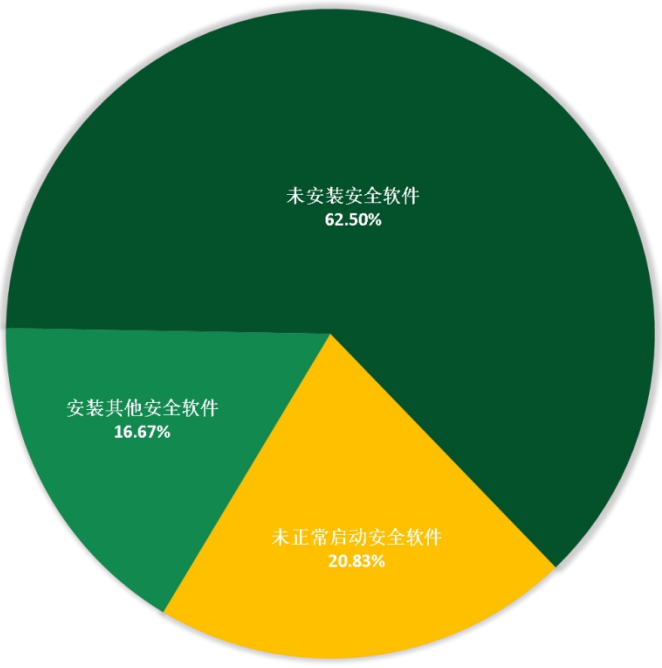

图 1. 2026 年 3 月勒索软件中招设备中安装的安全软件占比

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：Wmansvcs 家族占比 30.19%居首位，第二的是 Weaxor 占比 17.61%，LockBit 家族以 8.81%占比位居第三。

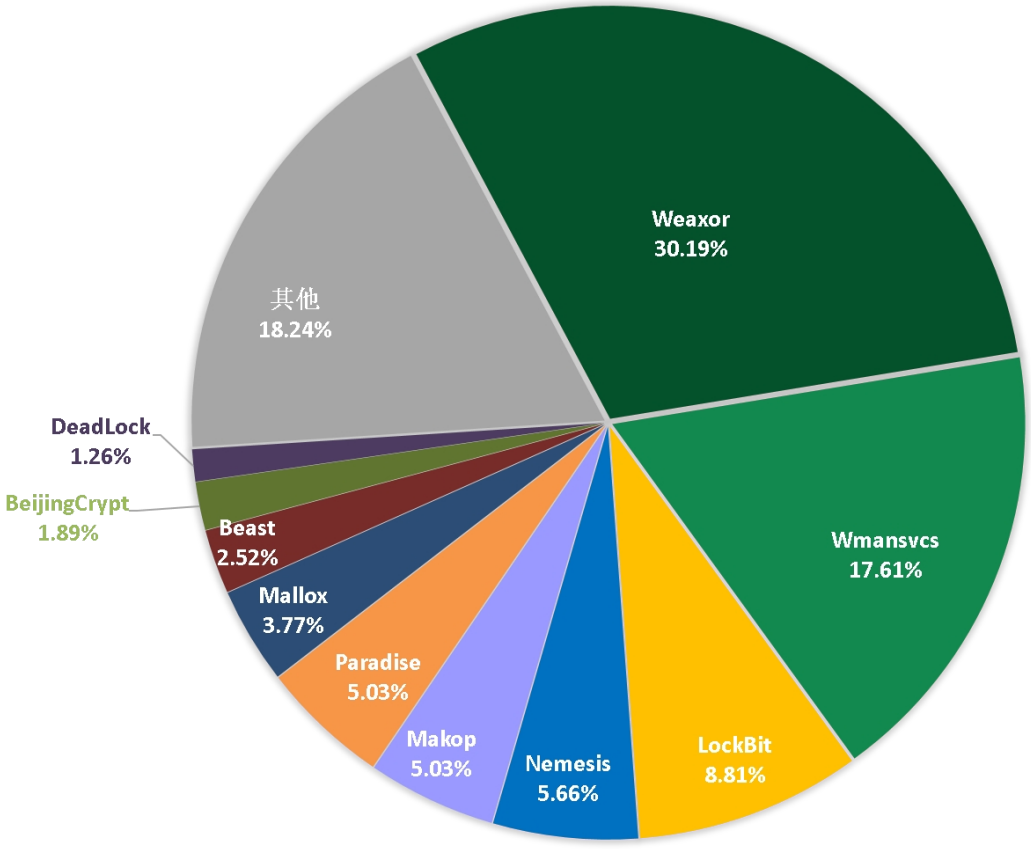

图 2. 2026 年 3 月勒索软件家族占比

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 Server 2012 以及 Windows Server 2019。

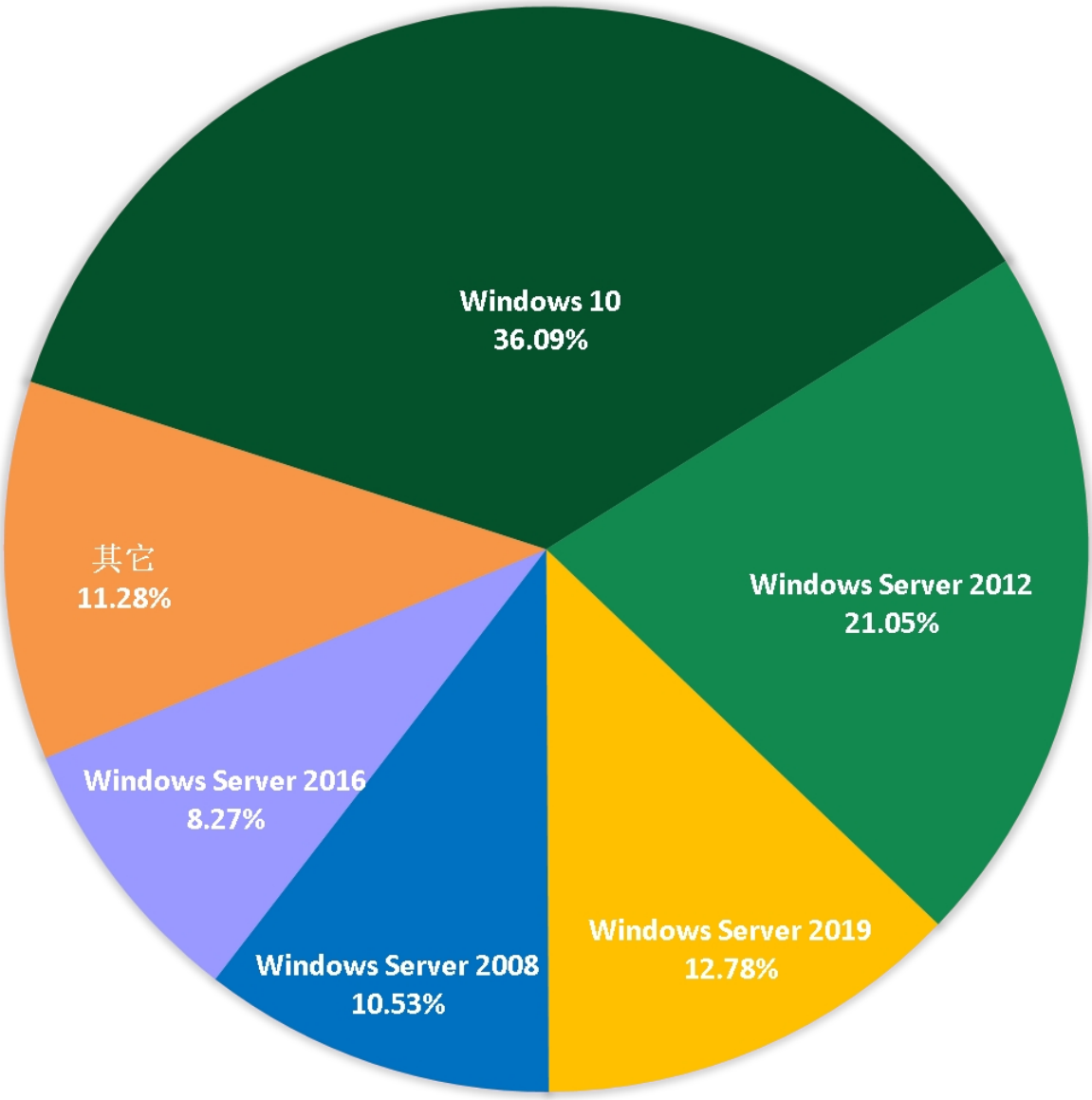

图 3. 2026 年 3 月勒索软件入侵操作系统占比

2026 年 3 月被感染的系统中，桌面系统和服务器系统占比显示，受攻击的系统类型以桌面 PC 为主，服务器和 NAS 平台攻击行为有所增加。

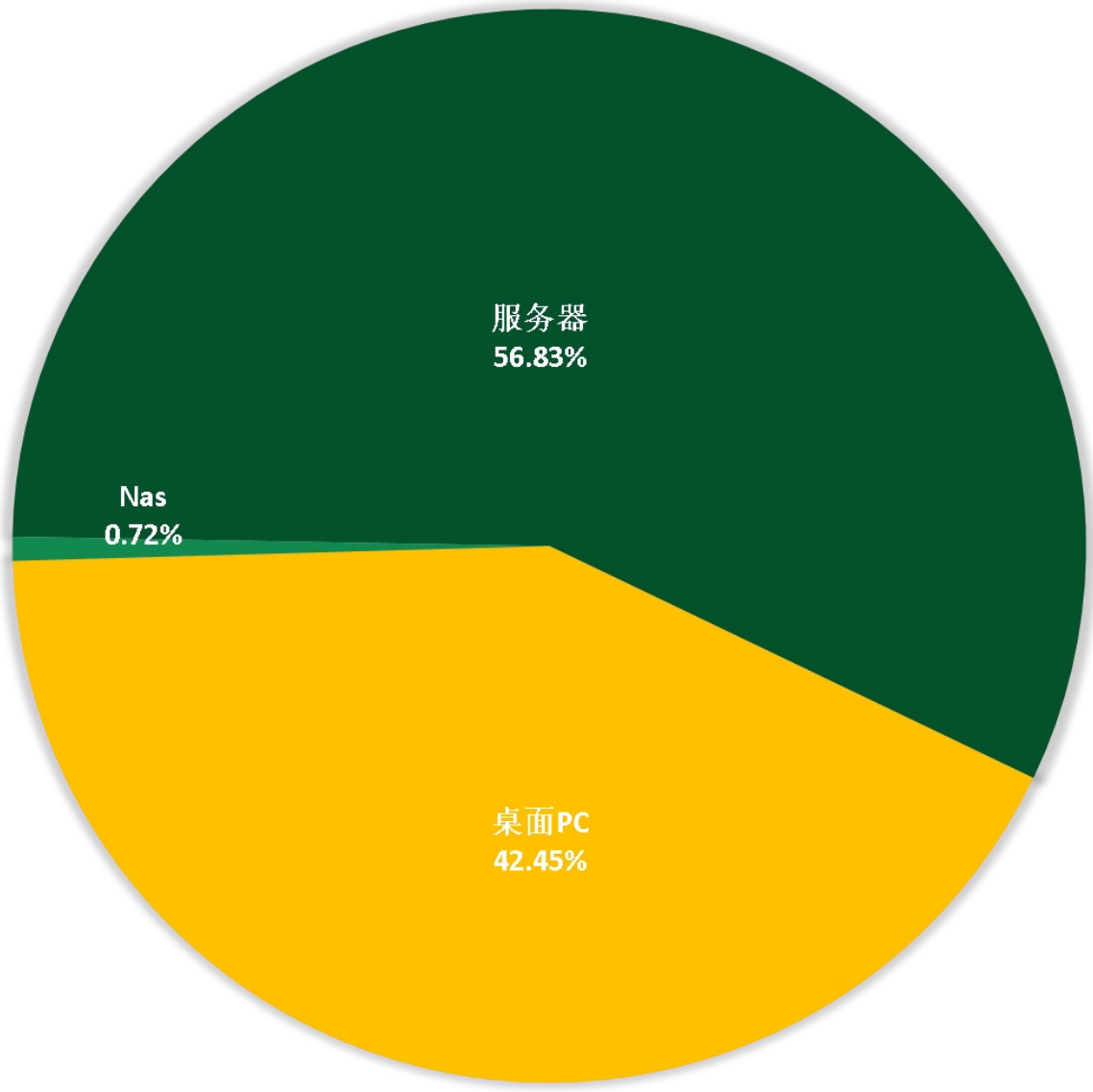

图 4. 2026 年 3 月勒索软件入侵操作系统类型占比

勒索软件热点事件

Sorry 后缀勒索软件利用 Web 漏洞大肆传播

本月加密文件名被修改为.sorry 后缀的勒索攻击出现大量反馈，本轮攻击的时间集中在 3 月 14 日—3 月 15 日。

图 5. 2026 年 3 月.sorry 勒索的传播流程

分析本轮突发的勒索软件攻击所针对的各类服务进程名称，其占比如下：

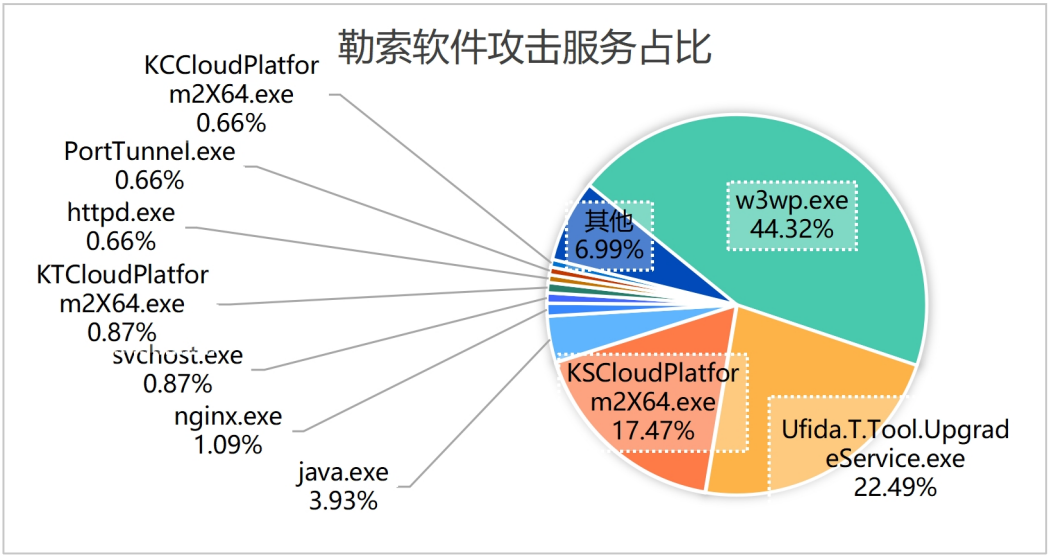

图 6. 2026 年 3 月.sorry 勒索攻击的进程占比

本轮勒索软件攻击发生的地域分布，发现北京、广东、上海位列前三，总体分布情况如下图：

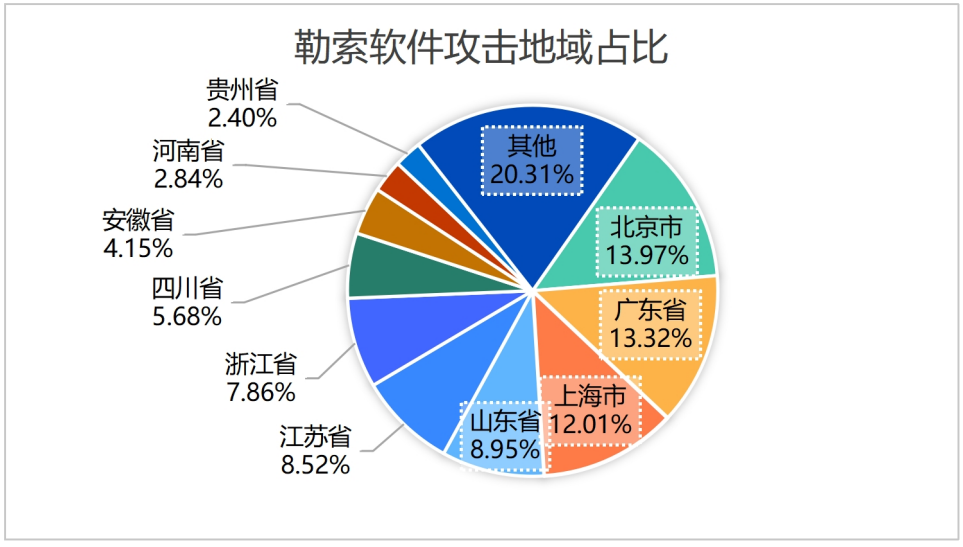

图 7. 2026 年 3 月.sorry 勒索攻击的地区占比

本轮 Sorry 勒索软件采用了时下较为流行的无文件攻击手段——

从最初的入侵到最终的文件加密，一切攻击行为仅存在于系统的内存中，不在硬盘中存储。加之目前 360 反勒索服务收到的受害反馈案例绝大多数来自事前未安装 360 客户端的用户，导致分析人员暂未获取到完整的加密器样本，故此也暂不对该勒索软件做明确的家族分类判断。

但分析人员根据以往经验，结合现有信息进行推测，认为该勒索软件的攻击手段与流行的 Tellyouthepass 勒索家族颇为相似，而其留在受害系统中的勒索信格式特征则更像是 WormHole 勒索家族。

医药巨头史赛克因与伊朗相关的擦除软件攻击而被迫离线

美国医疗技术巨头 Stryker（史赛克）遭到网络攻击，事件由与伊朗相关、支持巴勒斯坦的黑客组织 Handala 发起。该组织使用“wiper”恶意软件，在窃取 50TB 数据后，清除了该公司网络中数十万台系统和服务器，迫使 Stryker 全球范围内停工。这次攻击涉及 Stryker 在 79 个国家的办公室，多名员工报告公司设备在夜间被远程清除，部分个人手机也因注册工作访问而丢失数据。员工被要求移除公司管理和应用程序，包括 Intune Company Portal、Teams 及 VPN 客户端。

此次攻击严重影响了内部系统和应用访问，一些办公室不得不回归“手工操作”流程。Stryker 正在全球范围内恢复系统，并已与微

软及外部网络安全专家合作处理该事件，但尚未确认具体原因，也未能给出完整恢复的时间表。

Handala 黑客组织自 2023 年 12 月起活跃，曾针对以色列组织发起破坏性攻击，使用恶意软件清除 Windows 和 Linux 设备，窃取敏感数据并在其数据泄露门户公开。Stryker 在向美国证监会提交的 8-K 表格中确认了事件，称其 Microsoft 环境遭受影响，事件目前被认为已得到控制，该公司无迹象表明存在勒索软件感染，但工作环境仍将持续受到干扰。

总之，此次事件是一次大规模破坏性网络攻击，涉及数据盗取与设备清除，对 Stryker 全球运营造成前所未有的冲击。

勒索软件攻击扰乱西班牙主要渔港运营

西班牙维戈港遭受勒索软件攻击，导致港口数字系统中断，当局被迫断开部分网络连接，并临时转为人工管理货物作业。此次攻击于 3 月 21 日周二凌晨被发现，影响了位于西班牙西北海岸加利西亚地区的港口，该港口用于管理货物流通及其他数字服务的计算机服务器。此次事件导致部分设备被锁定，并涉及赎金要求，港口的技术团队将受影响系统与外部网络隔离以限制影响范围。港口负责人表示在安全团队确认网络安全之前，港口不会重新连接相关系统。目前尚无恢复正常数字化运营的时间表。

港口的物理运营包括船舶移动与货物装卸仍在继续运转，但通过港口数字平台管理的物流协调工作已受到干扰。部分承包商已被指示依靠人工程序和纸质文件继续作业。

目前事件正在调查，以确定攻击者如何进入网络以及是否有敏感数据遭到泄露。渔港负责人将此次事件描述为以索取赎金为目的的财务动机网络攻击。目前尚无网络犯罪组织宣称对此次攻击负责。

近年来，港口和海事组织因其在全球贸易中的关键作用，成为勒索软件团伙的重要目标。

2023 年，日本名古屋港在遭受据信由 LockBit 网络犯罪团伙发起的勒索软件攻击后，曾暂停运营。

比利时、荷兰、德国、葡萄牙、日本、澳大利亚以及美国休斯敦等国家及城市的港口都曾遭到攻击。

多家航运技术巨头也曾遭遇网络安全事件，导致运营中断数日。

黑客信息披露

本月收集到的黑客邮箱信息如下

demetro9990@cock.li	datahelperrx@cyberfear.com	unlocking.guarantee@aol.com
teamblding@outlook.com	hola-veglass@x-mail.pro	TrustCode@mailum.com
primedecrypt@onionmail.org	Redstarme@proton.me	up-coding@proton.me
killbillkill@protonmail.com	filessupport@onionmail.org	soria.franzeski@cyberfear.com
nhuvgh@outlook.com	brunobiden76@gmail.com	piztoreco@gmail.com
jaredwinter65@2mail.co	brickscold6@gmail.com	v3_lab_support@protonmail.com
teresabrosco136@onionmail.com	ransom@example.com	whiteshgd627736@gmail.com
decryptionfiles@protonmail.com	minimflea@gmail.com	decrypt@evil.example.com
decryptionfiles@gmail.com	fredoms_docktor@outlook.com	Gol@mailum.com
support@laboo.boo	BlueWindGroup@onionmail.org	ransom@tabnewszamanpaper73.za.com
oil@laboo.boo	SAMJINTECH@mailum.com	dschen01@mailum.com
far@laboo.boo	recoverymydata@protonmail.com	ransom@coin.sa.com
xjieb@laboo.boo	recoverydata@india.com	keylogger@asyncrat.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漏的风险也越来越大。

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）。

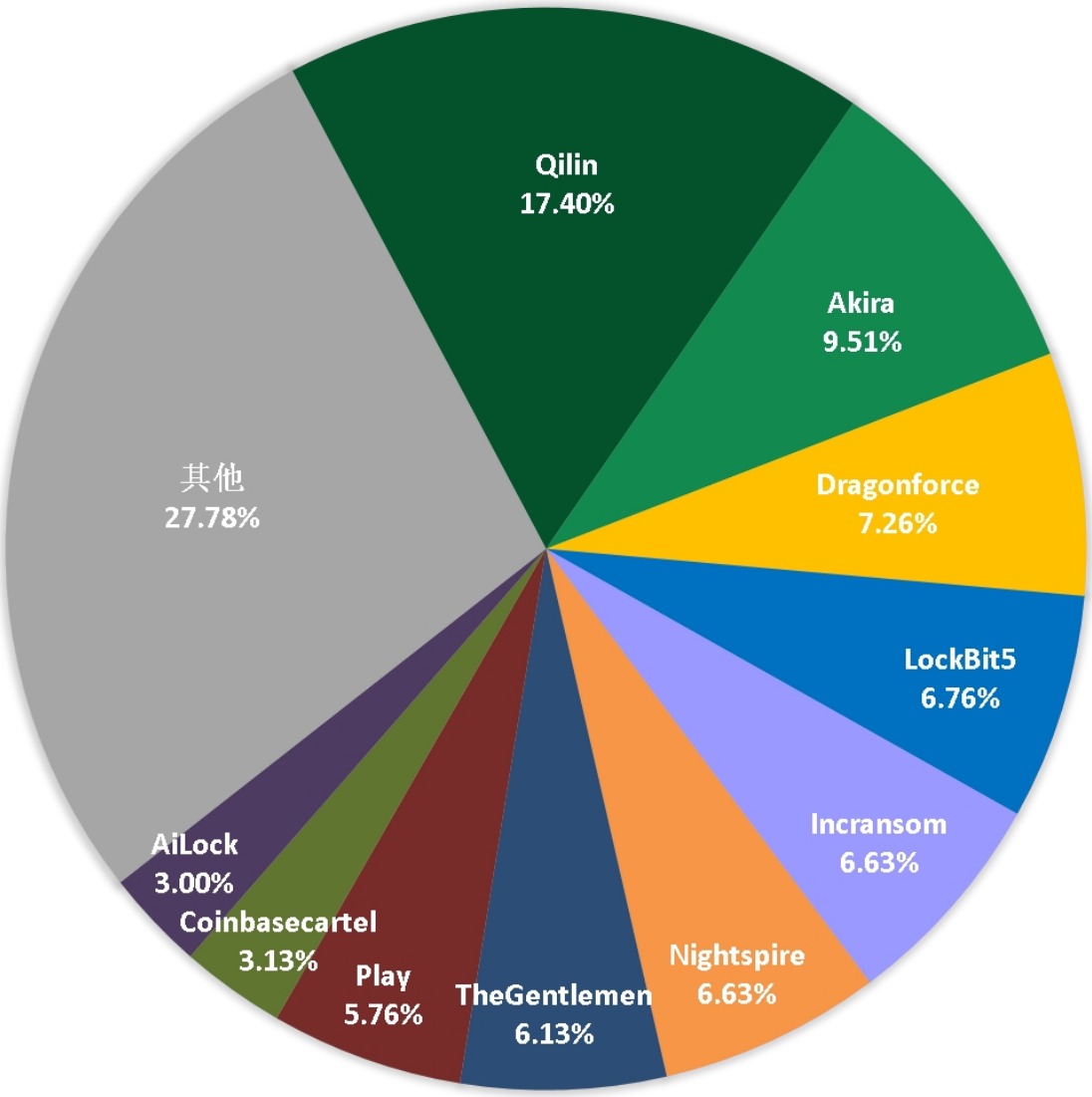

图 8. 2026 年 3 月通过数据泄露获利的勒索软件家族占比

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，做好数据已被泄漏准备，采取补救措施。

本月总共有 801 个组织/企业遭遇双重勒索/多重勒索攻击，其中包含中国 12 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 22 个组织/企业未被标明，因此不在以下表格中。

Service Star Freightways	City of Los Angeles (LA)	Taylor County Property Appraiser's Office
Seeing Machines	Town of Blacksburg	First Priority Group
SERAM SpA	Pearce Services	Estra Automotive
Cox Design & Metal Fabrication	TSN Co., Ltd.	Invaccs software technologies pvt ltd
Dean Supply	Oriska Insurance	Wagon Mound Public Schools
Excel Healthcare Receivable Management &Consulting	GD France	RWB Consulting Engineers
Catalyst Learning Company	Berkadia Commercial Mortgage LLC	Vertex Inc.
B&R Sheet Metal	Mercedes-Benz of Arlington	altaortho.com
Raphael Ortho	Lucky Innovative Manufacturing Corporation	tupeloeye.com
Green Giftz	Notar í a 89	arbd.com
HMI Elements	Accolend	Comprehensive Orthopaedics and Musculoskeletal Care, LLC
MC-Rx	vatractor.com	eDevice
Modern Advanced Print Solutions (MAPS, Inc.)	Angus-Young Associates	Nenplas
Secure Health	The Decorative Paving	Kpropha
Xiamen Tungsten Co. (XTC)	Career Adventures	Sodimatel Fasteners
delapazlaw.com	ENENSYS Technologies	Cosmesia
submissionfinance.com	Health Management Systems	Grupo San Jacinto
Chickasaw Holding	MicroChem	Infinity Systems
https://www.lagoonpark.com/	Cerio	Serrano Industries
MerchNOW	Enviaseo ESP	Helen Kaminski
San Felipe Del Rio CISD School	airports.com.na	Byard F Brogan
Q-Lab	PC SOFT FRANCE	Facilities USA
Parque E ó lico Toabr é	Onyx Graphics	Southern Concrete Construction
Hallmark Cards, Inc. & Hallmark Plus	Tecnocap Group	nch.com

CERUMO Co., Ltd	Verimatrix	Peninsular Electric Distributors
Beltran & Garcia Financial Investment SLU	Ariston	Hauri AG Staffelbach
JT-ATFP, LLC	Petra Industries	WEDGE
PT Brantas Abipraya	Bonheure	Fiberglass Hawaii
domingogarcia.com	Elgi Electric & Industries	Woodfines
millersteelelaw.com	Amerinational Management Services (AMS)	Colliers International Idaho
Straight Line Logistics	gasteiger.design	Serviceplan Group (Korea branch)
Net Solace	Construction Equipment Parts	commerfrutta.com
Posiflex	Dynex/Rivett	fac-srl.net
Dronena	Flexform	McKenna Pro
Siveco	HARTMANN BAU	Pleiad Investment Advisors (Singapore brach)
Northcroft	Delta Manufacturing	Sagent Pharmaceuticals
Silver Peak	Conrad Capital Management	Geotec Surveys
Buffalo Neuroimaging Analysis Center	loopcap.com	Artemedica
Nashua	Valley Family Health Care	Kuzco Lighting
Studiosus Reisen Munchen	BTX Global Logistics	Brothers Produce
barrypgoldberg.com	hollu Systemhygiene	Dielco
Jones Day	Arca Service	Stalwart Development Group LLC
Brokk	Elite Flower	crescentenergyco.com
Colorado Construction	Jacobs & Sons	Sileno Companies Inc
Lucky Look	Sievert Electric Service and Sales	Griswold Controls
Weber Kracht & Chellew	Productos La Aguadillana	NADAP
Specflue	L H Lacy	City of Hart
Kivells	Affinity Designs	Brighton Eye
Dock Pros	Rainbow Technology	Cornerstone Financial Advisors, INC
Ampex Data Systems	Reflex Angelo	Sanders Legal Group
Valley Plating Inc	Texollini	OneSource Medical Group
Witt UK Group	Pyr é n é es	Sierra Management Group
Parkway Reality Group	Vexin Normand	societaitalianaalimenti.it

NKAR Travels & Tours	GPAINNOVA	AFDL
SBCTANZANIA	2LG Prod	Johnson Vollmerhausen & Gates
Dow	Excellentiam	Netwerk NV
Wm Erath & Son	Economia	Eeyou Communications Network
Richard J. Hackerman P.A.	Summa Energy	Ladue Family Dental
Wyatt Insurance Agency	Interpack Northwest	CPG Documentation
Summit Tax Advisory	Wood Smith Henning & Berman LLP	Northern Family Farms
Office Peeps, Nappie's Food Service, Janome America, IT-Supporten, A-1 Pools.	Fannin CAD	MAGNETA LOGISTICS, UAB
Miles Electric	hospitalvetdiadema24h.com.br	11th Street Veterinary Hospital
Blantyre Capital	palram.com	City of Huntington
Motleys Asset Disposition Group	brookercg.com	thallos AG
iliad.fr	tiefenbachergroup.com	T a Solberg
GYF	briwaycarriers.com	Don E Bower
Conveyors, Inc.	mattandsteve.com	Design To Print
knewin.com	thenavigatorcompany.com	Select Tool
VX Case	Eco Sound Builders	DFW Aero Mechanix
Alliance Select Foods International	McAfee Tool & Die	Garland Williams & Associates
Greenology Products	Teco	nelsonworldwide.com
Doctor.com	dpwh.gov.ph	Nephrology Associates
Ming Hwei Energy	Knight's Site Services	Malia Group
polsat.pl	Gsolutionz	LAF Hotel Aree
lacor.es	Shwapno	Gerleinco
kyoceradocumentsolutions.eu	doghairinc.com	smileteam.com.au
kob.com	vanheyghenstaal.be	ASB Saarland
European Commission	isosl.be	Albany Pumps
OTNet	Bonanza Casino	H & L Systems
Florida Therapy Services	bestgraphics.net	Suchthilfe direkt Essen gGmbH
IBB Institut f ü r Bildung und Beratung	Solutions Extreme Technology	Waterloo Information Systems
TR Construya	Passaic County	Orange Madagascar

Q2 Artificial Lift Services	Cape May County	Graham County Electric Cooperative
Don-Nan	Lehigh Carbon Community College	Hyundai Elevator
terix.com	Noll and Tam Architects	WAG Funktion Design
A A Al Moosa Enterprises (ARENCO Group)	Von Weise Associates	Siwax Specialties Group
kdmpop.com	Folet & Rivoire	The Delventhal Company
meridenct.gov	mcquaidinjurylaw.com	Advanced Rehabilitation Technology (ART)
Sheraton Hotel	Singleton Schreiber	R&C Fence, Inc.
CIM	PINNACLE TAX INC	Verdugo Tool & Engineering
Orient Petroleum	frazercenter.org	North Central HIDTA
Leighton	Tax & Accounting Plus	A C Scott Electric
Fondation Boghossian	Steve Quick Jeweler	ICS Electrical Services
GeoMechanics Technologies	MCC Economics	C.A. LINDMAN Inc.
Edward Beiner	Broadway National	INTERACT TECHNOLOGY SOLUTIONS
Axiomatic Technologies Corporation	Mingat Location	Edgar Agents
Quality Carton and Converting	Caribbean Medical Center	salfordcc.ac.uk
Sheladia Associates	Pilana Group, TRITCON	pacepacific.com
ITWAL	Ruhnau Clarke	Transsion
BHS Bau	Centro de Especialidades	CFGI Management, LLC.
Kerjaya Prospek Group	Cortporation Colina	MyFair
ACR1.COM Commercial Roofing	Kabelovna Kabex	MedicalGPT
Frontier Technologies	Payap University	yurdriversnetwork
Big Thumb	Canal Capital	northstaria.com
Schlam Stone & Dolan LLP	Chase Asia	parkerlipman.com
Scalian	BCN Medical	Tennessee Valley Electric Cooperative
STS Travel	Biogel	Cheongdam OracleClinic
Groupe Courtois Automobiles	Executive Aviation	Nopa Industriearmaturen
ActionPower	Salag	ELC Security Products
carlysle.net	Evaluate a Norstella company	A Lococo Wholesale
jaxa.jp	Royal Bahrain Hospital	Abutriek

njpcs.org	Aura Group, Inc. (aura.com)	Schaltbau
Netalia	Private University	Applied Products
Durable Superior Casters	ILLUMINA - Data uploaded	Donjon
ludlums.com	Augenomics	Ecofit
TPIS Industrial Services	nChroma Bio	K & S Company, Inc
Bedrosians Tile & Stone	Geno Bank	Trionex
Transgas	Neochromosome	DesignSourceCT
Washoe Tribe	Novogene	JBS Brazil - We have 3TB of your data
Maderas Del Noroeste	J.T. Pack of Foods	CTI & Coordinators
Voltamper	Grid Fine Finishes	Rowad Modern Engineering
Arnaud	Alcoholes Finos Dominicanos	barberopietro.it
Sacor	In.Sa.Cor	Jameson Pepple Cantu PLLC
Kaemmerlen Solutions	Thai Solar Energy Public	KLEIN IBERICA SA
Louise Medical Center	United Limsun International Trading	piglerautomation.com
ires.ma	Tyler Media	Environmental Air
2m.ma	Río Grande (Puerto Rico)	saturnmachine.net
centrum.sk	westport.com	CJL Engineering
www.davidhelfandlaw.com	indrub.com	AHMED MUBARAK DEBT COLLECTION
iam.ma	Trinity Catholic High School	Pantomath Group
ETFSA	Communicate UK	Tenteks Tente
Living in green, s. r. o.	Mid-America Export Experts	Öztekin Group
Mac Interiors	Duffy's Sports Grill	Communitymosaic.co.uk
Goodwill	meena health	Eos Technology srl
Monmouth University	NextCapitalTrust	MarketGraphics Research Group
LP Kolding	www.integer.net	lawofficesoferichershler.com
Noi Hotels	KLA Laboratories	hopkins-law.com
ssp-ce.de	Alarmco	bclawoffices.com
kalimaresort.com	Stokes	Reynolds DeMarco & Boland
pridesol.com	FMRS Health Systems	Huffman Insurance Agency
C..er CPA	Wills Point Chevrolet	Business Automation Specialists of

		Minnesota
ZenBusiness, Inc.	Millard Manufacturing	HTH Companies
esprinet.com	Hebrew University of Jerusalem	Nicholas & Tangeman
pulpdent.com	emp.id	Primus
Live! Casino	atrium.com	Comtec 2000
glenmarkpharma.com	paolidental.org	Reanthong Partcenter
Anbogen Therapeutics Inc.	sportvision.ba	Outsourcia
Eastex Environmental Laboratory	cti-bat.fr	Golden Clay Industries Sdn Bhd
HLF Heizung-Sanitär GmbH	praxis-oberhof.ch	NEW GENERATION MEDIA
Vancompare Insurance	thaihua.com	The City of Hesperia, CA
PWNA Plains	landsteiner.net	BK Group
cerboniservices.com	hb-technik.at	ATS Group
jenningsk12.org	tanufwater.com	Vision Aero
Aroostook Mental Health Services	elmwoodhomecare.com	Lincoln Green Brewing
Retail Centenario	townoforangeva.gov	cwpa.com
All Real Estate Title Solutions	pkmsteel.com	formula50.it
Roxiticus Golf Club	al-alawi.com	Bravo Electro Components
Pinnacle	index-precast.com	ICAFe Companies
Ascent Asset Group	ikron.org	Dr. Pizzoglio
Capital Wholesale Drug	webster-schools.org	Klevorn
Block Engineering	audiconcontadores.com.br	AKOL LAW
Window & Door Design Center of Florida	limpebras.com.br	Verlat Energy
Concord Components, Wefapress, Environment Masters, FairmontHot Springs Resort,Road Americ	facsrl.net	Napolin Law Firm
Concord Components, Wefapress, Environment Masters, FairmontHot Springs Resort,Road Americ...	alcornschools.org	Law Offices of Mark E. Lewis & Associates
Mooers Immigration	frasierlaw.com	importservices.co.uk
M3 Group	cognitivehealthit.com	Brockman Injury Lawyer
French Engineering	Irec Sas	Hersher Law
Gustavo Preston	phoenixlabs.com	Hopkins Law

The Russell's Law Firm	Keller Polska	Lawrence Journal - World
Estudio O'Farrell	Africa Insurance	Minogue Associates
Kiswire	Einstein Technology	ripobec.com
iGLS	St Fabian Catholic	Luro
Marborges Agroindustria	ControlGMC	Viviany
Groupe SFPI	Syed Professional Services	Aluthea Group
Atlas Ocean Voyages	TDS Construction	ukimportservices.com
Nafco	Silvon Software	Franz-Sales-Haus.de
CONCEPTNET	Financial Brokerage	Equine Canada
Rioja Motor	Bioptik Technology	GapVax
Mantra Softech Pvt	Circle Floors	Katz Kantor Stonestreet & Buckner
Marion Military Institute	Eagle Industrial Equipment	Conklin Office Furniture
Schmiede	flad.com	JBC Computers
Autitransa	Extreme Trailers	www.chrishudsonlaw.com
Delta Ducon Engenharia	Porsche Zentrum Fulda	Encompass
Grupo Tawa	moccae.gov.ae	Camelot Electronics Technology Co., Ltd.
Omikenshi	Giaroli S.A.S	CHS Villach
Distritech	Mh Soluciones	Belmont Plastic Surgery
Dixon Electrical Systems & Contracting	University of Mississippi Medical Center	maisonlaw.com
JDV Products	shj.ae	Les Oliviers
Ameriprise Financial, Inc.	bassignanicave.it	Union Laitiere de la Meuse
Infinite Campus, Inc.	gedco.ps	Demanor
Southern Commercial Real Estate	haca.ma	Aaronson Rappaport Feinstein & Deutsch
Southwire	England Hockey	Dallas Regional Chamber
pellenc.com	AbelZeta	ShopBot Tools
nPower Technologies	NIXVAL IT Infrastructure	Navicore Solutions
Elite Limousine Plus	Aura Group, Inc	Professional Retail Outlet Services
J E Culp Transport	Arimex Importadora	S&R Compression, LLC
Phelps Dunbar	Fortress Systems	Emanuelson-Podas

Marc Dorcel	Stryker Corporation	ELO Digital Office
Cannavative Group	Verifone	Promotion Management Center
SAS CAP ESTEL HOTEL	Canada Goose	Sterling Industries
Semenya Furumele Consulting Engineers	Lacoste	Raw Seafoods
HOPPECKE Singapore	Staples	FUJIFILM Speciality Ink Systems
PTT Philippines	E-Fci	Lewis Drug
SATS Sports Club Sweden	JJR Engineering & Fabrication	HomeSite Services
toncandigital.com	Alef Realty, LLC	Revival Animal Health
ssskwt.com	seclore.com	AJ Networks
roamingnetworks.rs	D3 Embedded	Integral Analytics
manchester.com.mx	Big Brothers Big Sisters	IOTA HOTEL TBILISI
glop.mx	Tecnoedil S.A. Constructora	Andal Law Group
flamagasindia.com	CFTC M é tallurgie	Woflow, Inc.
charliebears.com.au	Chartre Consulting	Bartram Trail Surveying
rovinj-rovigno.hr	ToolpartsPro	Lundeen Consulting
breastcare.com	AMEVIDA	Fusion Superplex
jean.com.tw	Internation Planning Group	Bayshore Ford Truck Sales
sidercentersas.com	Shaft Drillers International	Gordon/Clifford Realty
sesi.org.br	Acme	Cabka
senai.br	Frauenshuh	The Kuker Group
fiepe.org.br	AIGHEALTHCARE.IN	LRA Constructors
luetz-binder.de	CLOUD.CLEARWAYGROUP.COM	Cobblestone Creek Country Club
gov.krd	Priderock Capital Partners	Project Consulting Services
ombudsman.gov.ws	thethibeauxfirm.com	Go Professional Cases
nandrin.be	Kentucky Injury	WCC Technologies Group
maritasdenim.com	ubm.hu	Favaro Lavezzo Gill Caretti
isoledilcappotti.it	Special Shapes Refractory	Phoenix Systems
Grupo Coril	Powers HVAC	Akkök Holding
Muffett	Jadtec Security Services	IDH Entertainment
hikvision.com	Omega Optical	Soreco

irco.com	Robinson Nursery	https://www.precisioncoating.com/
Millerfoto	Murray's Cheese	Bain Oil Company
Nanxun Enterprise Co., Ltd.	Peak Toolworks	SIMETRI Inc
IASMOS	Curtiembre Austral S.R.L.	Martin, Cukjati & Tom, LLP
Fidanque Hermanos e Hijos, S.A	Yuma Sun	TIW Group
MEDICUS SHUPPAN	Composition Systems	giunti.it
Rajagiri Hospital	Retamar	Southold Town Senior ServicesSouthold Police Department
Micro Leasing	UMBERG TREUHAND AG	Grupo D'arc
Groupe Caddac	seit.cl	fgv.br
Elundini	hazeldenes.com.au	AkzoNobel
Resch Maschinenbau	bg.ac.rs	http://ramet-trom.co.il/
WAL Consultant	novoair-bd.com	City of Seal Beach and Seal Beach Police Department
Edifice Design + Architecture	Elliott-Lewis	Enterprise Network Group of Indiana
The Farese Group	Docaret	denmark.k12.wi.us
TS Lines Philippines	shlomo bit	abramssales.com
smythco.com	L. S. King and Associates	lke-group.com
Savvy Hawk	Institute of Social Security - Paraguay	Afezo
theunlimited.co.za	Paass Logistik	Ricopia
wardencc.com	csi-ri.com	All India Minerals
odayequipment.com	banak.com	Labtician Ophthalmics
AGENCAVI SRL	bankasia-bd.com	Special Shapes Refractory
INP Schweiz	Exhibit Network	LISI Group
sopower.com	netCOMPONENTS	yaomazi.com
liverpoolphil.com	maa-architects.com	omaxauto.com
centreconcrete.com	tazzetti.com	brassuco.com.br
Madesmart	LHT Holdings Limited	diesel-electric.co.za
VirtualExpo Group	Teknopres_TR	Riach Gese Jacobs
Motorpal	Advanced Animations	Traffic Tech
bdtronic	A-Fast Tile & Coping	PLUS Malaysia Berhad

Matthews Real Estate Investment Services	RetireRight Financial Planning	https://www.hegelmann.com
Winmate Inc.	Salford City College	USHA International Limited
Legacy Health LLC	Root Security	DAINTY CLOUD INC
Finance of America Companies Inc.	A J Taylor Electrical	

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，具有黑客入侵防护功能。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。

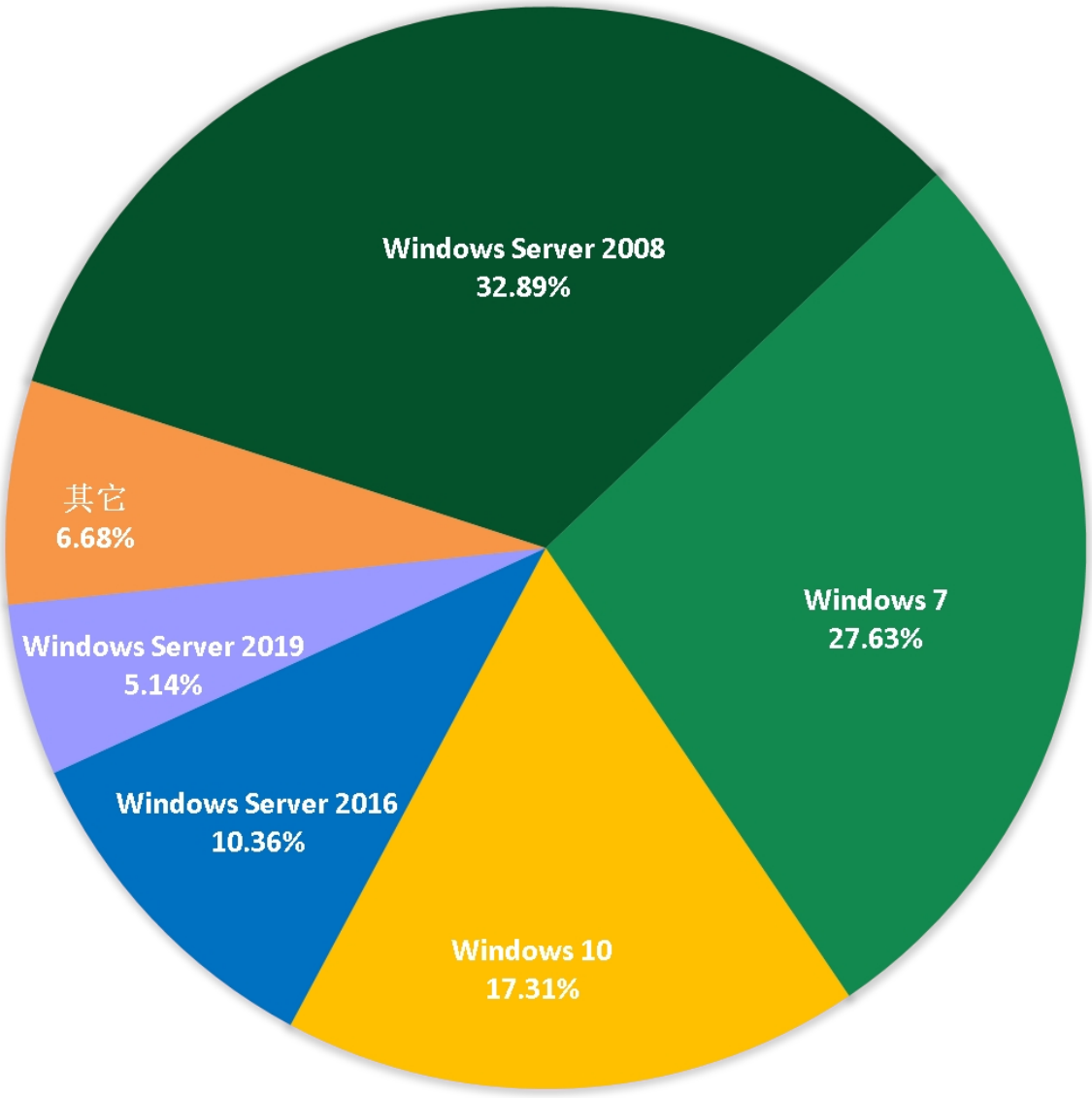

图 9. 2026 年 3 月受攻击系统占比

对 2026 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。

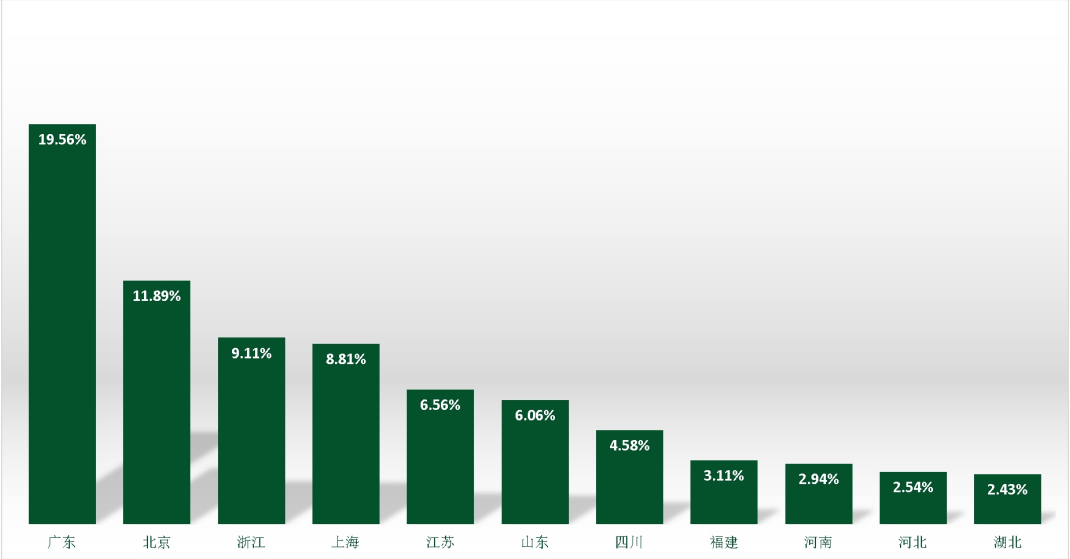

图 10. 2026 年 3 月国内受攻击地区占比排名

通过观察2026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。

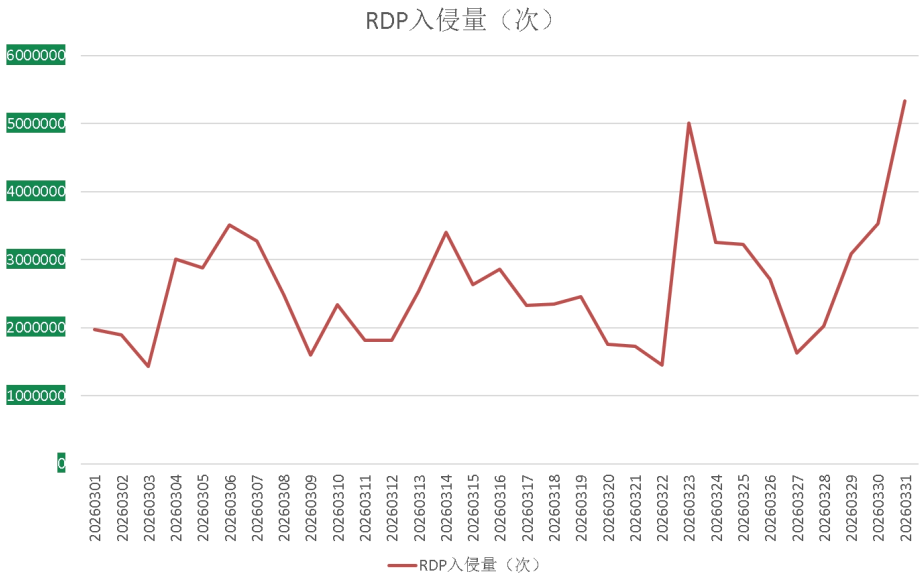

图 11. 2026 年 3 月监控到的 RDP 入侵量

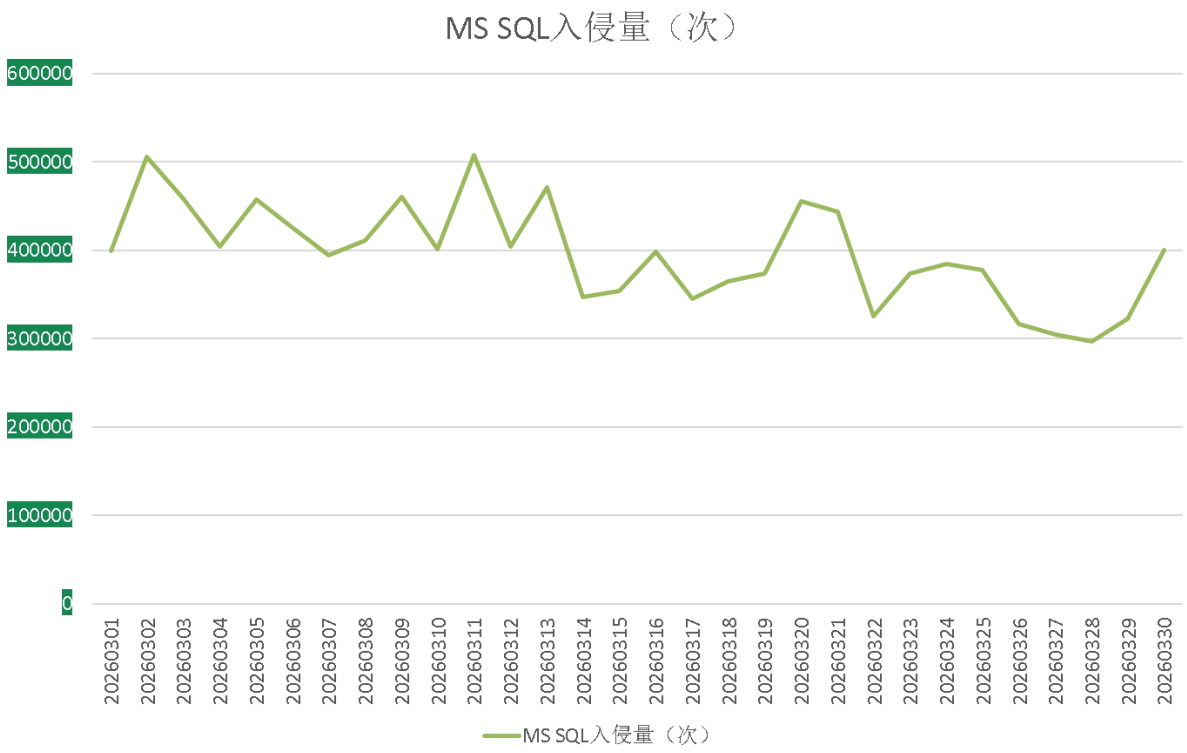

图 12. 2026 年 3 月监控到的 MS SQL 入侵量

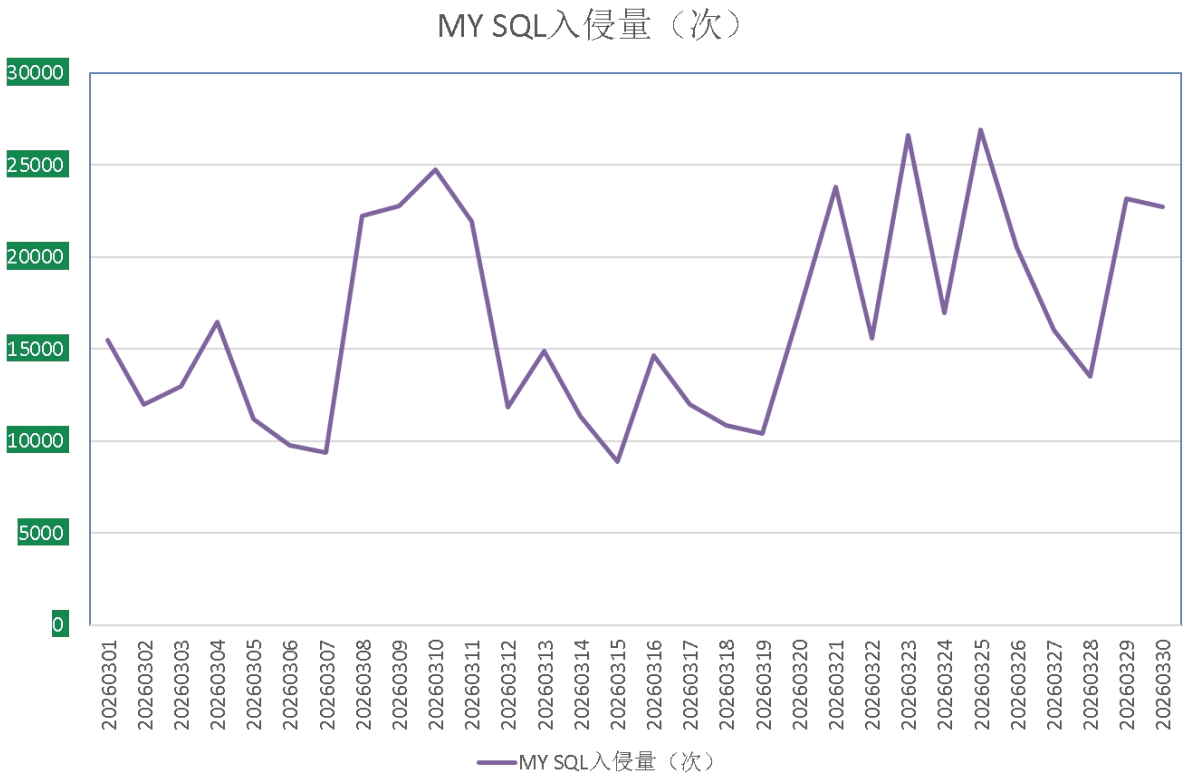

图 13. 2026 年 3 月监控到的 MYSQL 入侵量

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。

- rox：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，通过 powershell 加载攻击载荷并注入系统进程，多轮加载不同的漏洞驱动与安全软件进行内核对抗。部分版本会通过暴力破解登录数据库，植入 Anydesk 远控进行手动投毒。
- sorry：暂未明确家族归属，通过 Web 漏洞发起无文件攻击。全部攻击行为仅存在于系统的内存中，不在硬盘中存储。
- ink：无明确家族归属，需待后续有效反馈再进行研判。
- taps：属于 Paradise 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与数据库弱口令，成功后手动投毒。
- wman：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。
- beast：属于 Beast 勒索软件家族，该家族的传播方式多样，具备暴力破解、漏洞利用、共享加密等多种攻击方式，同时具备跨平台加密能力。
- baxia：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。

✧ helpers：同 beast。

✧ mtullo：未知勒索家族或变种，由于相关受害者均未配合进行溯源分析，故待后续有效反馈再进行研判。

✧ rx：同 rox。

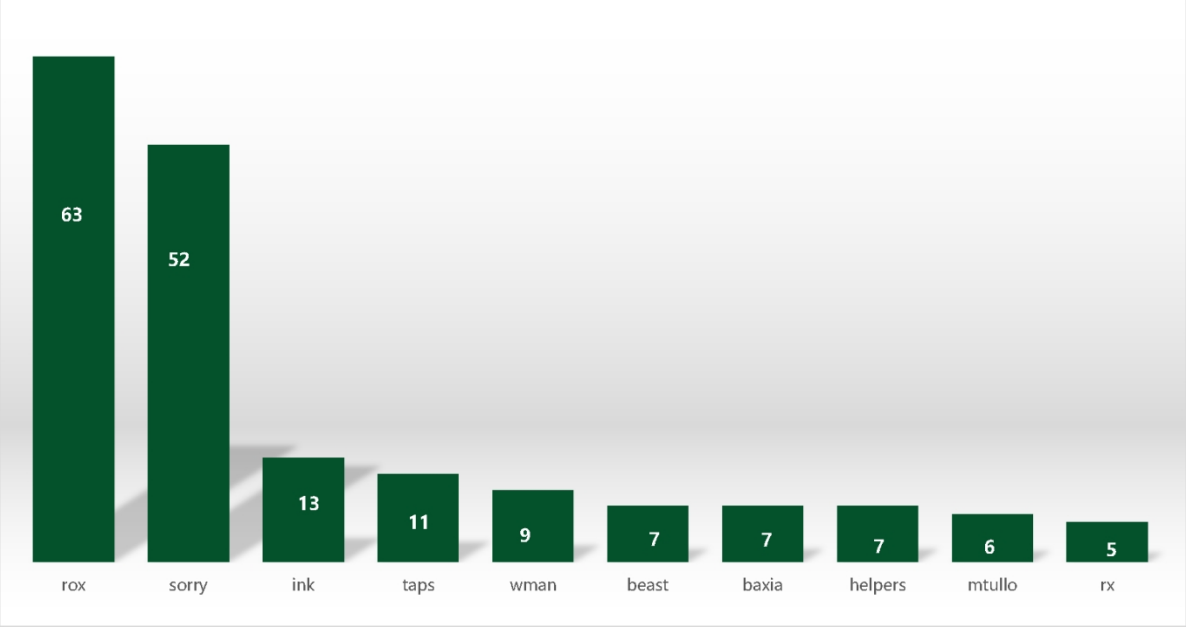

图 14. 2026 年 3 月反病毒搜索引擎关键词搜索排名

解密大师

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

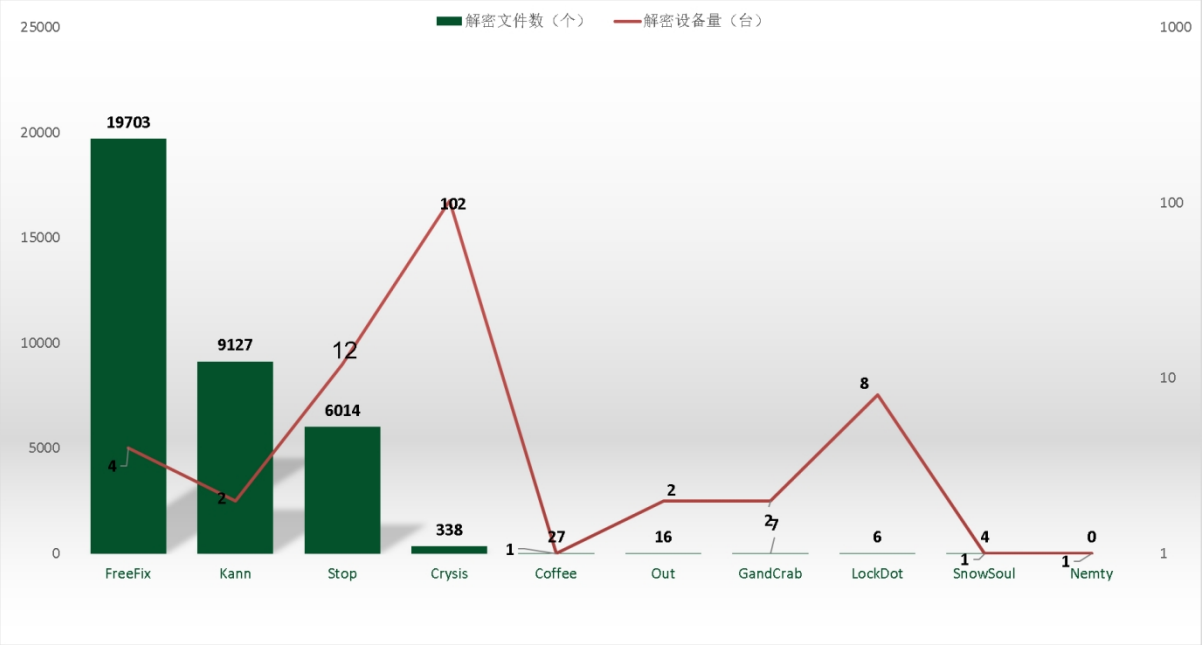

图 15. 2026 年 3 月解密大师解密文件数及设备数排名