2026 年 2 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 2 月，全球新增的双重勒索软件有 Reynolds、Payload、Cipherforce、ShadowByt3$家族，传统勒索软件家族新增 NopName、Внимание、Moniro、IronChain、EagleLocker 等多个家族。

本月在国内持续热门的勒索家族 Wmansvcs 家族新增了多个远程桌面攻击 IP,终结了自 2025 年 6 月以来仅靠唯一 IP 发起攻击的模式。

本月 Mallox 家族针对某品牌 NAS 设备的勒索反馈有所增加，攻击方式以 N day 漏洞 CVE-2023-48795 利用为主。提醒使用 NAS 设备的用户需及时更新厂商的系统版本，修复安装漏洞。

以下是本月值得关注的部分热点：

① TlerOne 勒索论坛在监管执法行动后被迅速创建

② 罗马尼亚石油管道运营商 Conpet 证实在勒索攻击中数据被窃

③ ShinyHunters 勒索团伙声称 Odido 数据泄露事件影响了数百万人

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 反勒索服务已经存在十年以上，并长期致力于全网勒索病毒攻击的响应、分析、处置、攻防、预警、解密等工作。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 65.33%，未**正常启用** 360 安全软件的设备占比 16%，安装了其他安全软件的设备占比 18.67%。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。

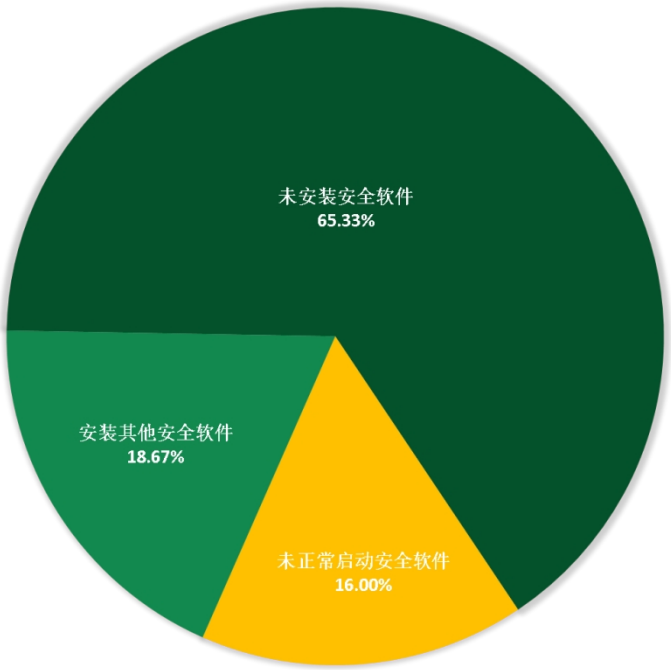

图 1. 2026 年 2 月勒索软件中招设备中安装的安全软件占比

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 31.40%居首位，第二的是 Weaxor 占比 16.28%，BeijingCrypt 家族以 13.95%占比位居第三。

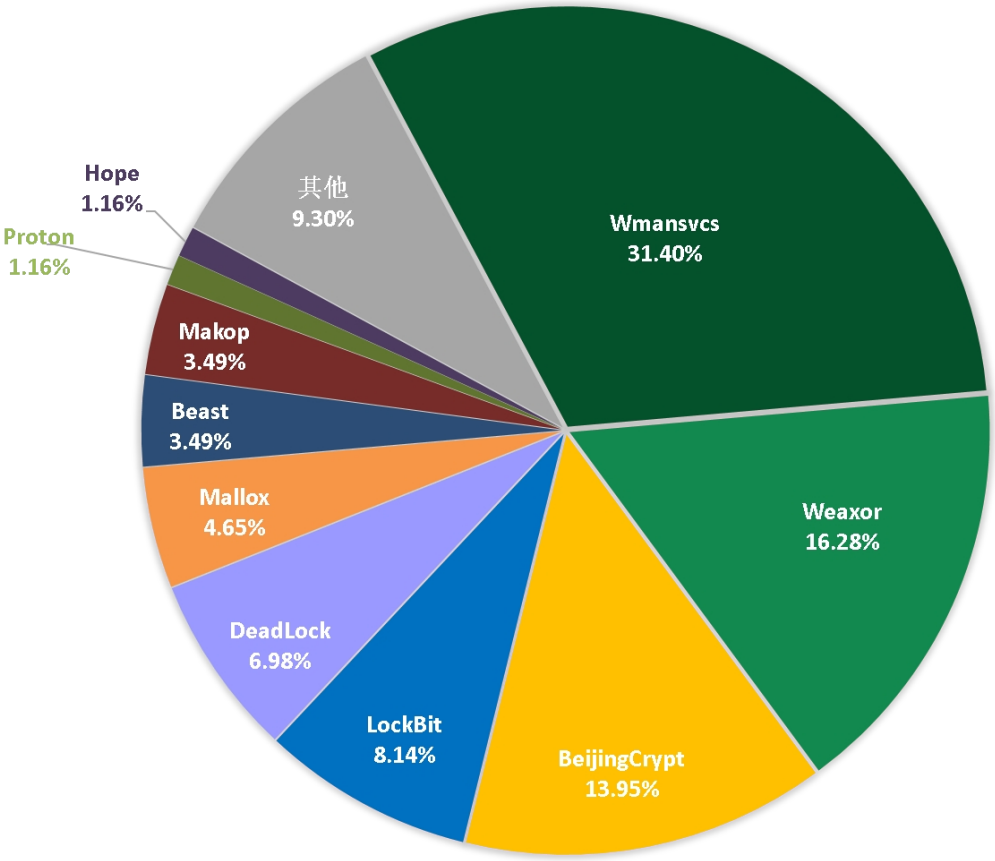

图 2. 2026 年 2 月勒索软件家族占比

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 2012 以及 Windows 7。

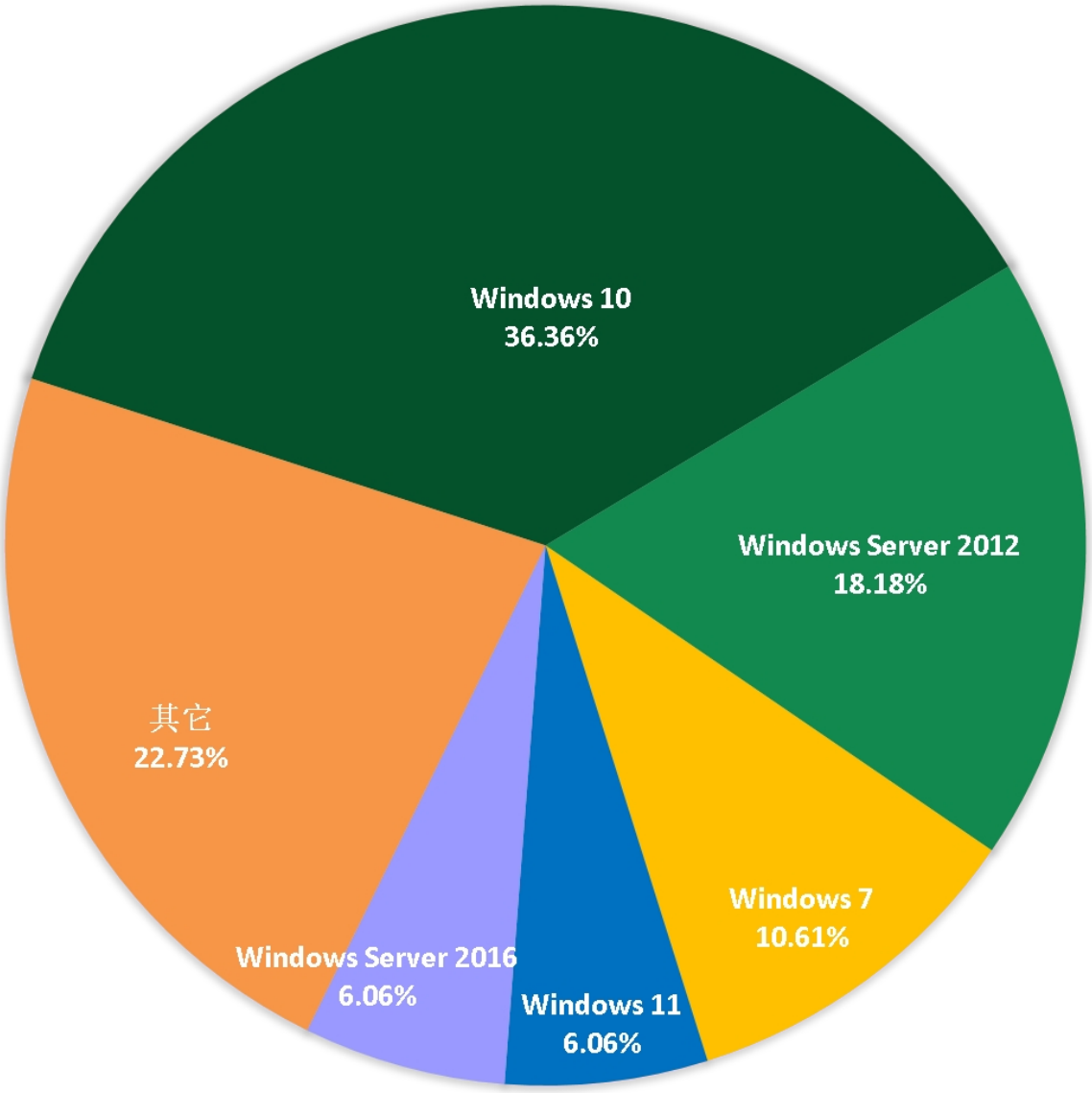

图 3. 2026 年 2 月勒索软件入侵操作系统占比

2026 年 2 月被感染的系统中，桌面系统和服务器系统的占比显示，受攻击的系统类型中，桌面 PC 领先于服务器，NAS 平台攻击行为有所增加。

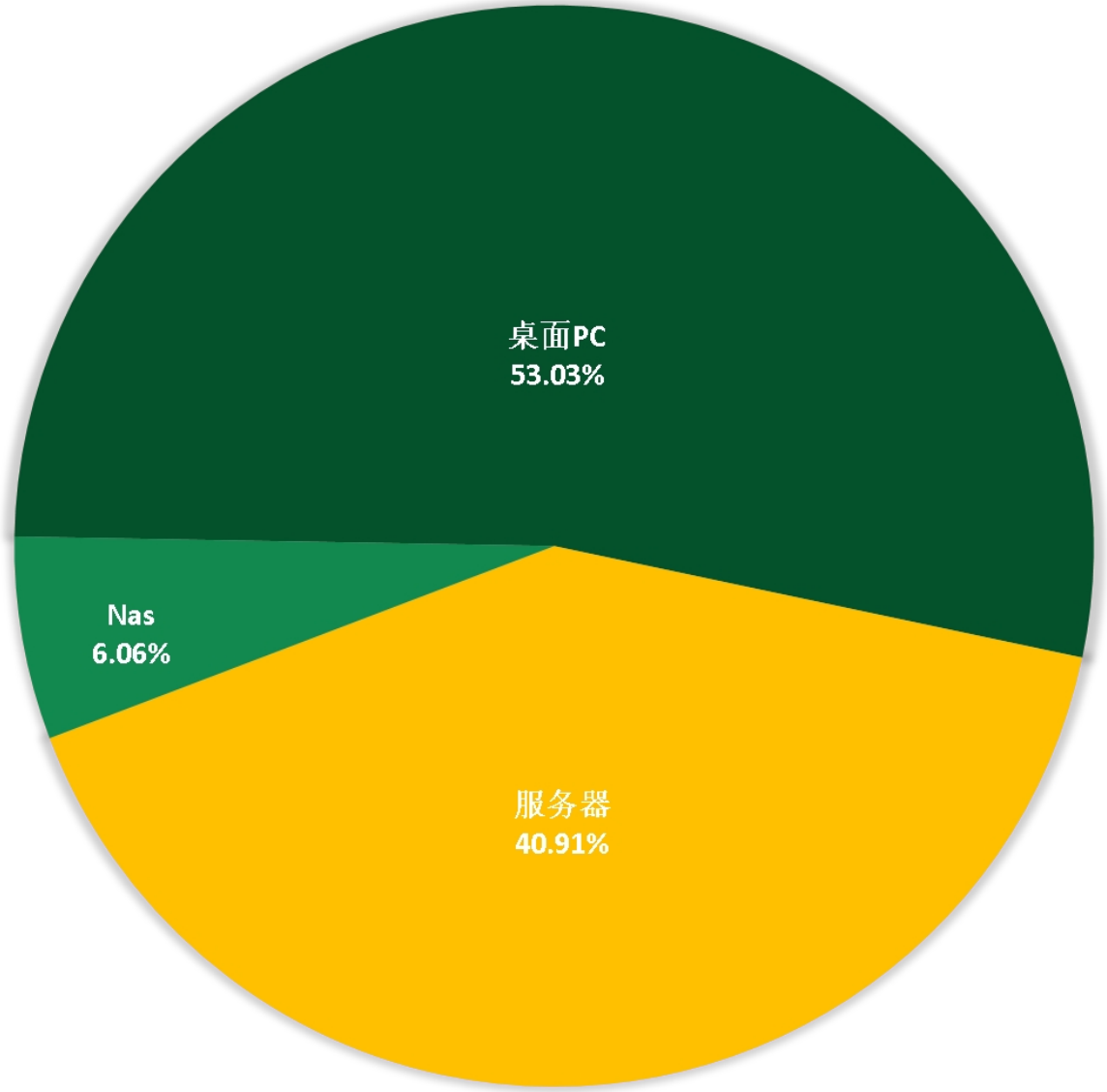

图 4. 2026 年 2 月勒索软件入侵操作系统类型占比

勒索软件热点事件

T1erOne 勒索论坛在监管执法行动后被迅速创建

监管机构在 2026 年 1 月 28 日查封了全球知名的勒索软件论坛 RAMP，与该论坛相关的勒索家族包括 Conti、Black Basta、LockBit、BlackCat、Hive、Ragnar Locker、DragonForce 等。但在 2 月份就出现了新的勒索论坛 T1erOne 作为其潜在的继任者。T1erOne 是一个封闭论坛，采用邀请与付费会员制模式，要求用户在其他黑产论坛上有攻击经验背书，或支付 450 美元，同时会向用户强调排他性并进行信誉审查。

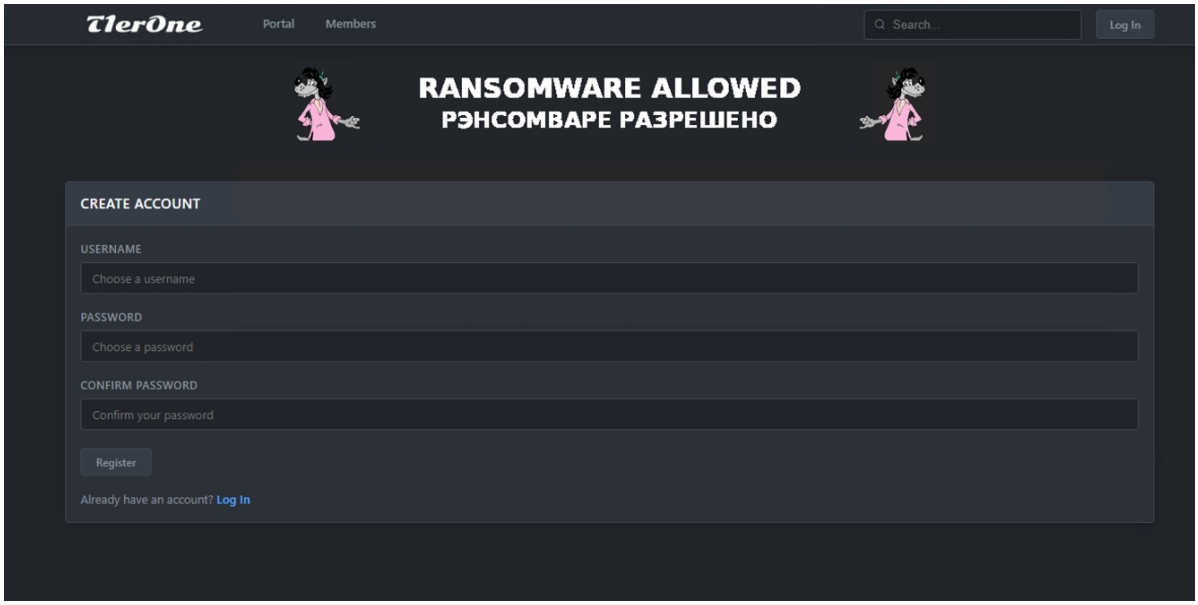

图 5. 2026 年 2 月创建的 T1erOne 勒索论坛

为了方便快速理解这一运营模式，这里我们将其类比为影视娱乐类资源类的 PT（Private tracker）下载站点。黑产从业者通过相关

地下论坛进行攻击者招募、交流咨询、投放广告等运营活动。通常勒索组织成员会同时活跃在多个地下论坛站点。其中 T1erOne 的这一模式与此前的 RAMP 论坛的运作方式极为相似。虽然这种相似性并无法证明 T1erOne 是 RAMP 的直接继任者，但从行为习惯上看 RAMP 的老客户大概率会选择快速迁移，填补被监管查封后的真空。

罗马尼亚石油管道运营商 Conpet 证实在勒索攻击中数据被窃

罗马尼亚国家石油管道公司 Conpet S.A.确认遭到 Qilin 勒索软件团伙的攻击，导致公司数据被窃取。Conpet 是由罗马尼亚能源部控制的一家战略性公司，负责通过 3,800 公里的管道网络运输原油、天然气和凝析油。

事件发生后的次日，Conpet 发布新闻稿称，攻击者突破了其企业 IT 基础设施，但运营未受到影响。公司目前正在与罗马尼亚国家网络安全局（DNSC）合作进行调查。

Conpet 进一步确认，Qilin 勒索软件的攻击导致了数据外泄。由于调查仍在进行中，该公司尚未确定被盗数据的具体量。Qilin 团伙声称从 Conpet 的系统中窃取了近 1TB 的文件，并通过泄露 16 张含有财务信息和护照扫描件的内部文件样本来证明其入侵。这些文件中包含个人信息，如姓名、邮政地址、个人识别号码和银行账户信息，一些文件标记为机密，日期包含至 2025 年 11 月。

Conpet 在最新的更新中警告,泄露的数据可能会被用于诈骗活动。该公司建议受影响的个人要警惕来自电话、电子邮件或其他渠道的紧急请求，诈骗者常冒充知名机构员工，要求提供个人或财务信息以便实施欺诈。该公司提醒用户通过官方网站或已验证的社交媒体账户核实此类请求的合法性。

ShinyHunters 勒索团伙声称 Odido 数据泄露事件影响了数百万人

ShinyHunters 勒索团伙声称对荷兰电信公司 Odido 的网络攻击负责，并窃取了数百万用户的个人数据。Odido 是荷兰最大的电信公司之一，提供移动通信、宽带和电视服务。该公司在 2026 年 2 月 12 日披露了这次泄露事件，表示攻击者在 2 月 7 日通过侵入其客户联系系统获取了大量用户数据。暴露的个人信息包括全名、住址、城市、手机号码、客户编号、电子邮件、银行账户号码（IBAN）、出生日期，以及一些身份证明信息（如护照或驾驶证号和有效期）。

然而，Odido 强调此次泄露并未涉及用户密码、通话记录、位置数据、账单信息或身份证件扫描件。Odido 在发现泄漏后及时向荷兰数据保护局报告，并通过封锁攻击者的访问权限，以及聘请外部网络安全专家协助来应对该事件。

根据 ShinyHunters 的声明，他们窃取了近 2100 万个记录，其中包括 Odido 此前披露的敏感数据。ShinyHunters 还声称获取了 Odido

的内部公司数据和明文密码，但 Odido 对此予以否认，表示没有涉及密码或账单信息。ShinyHunters 进一步警告称，如果 Odido 不妥协，他们将公布更多数据并制造其他“麻烦”。

此次攻击与 ShinyHunters 近期的一系列网络安全事件相关，该团伙还声称对 Panera Bread、Betterment、SoundCloud、Canada Goose 等多家公司实施过攻击。值得注意的是，ShinyHunters 还采用了语音钓鱼（vishing）攻击，并通过滥用 OAuth 2.0 设备授权流程等方式入侵了多家企业的单点登录（SSO）系统。

黑客信息披露

本月收集到的黑客邮箱信息如下

spaceb.support@onionmail.org	thomasandersen70@onionmail.org	Vvvnet396@gmail.com
support_spaceb@mailum.com	openking995@gmail.com	Yason@mailum.com
ithelp01@securitymy.name	fancrylock@gmail.com	Yason@cyberfear.com
recovery@onionmail.org	Dalvinhoomer@tutamail.com	zhirtex@proton.me
controldata2026@outlook.com	GetYourData@onionmail.org	artchin9@aol.com
data771@cyberfear.com	boxforfox666@mailum.com	runandpay@outlook.com
data771@tuta.io	Recovery.System@onionmail.org	ShadowByt3S@proton.me
recovery-7dd1a2d343289d84@safe-mail.net	ourxmr@tutamail.com	fileparadise@cock.li
IONIAA@tutamail.com	HashTreep@waifu.club	outea2025@onionmail.org
Kevin_Denison_1983@protonmail.com	ransomclub@yahoo.com	yulkok@mailum.com
Sherry_R_Pearson@protonmail.com	cortizol@atomicmail.io	demetro9990@cock.li
moniro@tutamail.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）。

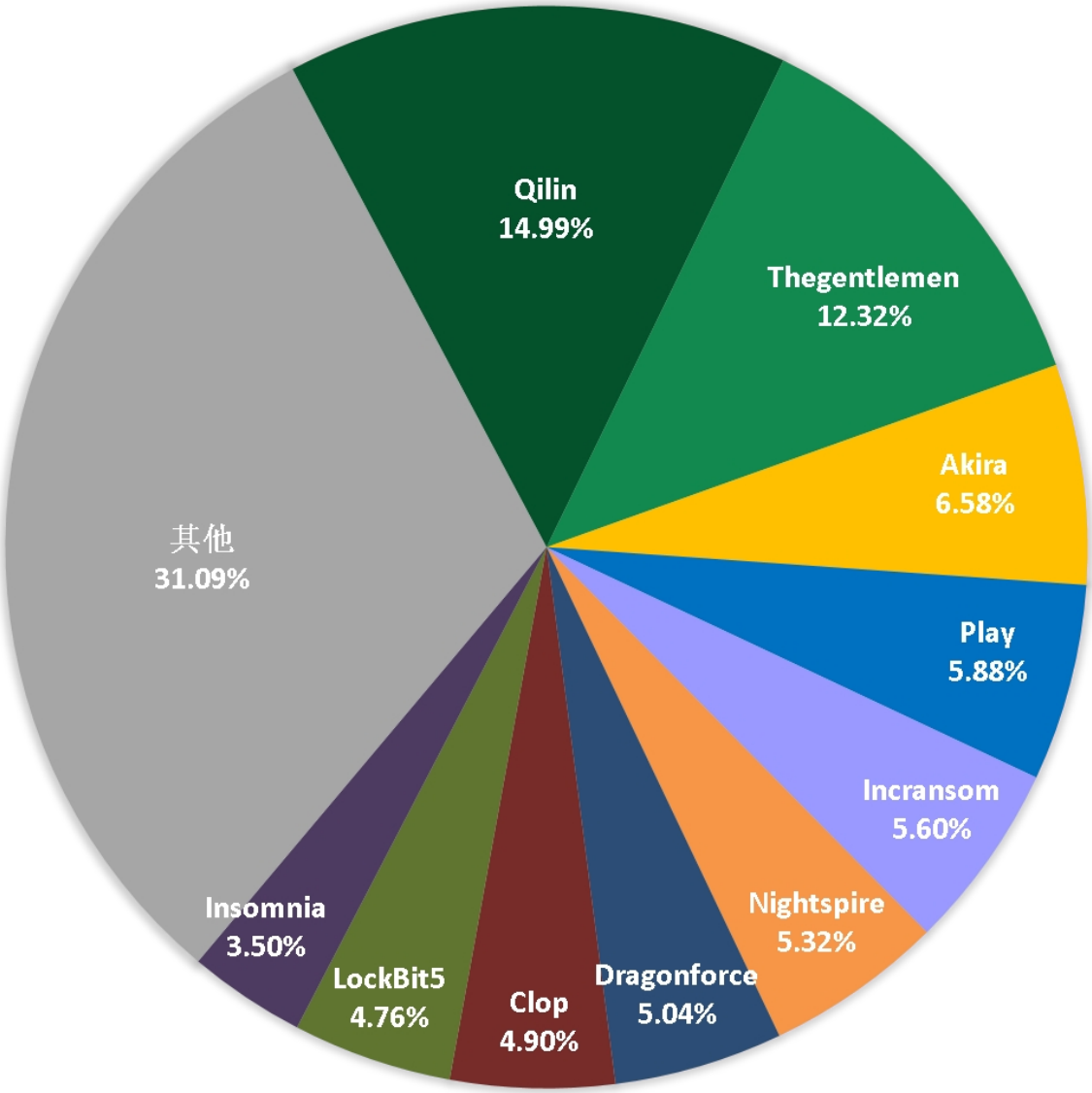

图 6. 2026 年 2 月通过数据泄露获利的勒索软件家族占比

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，做好数据已被泄漏

准备，采取补救措施。

本月总共有 714 个组织/企业遭遇双重勒索/多重勒索攻击，其中包含中国 17 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。

Schmuck Welt	Saltech Systems	AIGBUSINESS.COM
Unibros Shipping	Electriduct	HYDEPARKUMC.ORG
Pro-Plastics	Mayfair Hotels & Resorts	GIACARE.COM
North Andover Country Club	Marwood	GIASPACE.COM
https://www.pyramisgroup.com	Sika Technology	ONESUPPORT.COM
PriceTable	Paisley Products of Canada	HUDSONSUSTAINABLE.COM
hicare	Kirbor Homes	GOKALLIT.COM
GoHighLevel	Tropic Tool & Mold	CHEHARDY.COM
Whipflip	Arizona Lighting Sales	RBDCONSTRUCTION.COM
Aegis Project Controls	Indianapolis Car Exchange	BROADREACHRETAIL.COM
Skibiel Law	Oklahoma Auto Exchange	BE09.FR
J.R. Martin & Associates	Auto Auction of New England	The Sundher Group
jdaas	Spring Brook Country Club	Venesco
Casas del Mediterraneo	fivestates.com	Snyder Diamonds
keliweb	cepezed.nl	Halcyontek
UD Trucks	Kroll International	Milwaukee Forge
Rockwood Retirement Communities	Telecare	PCCA
Plaza Home Mortgage	TCPN Inc	Beasley & Gilkison
US.MAD DOG CONSTRUCTION	Fico Ferragens Indústria e Comércio Ltda	Smartply Europe
Two River Group Holdings LLC	RS Development LLC	Instituto Nacional de Derechos Humanos
Nations Financial Group Inc	Ausgewählt Vertriebs GmbH	UniFil
HEMIC - Hawaii Employers' Mutual Insurance Co	Kensington HPP	NFT Technology
Hrp Hitesh Cpa	MD Charts	Museu do Caramulo

Gemsen	Dinnebiergruppe.de	Agis Civil Engineering Construction
Grand Hotel	secure.ae	Fgf Colleges & Universities
Sejlstrup	Willow Construction	Texcomp
Thg	Graneles de Chile	PrintForm
Ching Feng Home Fashions	aircotedivoire.com	Junta Local de Conciliació n y Arbitraje
Fundao Para	Valgo SA	Grandview Family Medicine
Ace Ethanol	CCR Solutions	SMITHIPSERVICES.COM
Land and Lakes	University of Mannheim	PROACTIVEMEDICAL.COM
Straive	O.Berk	ITARCHITECHS.COM
Golden GBC	American Piping & Boiler Co	HUDSONEXECUTIVE.COM
Unisoft Communications	KFZ Sauter GmbH Co. KG	ANSTECHINC.COM
Neinver	A&A Global Industries	C4 (Carroll County Cannabis Co.
Accelerated Services	Cargo Largo	PT. Mitra Antar Tangguh
Triumph International	Elgon Cosmetic	Sanoviv Medical Institute
Com-Tec	AdMark Asia Group	Anabuki Kosan
American Beauty School	Application Solution Providers	moultriesheriff.com
Lymphedema Therapy Specialists	DeWalch Technologies, Inc	Pavlus Travel
Audexia group	Cedar Grove Warehouse	Core Supply
Law Offices Taenzer & Ettenson, P.C. (tesalaw.com)	femar.it	tuftco
Empresa de Transportes Via Pajuçara Ltda.	真言宗智山派 成就院	Barrett Financial Group
SURTECHINC	amtaar.com	Tech Environmental
Pathstone Family Office, LLC	First 4 Recruitment	iQ NetSolutions
Tract Consulting	Daniel L Kaler, DDS, PC	horizonmedia.com
Ripple Neuro	Diversified Supply Inc.	Body By Fisher
Landmark Rehab Group	IFL Group	Gradient Wind Engineering
BT Services	Adelphi	Augusta Housing Authority
Integrity Building	corahperu.org	Hospital Sao Jose do Avai (HSJA)
https://daricon.com/	Cheyenne & Arapaho Tribes	RPS Consulting
Zabun	Wilson Workflow Solutions	Putnam Precision, Inc.

Sando Tech	Midwest Wheel	Getly
ACFA	Saiful Bouquet	Rutherford Investment Company
Amata	mahidol.ac.th	KlearNow.AI
Universidade Federal de Sergipe	Stockton Cardiology Medical Group	San Diego Eye Bank
Evolutive Systems	Community Management Associates	rea Limpia
Alpha Consult	Robeck Fluid Power	Abel Schillinger
ntic.com	Fong Ilagan, LLP	granmanor.org
Physicians Clinic of Iowa	OfficeWorks	zeroenergy.com
Malaysia Airlines	Miller Johnson Jones Antonisse & White	poweron.com
Thrash Commercial Contractors	gbaco.com	castlestechemea.com
WE Fitness	powersmiller.com	abdata.com
APRO Asian Protection Pte Ltd	sodic.com	voyages-robin.com
JA AKITA KITA LIFE SERVICE, K.K	Almacenes Distribuidores de la Frontera	Municipio de Chihuahua
Carlo J. Martina, P.C.	Brm	atadler.com.sg
The Odom Firm	Castle Group	kres.cz
Salvatori Group of Companies	structuredassetservices.com	groupepiche.ca
thinlinetech.com	Wagner Metal Concept	Advanced Healthcare Professionals
milespartnership.com	Kymco	Integrated Fresh Solutions
Envirogen Technologies	Hiwassee Builder Supply	Gruel Mills Nims Pylman
Al Arif Contracting Co. (L.L.C)	farbank.com (flywatertravel)	Carlyle Senior Care of Florence
martec.it	Nebraska Health Imaging	Internal Medicine of Milford
Sus Insumos S.A.S	Orain.io	Rella Associates
Del Rey	PT Ikapharmindo Putramas	Flint Hills Dialysis
Zaner Group	Mold Tech	Southern Illinois Dermatology
Jones Haber	Efficy	Parts Life, Inc
The Siskiyou Telephone	Casartigiani	DeVal LCS
SATO	Darma Henwa	SchureMed
REDACTED	Sitran MG	Optimum Health Institute
Advanced Connection Corporation	Modoc Medical Center	Anatomic Clinical Laboratory Associates

OCEANIST ENGINEERING	Thames Valley Chamber of Commerce	Dunn and Dunn
UMSA	Williams Brothers Construction	Tri-Cities Gastroenterology
Boutique Harley-Davidson	Abbott Media Productions	Enviro-Hub Holdings
Silvestres	Yew Tree Dairy	Chiarottino
Nathalin Group	Marshall & Stevens	bardahl.com.mx
OFFICINE FRATELLI AMADORI snc	hh2home.com	latinoseguros.com.mx
Vera, spool. s.r.o.	faswealthpartners.com	autoservizilocatelli.it
Tricolor Holdings	Icat Food SpA	gruposelpe.com.br
Birmingham Museum of Art	Charm Diamond Centres	guarnera.com.br
primaria ungheni	Hagen Rosskopf	kenta.com.br
Symeta	adelphi.uk.com	grupoferrosider.com.br
Triumph Group	wiproferretto.com	Carlton Scale
Insight Hospital & Medical Center Chicago	iSMA CONTROLLI	De Gruyter Brill
Auvo	traceenv.com	ESS Metron
Grupo VerdeAzul	mapsweb.com	Ilderton Contracting
Was Madeiras	ACS Accountancy	Bloom's Bus Lines
Mutualista Imbabura	Ondine Biomedical	RAL Companies
EnerTec	OEC Bretagne	KaiserAir
ApexHospitals	Nang Kuang Pharmaceutical Co., Ltd.	Open Retail
MB Contabilidade	Branagh	AMR PEMCO
Pappytech	La Rioja Alta	MNKASSOCIATES.COM
A large bank in Asia	Comdat Datasystems	VIPPLLC.COM
Westwing Home & Living	CROSS JEANS Zakrt	TRJLTD.CO.UK
Ruamjai	BITS	STRATEGICOBJECTIVES.COM
MUST Informatique	Intsika Yethu Municipality Government	IDEALWELDERS.COM
OKJ Group	Global Group	CROWDEDISLAND.COM
Smartbytes	Copamarina Beach Resort	DUKOSI.COM
Industrias Iberia	Oceania Gas Chemicals & Related Products	CONWEST.COM
El IBR	Bigso	NGATTORNEYS.COM

Dos	Bitgo	LABINF.IT
Global Trust Advisors	Adirondack Networks	Atlas Air
Wachendorff	A.T.I di Zuinisi srl	CPQ Ingenieros
Hudson Awning	PERLITE, S.L.U	Hafa
Middlesex Transporters	S.Y.L Pastilhas e Sapatas de Freios	Novetex Textiles
Sungwoo Co., Ltd	Abrahamsom Center	Wells Fargo
SAIC Motor Corporation	Master Handlers	L'Aeroclub
AJU Pharm Co., Ltd	RIECO Industries Limited	Accountnet
Microforum	Makimura Co., Ltd.	Associated Endocrinologists
CognitiveTPG	UniTurn Kft.	Parente Fireworks
Huber	Northeast Pharmacy Service	Infinite Tiers Group
Dalet	MESA Products	Silvi SRL
Aptean	cs.at	Marina Home Interiors
Westiform Germany	hanover-ma.gov	Nishiyama Seisakusho
Nebraska Hearing	sands.mu	BAM - Brand Art Media
Regal Building Materials Ltd.	cmcconstruct.com	Gady Family
Employer Solutions Group	renovagy.com	Dome Partners
University of Pennsylvania	aeromedsocaustralasia.org	Chonburi Provincial Administration
Harvard University	isesa.cl	Torus
Figure Technology Solutions, Inc.	sosltda.com	PLUS Malaysia Berhad
Canada Goose	sevenstarsgracebay.com	EXIM Bank
CarGurus, Inc.	JC Resorts	Ankara-İzmir
Mercer Advisors	Buff Law	Trace
Beacon Pointe Advisors	Robbins Parking Service Ltd	Far East
Odido NL & Ben.nl	MAIRIE DE FUMEL	TriPartum
suffolkva.us	SPIR STAR Asia	Logility
Induherzig SAS	Shining Labels	Peerson Audio
PoindexterHill	Yem Chio Co	TMPartner
Envelex Thailand	Betesan	Advent Aircraft Systems, Inc.
Jac Vandenberg	Copier Careers	Esposito Bros. Construction Ltd

Silver Lake Medical Center	The Syverson Group	La Fabrica
acwapower.com \ https://www.larsentoubro.com/	Archaeological Institute of America	Heavy Motions Inc
Orrick, Herrington & Sutcliffe	CHASI (A part of Sun River Health)	Penn Fencing
Rocky Mountain Care	Heartland Title Services	Leading Edge Speciali
Rivages Du Monde	UCG Associates	https://www.platinumdrywall.com/
Zelenkofske Axelrod	Unified Engineering	Wayco Inc
Spire Payments	HMA	Exco
GENERON	Lusamerica Foods	InfoMontreal
Accuick	White Beach Hotel	Western Slope Iron & Supply
TWU Local 100	Futue Bath	Reilly Foam Corp
Plan-IT Office Solutions	LSA International	Yulkok Ltd
FAMILY EYECARE LLC	Gruppo Avanti	Farsound Aviation
The City of Cocoa	Carrera Casting	United Hospital Supply
primepak.com	Ardene Holdings	LumioDental
Zip24 - ShipOx	Michael L Larson	Perpetuuiti
FindNear	Yash Highvoltage Insulators Pvt	University of Applied Sciences,Worms
tektreeinc.com	City of New Castle	Conpet S.A. (COTE.RO)
hiringsteps.com	Nile Air Information	AOT Japan
Biaodianyun Group Ltd	Smart Glass	brooklyn group
Rohner	The Marena Group	megasilver.com.tw
Rainier Clinical Research Center	Elite Screens Inc.	ISTS
Atlantic Design Engineers	Siem Srl	CBH Homes
Faulkner+Locke	Samkwang	Woodfield
Hendrick Construction	Autostrad Rent a Car	Ashby Computers
Young & Associates Consulting Engineers	Empire Express	Richey Tax Solutions
PenLink	Yelete Group Inc	Karl Geuther
Gulfstream Services	Seagrass Boutique Hospitality Group	Royal Wine Corp
Chemical Computing Group	Halcyon Technologies	efulfillment Service
AllChem Industries	Emirates National Group	D'Onofrio General Contractors

Cumberland International Trucks	Mep Technologies	www.trisa.ch
North Woodlands Medical Centre	Midwestern Oil & Gas	Thin Red Line
Okanogan County Vets	rswater.ae	MB Distribution
Tactis	Pathway Reads and Data Analysis	RENAFAN
Maintenance & Project Engineering	A1 Capital	Ch è vre & Rutsch & Herren Notariatsb ü ro
Complete Thermal Svc	Stanley Autenrieth Auction Group	ChainPower Technology
CYMOT	Phoenix Art Museum	JOSE COMBALIA SA
US Trading	lohmann-tapes.com	Lakeside Union School District
True Value	Anchor Computer Systems	RC Collecting
Pollo Cibao	Derbez	GC Dental
Sasin Colleges & Universities	Campbell Rappold & Yurasits	Crystal Coast Pain Management
Line Up Korea	Conectados Chile S.A.	Interplan
Seac	Sakata Seed America	peterboroughpublichealth.ca
Qingtian Express Co.	Ducasse Comercial Ltda	Western New York Energy
Garuda Indonesia Airlines	Segue Manufacturing Services	Forella Group
Grupo Progresso	auxhomeservices.com	PTI
Sawafi	atchadwick.net	Drake Precision Dental Laboratory
HUGS Insurance	excavationtourigny.ca	Medasa
Perfumeria Pigmento	Atlantic Refinishing & Restoration	Travelmarket
Bluefish Dental & Orthodontics	Law Office of COX & SANCHEZ	Law Offices of Thomas J Skinner, IV
Grupo Tomza	Andringa Law	Rosenblum Schwartz &Fry
WTSmedia	WCT Holdings Berhad	Balloons Everywhere
Esperance Metaland	Erg Otoyol	South Hays Fire Department
onlinedivorcetexas.com	Thammasat University	Comune di Battipaglia
Micaforce Technology	Ghana Bauxite Energy, Utilities & Waste	Blystone & Bailey
LaBaguette	Clark Foam Products	H-Behbehani Brothers WLL
fcc-inc.com	www.hfplanners.com	ENCOMPASS-INC
vilati.com	R.J. Zavoral & Sons, Inc.	Family Health Center
utc.com.kw	Altak	Muebles Dico

mengseng.com	Catalanatto & Barnes	Erickson Thorpe & Swainston
maxusacorp.com	Makivik	Medinah School District 11
lasevillanita.com	On-Point Defense Technologies	ChokChey Finance
dmxm.com	COIT	JST Power Equipment
yfynqygs.com	Northbridge	www.pucobre.cl
czkingdee.com	Tsunami Tsolutions	KOUEI
humsnlr.com	Aviam Corporate Housing	Elabs
crystalcoastpm.com	Topkin & Partlow	Exterior Worlds
xpressnebs.com	Tower Insurance Services	Workers Health & Safety Centre
wjnklaw.com	Andringa Law	Range Cooperatives
smilescare.com	Cox & Sanchez	The Hechtman Group
moa.gov.eg	falconmgt.com	Kilograph
associated.org	Hood River Dental	Zurflüh-Feller
wilhelmsen.com	WVPCA	Ferretti Construction
davila.cl	SPEC	Jcm Agricola
Altalingua	FUSION HILL	INGUS
Colonial Van Lines	John O's Foods	Sprokkit
RTC	jasper-avocats.com	Stephenson Ziegenhorn & Bernard
Aramsco	[Redacted]	Best Attorneys
Madison Services, Inc.	Lindenhurst Fire Department	Polycom
Stera Chemicals	Mississippi Market	Iron Mountain
The Cherokee Group	Castles Technology UK & Ireland	Shinwa Co Ltd
McFarlane Agencies	Mt Barker Co-Operative	Hosowaka Micron Group
Fabcon	BCS ProSoft	T & M Electric LLC
polymedicure.com	DAD.CO.TH	Deatak
Pearl Institute for Clinical Research LLC	THEMORTGAGEFIRM.COM	Stellium
www.shora.ma	FISHWINDOWCLEANING.COM	Acu Trans Solutions LLC
ABAR S.p.A.	SOLUTIONSINSAFETY.COM	SIGMA Processing Group
Gentegra	BOYDEN.COM	Foamtec International

Graymatter	CFDT.FR	Odyssey Academy
Iblesoft	SPOHNASSOCIATES.COM	Mullinax Ford
The Corradino Group	GARNERGROUP.NET	SoCal ROC
THEPERPETUAL.COM	Hawk Law Group	

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 7、Windows 10 以及 Windows Server 2016。

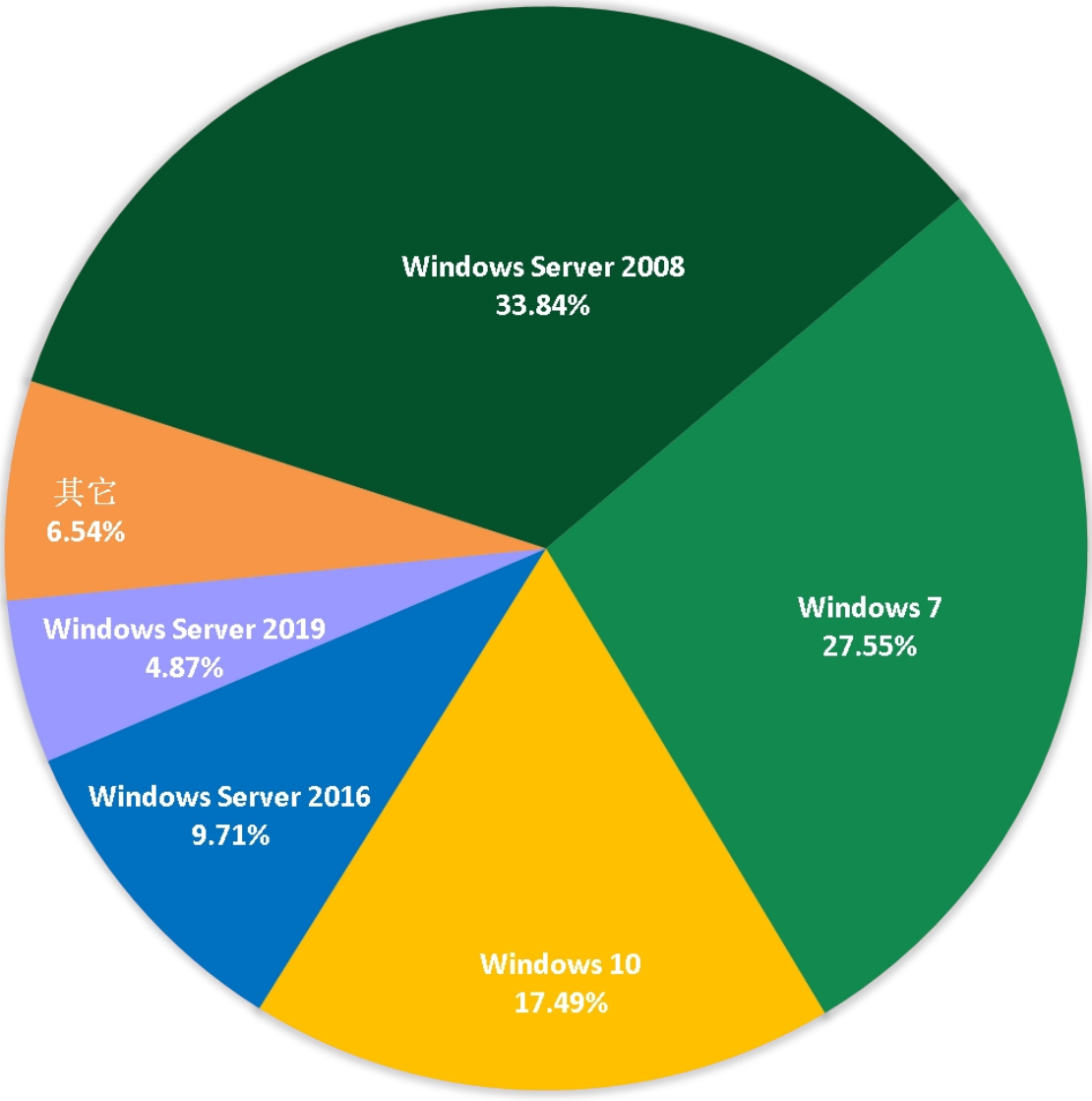

图 7. 2026 年 2 月受攻击系统占比

对 2026 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。

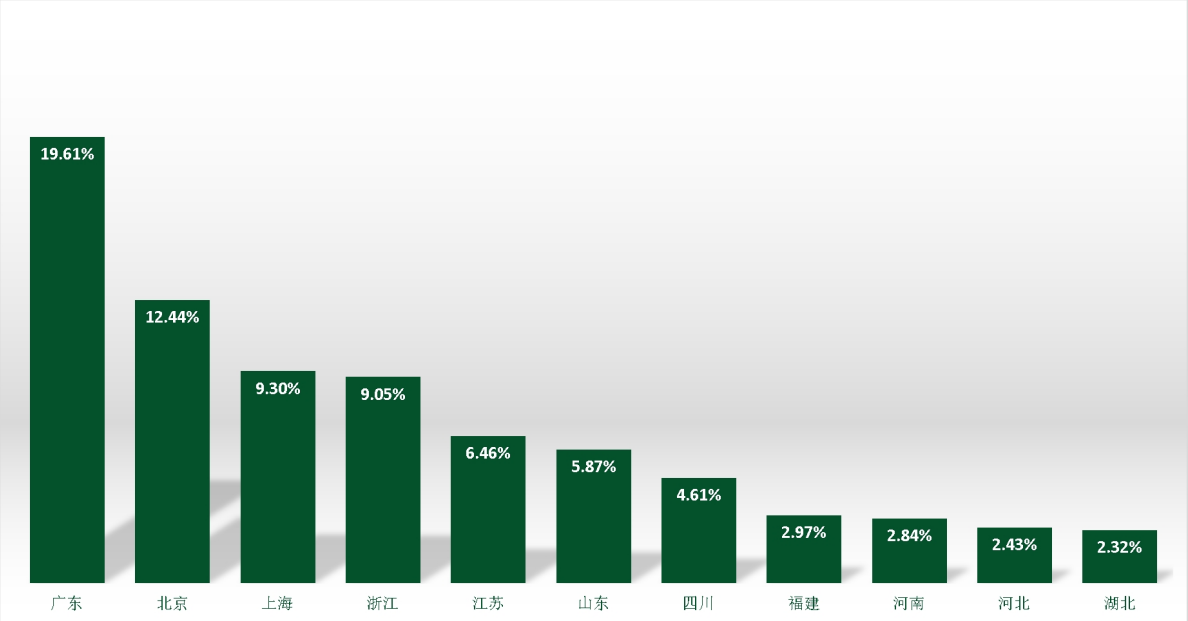

图 8. 2026 年 2 月国内受攻击地区占比排名

通过观察2026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。

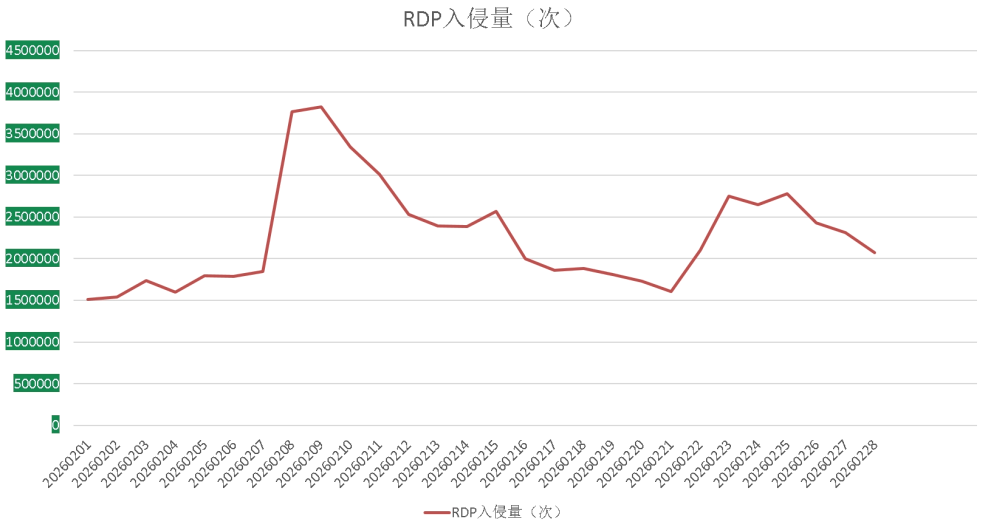

图 9. 2026 年 2 月监控到的 RDP 入侵量

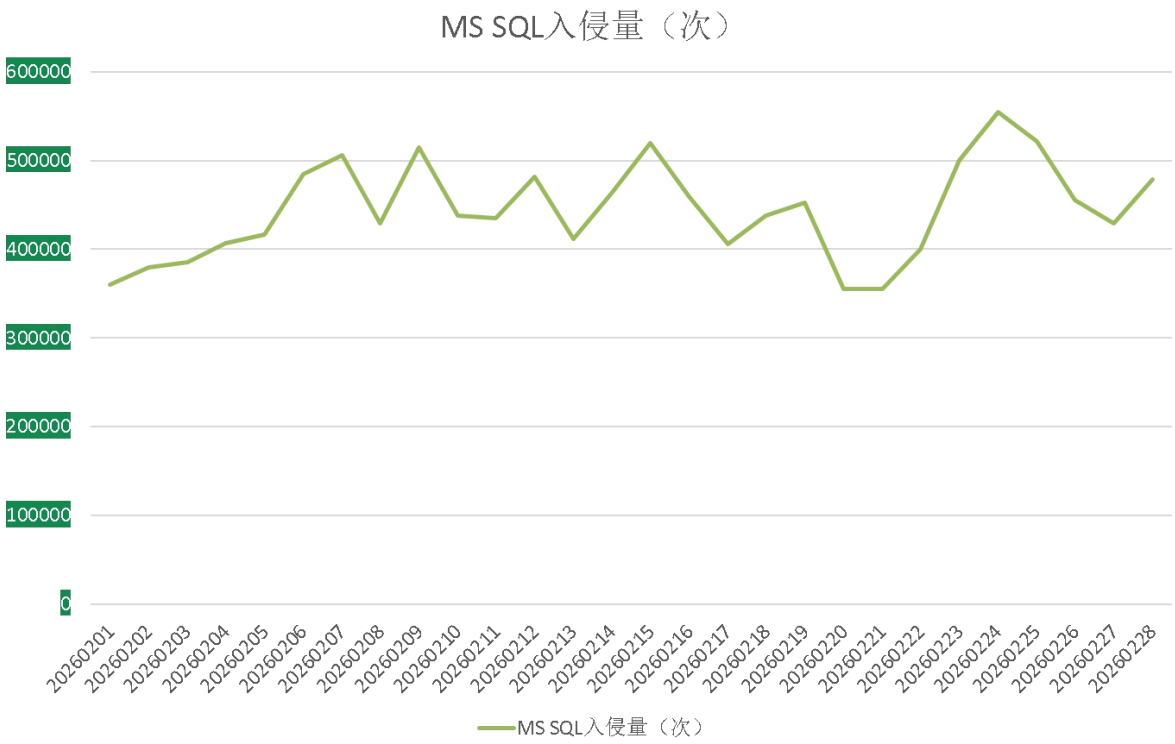

图 10. 2026 年 2 月监控到的 MS SQL 入侵量

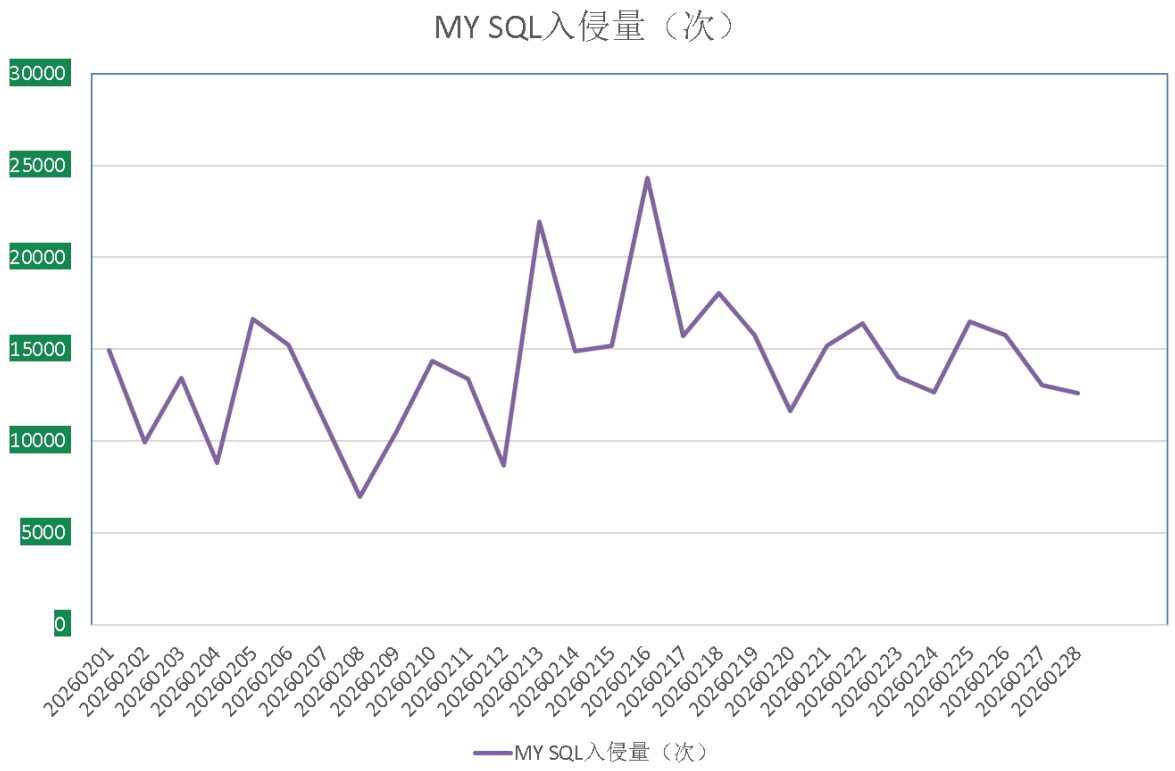

图 11. 2026 年 2 月监控到的 MYSQL 入侵量

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。

- ✧ 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。

- ✧ 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。

- ✧ 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。

- ✧ ink：无明确家族归属，需待后续有效反馈再进行研判。

- ✧ 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与数据库口令，成功后手动投毒。

- ✧ baxia：同 bixi。

✧ 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。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，后来增加了漏洞利用的传播方式。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。

✧ mallox：同 devicdata。

✧ xor：无明确家族归属，通常在一些验证类勒索测试中出现。

✧ mtullo：新增勒索家族或变种，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。

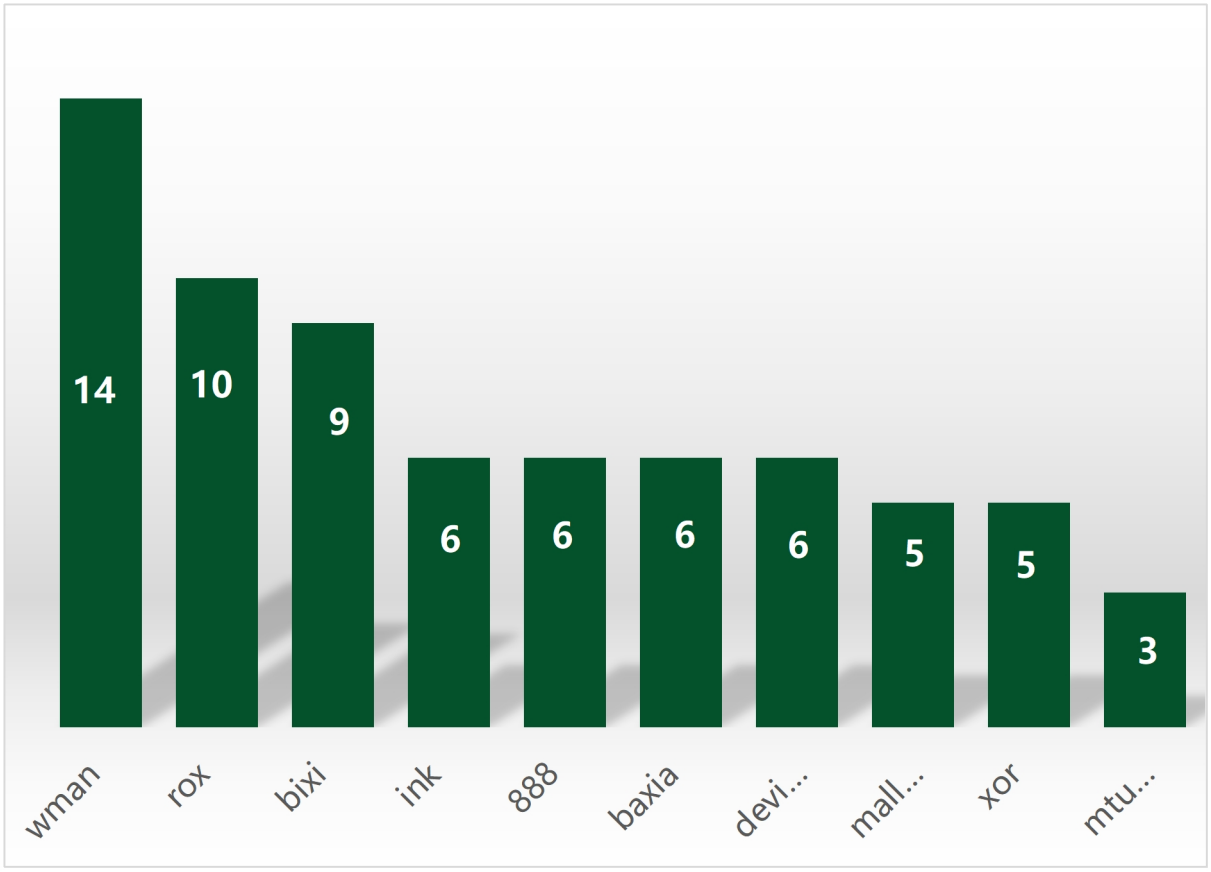

图 12. 2026 年 2 月反病毒搜索引擎关键词搜索排名

解密大师

从解密大师本月解密数据看，解密量最大的是 Phobos，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。

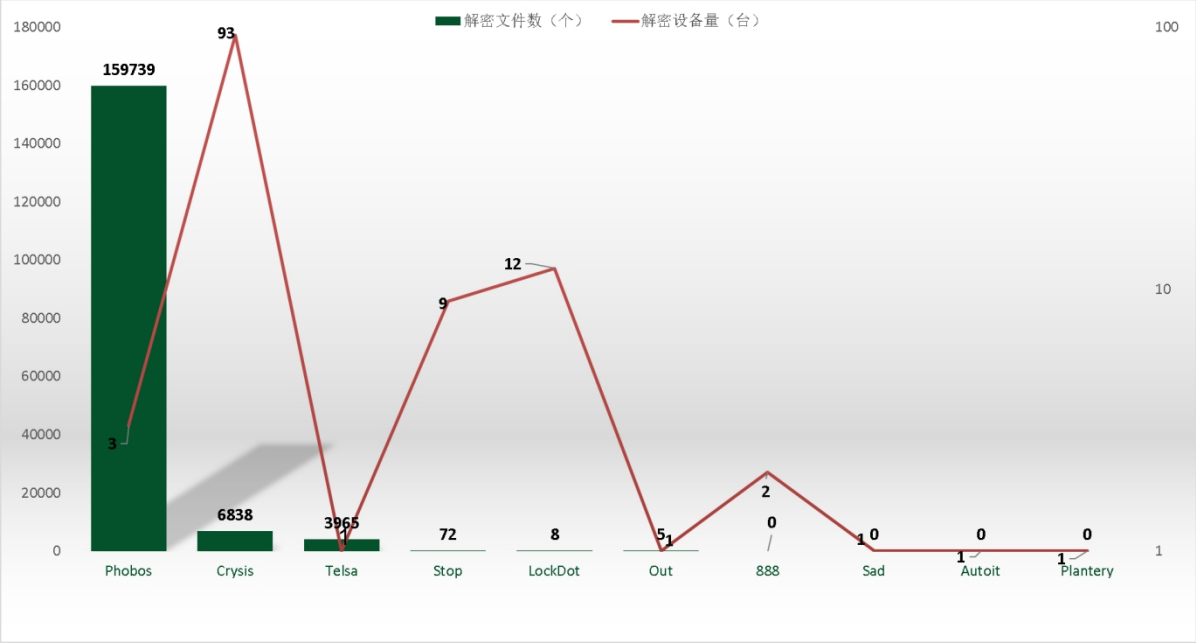

图 13. 2026 年 2 月解密大师解密文件数及设备数排名