

2026 年 1 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，为需要帮助用户提供 360 反勒索服务。

2026 年 1 月，全球新增的双重勒索软件有 BravoX、ClearWater、Vect、GreenBlood 家族，传统勒索软件家族新增 Milkyway、RahidsLocker、GrandMonty、PurpleCryptor 等多个家族。

本月在国内持续热门的勒索家族 Weaxor 家族新增了一个分支变种，主流加密后缀变更为.xr，攻击方式依旧是利用 Web 漏洞发起攻击并通过注入系统进程轮询加载漏洞驱动，与安全软件做内核对抗。

本月出现了一个名为 OAPT 的勒索软件组织，但实际上是一个诈骗团伙。该组织利用 AI 生成的虚假受害公司对外发布信息，并夹杂少量真实的受害公司，以制造看似真实的假象。目前该组织开始招募所谓的“黑帽黑客”，但其真实目的并不是组织勒索攻击，而是诈骗并窃取被招募者的比特币。此案例佐证了一个长期存在的现实：网络诈骗攻击不只面向普通民众，同样广泛针对安全分析人员、黑产从业者、IT 管理员等传统意义上的所谓的技术认知强的目标群体。

以下是本月值得关注的部分热点：

- ① LockBit 变种两度利用僵尸网络下发
- ② MiddCrypto 勒索软件利用国内全实名平台链路进行投毒
- ③ Nike 在勒索团伙公布文件后调查数据泄露事件

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，并长期致力于服务来自全网的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装安全软件的占比达到 70%，而未正常启用 360 安全软件的设备数量则占比 12%，安装了其他安全软件的设备则占比 18%。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。

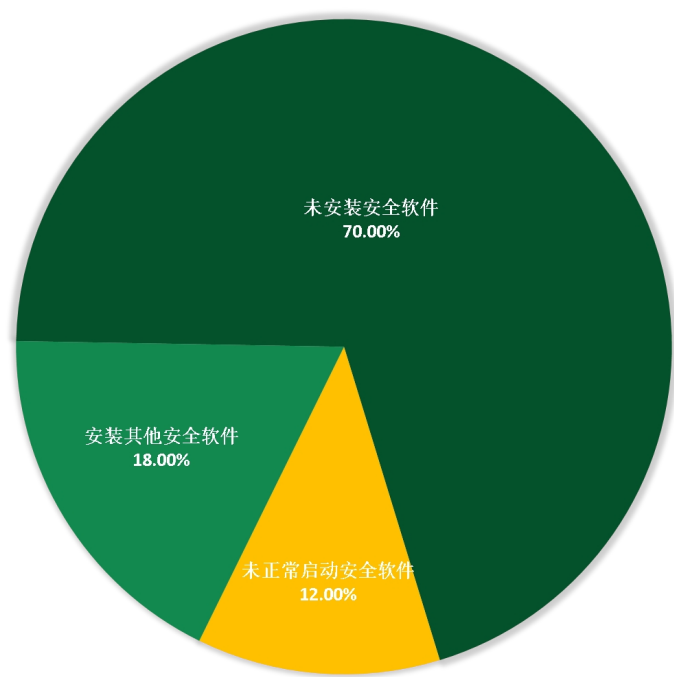


图 1. 2026 年 1 月勒索软件中招设备中安装的安全软件占比

感染数据分析

针对本月勒索软件受害者设备中所感染病毒家族进行统计：Weaxor 家族占比 38.55%居首位，第二的是 LockBit 占比 21.69%，Wmansvcs 家族以 16.47%占比位居第三。

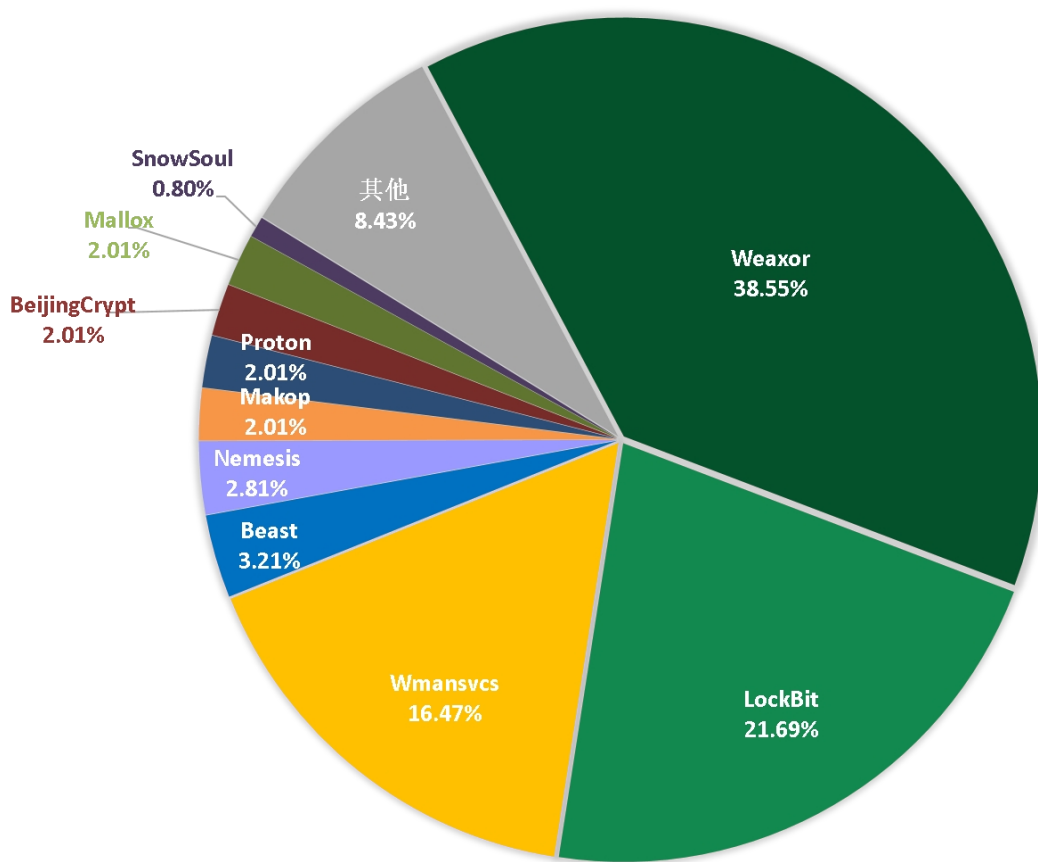


图 2. 2026 年 1 月勒索软件家族占比

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 11 以及 Windows Server 2012。

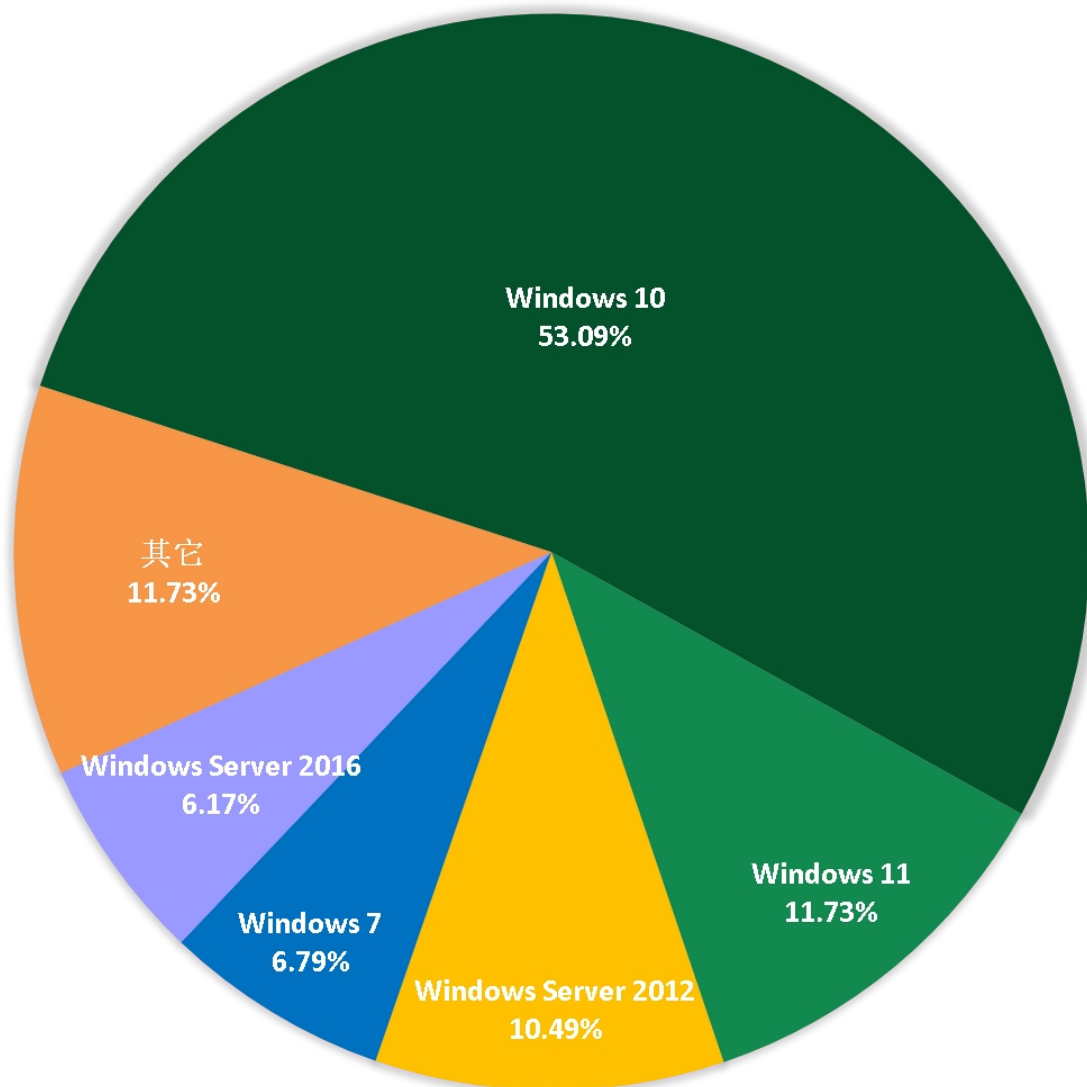


图 3. 2026 年 1 月勒索软件入侵操作系统占比

2026 年 1 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 平台攻击行为有所增加。

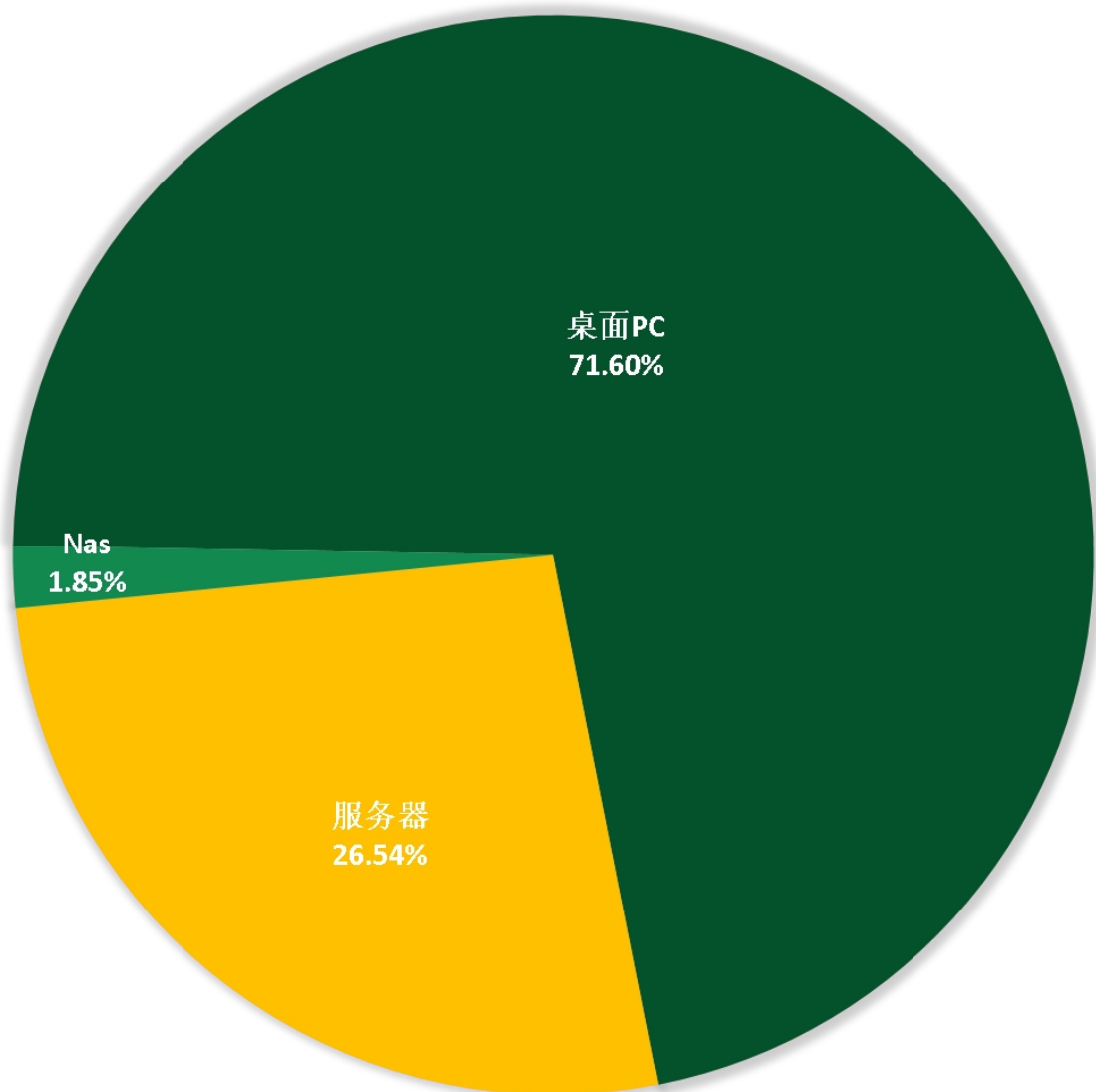


图 4. 2026 年 1 月勒索软件入侵操作系统类型占比

勒索软件热点事件

LockBit 变种两度利用僵尸网络下发

360 反勒索服务在 1 月 5 日与 1 月 23 日分别接到数十例 LockBit 家族变种感染的集中反馈, 在一些社交媒体平台也会看到同期 LockBit 家族相关的受害案例。经 360 溯源分析确认相关 LockBit 变种是通过先前感染过的僵尸网络渠道进行的联网下发, 感染设备均无 360 防护。受害者包括企业与个人用户, 相关僵尸网络具备内网渗透能力, 一经发现需全员杀毒加固。



	时间	行为	简介
远程桌面登录	2025-11-20 10:07:27	关闭windows防火墙	关闭Windows防火墙可以减少网络流...
其它登录	2025-11-18 22:39:43	关闭windows防火墙	关闭Windows防火墙可以减少网络流...
系统日志	2025-11-18 10:12:30	关闭windows防火墙	关闭Windows防火墙可以减少网络流...
远程桌面登录	2025-11-17 13:58:43	关闭windows防火墙	关闭Windows防火墙可以减少网络流...
数据库登录	2026-01-05 20:59:31	MySQL相关服务异常退出	渗透攻击中结束MySQL服务进程会导...
SMB共享登录	2025-12-29 02:13:28	虚拟内存不足	虚拟内存不足通常是由于处理大型数据...
痕迹清理记录	2025-09-08 11:59:00	感染僵尸网络	感染僵尸网络会将受害设备变为黑产 “...
渗透痕迹记录	2024-06-07 04:46:02	清除即插即用设备日志	感染僵尸网络会将受害设备变为黑产“肉鸡”，平时潜伏在系统中不定期根据金主需求投放远控、勒索、窃密、挖矿等恶意程序。
文件共享检查	2024-06-07 04:45:41	清除Setup日志	清除Setup日志可以掩盖攻击者通过系...
下载记录日志	2024-06-07 04:45:41	清除应用日志	清除应用日志在渗透攻击中的作用是隐...
近期攻击日志	2024-06-07 04:45:41	清除系统日志	清除系统日志在渗透攻击中的作用是隐...

图 5. 360 渗透痕迹记录功能发现并拦截僵尸网络感染行为

在 1 月 23 日 LockBit 变种版本的勒索赎金要求降低为 300 美元,

相比 1 月 5 日那一批 500 美元的赎金降低了 40%。根据前一批 500 美元赎金的受害者反馈，第三方赎金中介打着解密或数据恢复幌子收取的成交金额是 3700 人民币。预计本批次的第三方中介的赎金费用在 2300 左右。由于受害金额无法立案，进一步杜绝了受害者尝试报警的可能性。

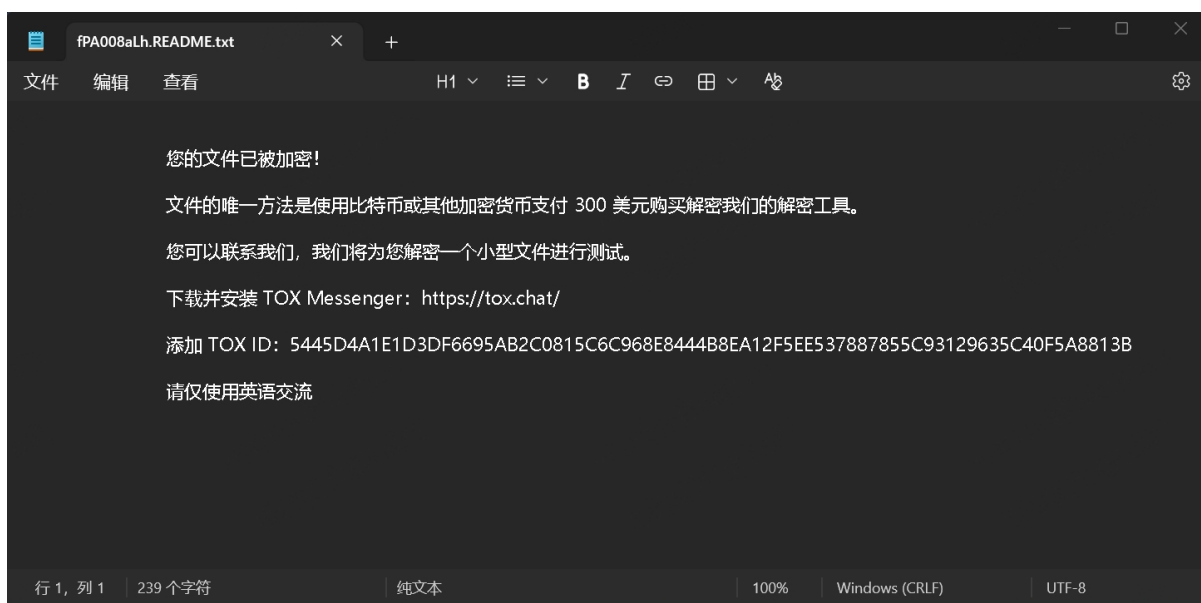


图 6. Lockbit 勒索信息

MiddCrypto 勒索软件利用国内全实名平台链路进行勒索投毒

本月 360 率先独家解密了通过激活工具与破解软件进行钓鱼传播的 MiddCrypto 勒索软件，其利用备案网站、博客园、51cto、百度网盘等渠道进行传播，同时利用微信与支付宝进行勒索变现。此勒索软件在受害用户设备上会上传数据识别用户画像，进行特定后缀的加密以及支付赎金的云控调整。

360 第一时间进行了勒索代码的分析与数据解密，并将分析与解

密结论形成了分析报告，报告详细内容可参见如下链接：

<https://news.safe.360.cn/n/12876.html>

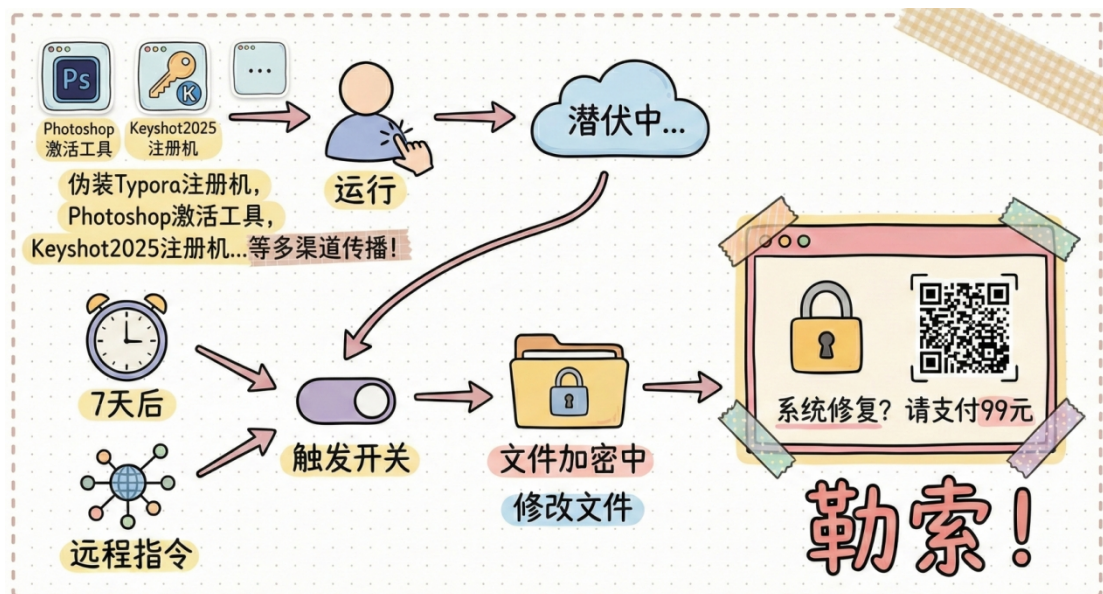


图 7. MiddCrypto 勒索软件感染流程示意图

Nike 在勒索团伙公布文件后调查数据泄露事件

Nike 正在调查一起其所称的“潜在网络安全事件”。此前，勒索与数据敲诈组织 World Leaks 在其暗网泄露网站上发布信息，声称从这家运动服饰巨头窃取了约 1.4TB 数据、近 19 万份文件，内容涉及 Nike 的企业内部资料和业务运营信息。Nike 在回应媒体时表示，公司一贯高度重视消费者隐私和数据安全，目前正对事件展开调查并评估影响，但尚未证实数据被盗或泄露的真实性。

值得注意的是，在相关报道发布前，World Leaks 已将 Nike 从其泄露名单中移除。这一举动被外界解读为双方可能正在谈判，或 Nike

已支付赎金以换取数据下架。不过，Nike 并未就此作出确认，媒体也无法独立验证所谓泄露文件是否真实有效。

World Leaks 被认为是勒索软件组织 Hunters International 的“重塑版本”。Hunters International 于 2023 年末出现，曾因代码相似性被怀疑与 Hive 勒索软件有关。该组织在 2025 年 1 月转向“仅数据窃取与敲诈”的攻击模式，放弃文件加密，原因是认为传统勒索攻击风险过高、收益下降。Hunters International 曾声称对 280 多起攻击负责，受害者包括美国法警局、塔塔科技、日本豪雅（Hoya）、AutoCanada 以及美国海军承包商 Austal USA 等。

此外，自 World Leaks 活跃以来，其泄露网站已公布了全球数十家机构的数据。其关联人员还被指与戴尔某产品演示平台被入侵事件有关，并利用已停止支持的 SonicWall SMA 100 设备植入自定义 OVER STEP RootKit 恶意软件。

黑客信息披露

本月收集到的黑客邮箱信息如下

cybersupport@protonmail.com	gimkoumo@outlook.com	decrypt_ruppur@outlook.com
cris_nickson@libertymail.net	support@amexmail.top	mrunlock494@gmail.com
decryption@mailum.com	support2@aminyx.com	Kingvps@cyberfear.com
dawsones@proton.me	support3@fastemailo.com	Kingvps1@cyberfear.com
EncodeMan@qq.com	ithelp@citytar.com	getsecurity@mailum.com
EncodeMan@protonmail.com	ithelp2@crefree.com	getsecurity@onionmail.org
EncodeMan@tutanota.com	avastdata@airmail.cc	Descrypter.pay@onemail.com
decrypthelp@qq.com	georgeair@tuta.com	MR. JUQ@MAIL. RU
decrypthelp2@qq.com	jionkate@tuta.com	BlackHatCyber789@gmail.com
generalchin@countermail.com	stephaniekifujo@web.de	blackhatcyber789@gmail.com
generalchin@smime.ninja	janinabosara@web.de	1eljicok@gmail.com
cryptonationusa@protonmail.com	susannelubofa@web.de	Hacker@mail.ru
bitanos@cock.li	grossland@mailum.com	mojxji@gmail.com
ioniaa@tutamail.com	snowsoul@mail2tor.co	GARCIA@PROTOEMAIL.COM
taskt001@tutamail.com	Henrylarkins1977@onionmail.org	gydrockfasl@tutamail.com
systemofadown@cyberfear.com	Andykameron1975@tutanota.com	thegreenblood@proton.me
systemofadown1331@onionmail.com	saymonlouis1967@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）。

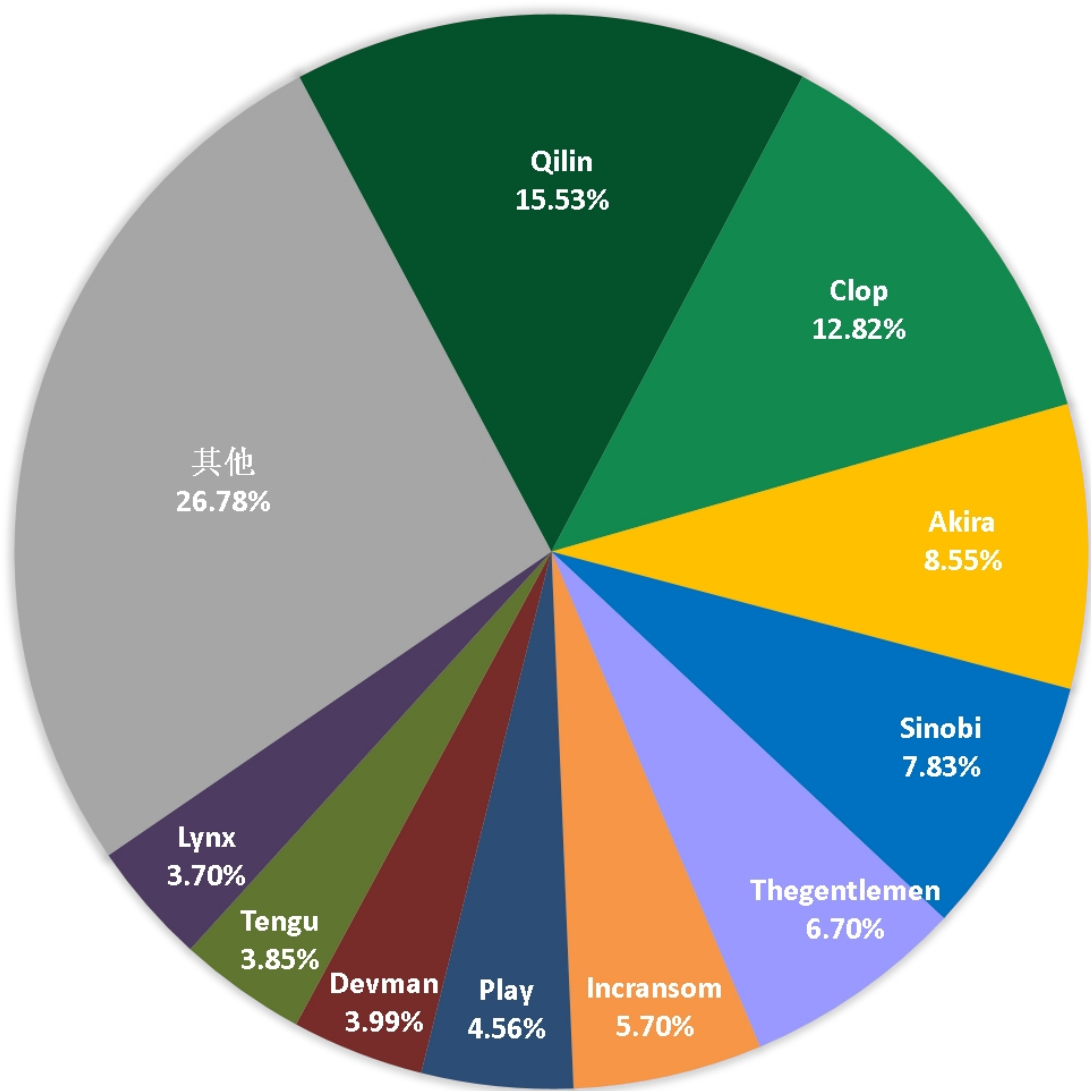


图 8. 2026 年 1 月通过数据泄露获利的勒索软件家族占比

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，做好数据已被泄露准备，采取补救措施。

本月总共有 702 个组织/企业遭遇双重勒索/多重勒索攻击，其中

包含中国 18 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 24 个组织/企业未被标明，因此不在以下表格中。

Handsome Manufacturing	MRC Prion Unit and Institute of Prion Diseases	Tepco-Group
Nobel Hygiene Pvt	hansemerkurintl.com	Perdana Petroleum Berhad
Bar S Services	advancedcoolingtech.us	Chemsain Konsultant Sdn Bhd
NAI Plotkin	Milott Laboratories	Bulk Handling Systems Companies
Transaction Packing	YCC Parts Mfg	Itasca Consulting Group
Hallauer Law Firm	JA Riollano	Richard Alibon Primary School
Neuviz	IGI Global	Ideal International
CigamSoftware	Aschwanden & Partner	Collett Hulance
Pellenc	Propane Levac Inc.	Dubai Air Wing
Dolby Laboratories	Uinta Bank	gbmme.com
Wieson Technologies	ECA-USA.COM	Commercial Paving Ltd.
Beacon Mutual Insurance	WARRANTYFIRST.CO.UK	stimgroup
Lawsoft	TOMLLAWYERS.COM	Rodney's Sign Company
Hydrometrics	INTEGROY.COM	Fit-Line Global
Röben Tonbaustoffe GmbH	ITROBOTICS.COM	Cape Fear Country Club
Abatix	MONTALBAARCHITECTS.COM	Pilot automotive
woodwardoralsurgery.com	EASTPLATS.COM	MyVete
We will be back soon	AERIFY.IO	Eco Green Group
FluidOne	BAQUS.CO.UK	Harrison Design
wjnklaw.com	SMITHDALIA.COM	Resource Corporation of America
casamedica.com.gt	ELKAIR.COM	Young Wealth Management
AUGUSTEA.COM	Nike, Inc.	klhindustries.com
MEDIAWORLD.COM.HK	Proleasing	G-WAY Microwave
WARDHAVENCAPITAL.COM	EDF Group	Superior Water Conditioning
LONGHORNORGANICS.COM	SiNetCon	pronaca.com
DCSNORWAY.COM	Farmacias Vilela	consigaz.com.br

SHACKELFORD.LAW	Ocean Fish	sealbeachca.gov
SERVE-CLOUD.COM	Copetrol	sealbeachpd.com
MARK-FINN.CO.UK	Radial Engineering	Best Insurance Agency
EMEG.CO.UK	Universal Builders Supply	Hayden Safe & Lock
LOGICALMICRO.COM	Van Eycken	Depth
HODERO HOLDINGS LTD	Spiros Industries	The Outdoor Recreation Group
Fulcrum Construction	Service Lane eAdvisor	Brockhaus
Littlefield Companies	OnSight	Rod Danielson
Rich Sport Public	CE Electronics	Syrstone
MBC	Cemtech	CSS Services
Cooperativa de Hostelería de Navarra	Midway Windows and Doors	Epport Richman & Robbins
Trace	Bayside Dental	www.charoenchai.com
Esperance Communications	Asian Heart Institute	InvivoGen HK
Bryant Consultants	MODERNISTIC GARDEN & PET SUPPLY LTD	Alpha Alternatives
Northeast IndustrialManufacturing	ShuBee	FOX Architects
compensatii.gov.md	Mutest	Cardiovascular Medical Group of Southern California
Rocky Mountain Associated Physicians	Centro de Desarrollo Emprendedor Ensenada	Ingomar Church
Atlantic National Trust	Mettler Partner	ITG Electronics
shorelinenyc.com	Clipper Petroleum	Granville Inn
www.roschvisionary.com	Serometrix LLC	Revoil
Tulsa International Airport	Orthopaedic Specialists of Massachusetts	Real Tech
PK PINHÃO & KOIFFMAN ATTORNEYS AT LAW	KOROLFINANCIAL.COM	Dsm Information Technology Trade Ltd.
DIEHL & CELLA ADVOGADOS ASSOCIADOS	TRUSTPAYMENTS.COM	Pos Bilişim Teknolojileri
Ruskin College	BRINKS.CO.NZ	Pecan Tree Dental
NGC Software	MCMATHLAW.COM	Youngstown Pipe & Steel
Crosslists Data	WORKFORCESOFTWARE.COM	Vernon Sales
Bantry Bespoke Joinery,	KCDWORLDWIDE.COM	Dekoyap

Murnane & O'Shea		
anomatic.com	ONYXEQUITIES.COM	Warka Bank for Investment and Finance
Urban Edge Architecture	Jet-care International	Hog Slat
iGlobal Services, Medenet	aditusbr.com	DTI Foreign Trade Service Corps
Easypak	us-duct.com	Pensam Residential
BrandingBusiness	gob.mx	Sarl Alliance
Moontown	frandent.it	San Silvestre School
Keil Erdbau	BUREAUX.FR	Novelty Technology Care Espana
b2motorsport.co.il	INTEGRITEK.NET	Advanced Family Surgery Center
Melton Machine & Control	CENTAURPRODUCTS.COM	Cisneros group
MG Oil	automax.com	CleverPower
Hillmann Consulting	Syrmasgs	Trend Import Export
MACT Health Board	www.mims.com	Thai Petroleum & Trading
SUNSETWORLDRESORTS	www.saundersandsaunders.com	STC Concrete Product
Community Property Management	Yource Bulgaria & Greece	REDtone
consultaegis.com	Bluemega	Launie & Marino
zallc.org	Sibca	Denny's 5th Avenue Bakery
RAKS Sp. z o.o.	Garko	WiZiX Technology Group
Clatronic International	Casa de España	Virginia Records
Pacific Airlines	Sincere Corporation	Nissan Motor Corporation
Warren County Sheriff's Office	Unimed Anápolis	Bouygues Energies & Services
NVHG.COM	NSSF	Foshee Architecture
WHEELLOCKST.COM	SASI JSC	publicsafety.ohio.gov
DESKTOPG.COM	Autofinanciera	CompactInd
CMHHELI.COM	CPF Financial Services	American Vanguard
COWANS.ORG	Orlík Compressors	Bauerfeind
HTHELI.COM	USTAR	Mohammad Omar Bin Haider Holding Group
GRANITEPOINTE.CA	Magen Eco Energy	Swavelle Group, Wearbest

		Sil-Tex Mills
SMTLAWYERS.CA	WRP Asia Pacific Sdn Bhd	Triple Eight Transport
CLOUDDATAWORKS.CA	Witzenberg Municipality	McCraw Oil
SENSIBLESOLUTIONS.CA	Sita Sud	The Carlson Law Firm
KVHELI.WORDPRESS.COM	Rola Motor Group	Grupo Ruiz
distinctive-systems.com	Paltrack	stignatiusijamsville.org
LeMatic	Lotus Bedding	About Women Ob-Gyn
Tahkout Group	Shtainmetz Aminoach	Federal University of Sergipe
Bumble Inc.	BIB Insurance Brokers	Gaviota
Philippine Savings Bank	Ayuntamiento de Beniel	STESAD
InfoCom	British School of Brasilia	Softlab SpA
Valbifrut	Eurotex	Spring Grove Area School District
Chu & Yang Dental	Release Marine	Retrofit Service
KRÜSS	Raymundos Food Group	hilden.in
Service Broadcasting Group	Riverwood Golf Club	MUTTI-PARMA.COM
NessCampbell	Eastern Ice	CPJ.ORG
CMA Flooring & Design	Kontena Nasional Berhad	BORING.COM
Family Partnerships of Central Florida	Ciena	TriVector Services
tiw-group.com	MecMatica	lpollockpr.com
WHOLEIT.COM.AU	ETC Companies	Morton Buildings
SKYEEXCAVATIONS.COM.AU	HexaCream Dental Laboratory	Fedcap
ROBERTSDESIGNS.COM.AU	PKT QS	Anteriad
Y-ARCHITECTURE.STUDIO	Might Electronic Co. LTD	These companies havebeen hacked.
VENTNOR.COM.AU	veenkoloniaalmuseum.nl	Udall Law Firm
RMWGROUPE.COM.AU	www.coconutboard.gov.in	Gordon Companies
PODIATRYWA.COM.AU	Sandberg	Luxshare Precision Industry Co. Ltd.
MRAGROUPE.COM.AU	McDonalds India	Applied LNG
THEHALEROAD.COM.AU	Altius Geotecnia y Obras Especiales	PTS Goldkist Industries Sdn Bhd

ETTOAUSTRALIA.COM	TriApex US Laboratories	The Cressi
NEXTPHAZE.COM.AU	San Carlo Gruppo Alimentare	Telstar-Hommel
KLMEQUITIES.COM	Kontena Nasional Berhad	National Water Authority
NYASPHALT.COM	Talleyville Fire	SCHNEIDER PROTOTYPING INDIA PVT. LTD
KRIEGMANANDSMITH.COM	Pivotal Healthcare	The Structures Group
ISLANDOUTPOST.COM	Geoplin	Evergreen Printing
GALEINTL.COM	Meissner Bolte	Sortimage
CENTINELA.COM.BR	PAO HWA TRADING LTD	Labeltex Group
MCKEEGROUP.NET	abcseamless.com	BUHLMANN GROUP
ESCALI.COM	wohnverbund-st-gertrud.de	Commercial Paving
COBU-ARCH.COM	ipu.co.il	Wilson Smith CochranDickerson
ARKTLA.ORG	GC Accounting	RJS
M-B.LAW	WANCHI STEEL INDUSTRIAL	Westlake Christian Academy
DataBank	Reeves Information Technology	RGD Consulting Engineers
JLK Rosenberger	ASRock Rack	strategic-ts.com
LGBTQ Center Orange county	GIBSIN Engineers	Wamtechnik
DeRenzis & Associates	Yumark Enterprises	Systherm Grupa
Impressico Business Solutions	Durashiloh	Hart
Affordable Housing Management Overview Metrics	Whitfield Welding Inc	Options
Active Green + Ross	Casadei	Berkmann Wine Cellars
JP Research	Ocean Fish	Morgan Records Management
FIAMPACK	Deck India Engineering Pvt. Ltd	Complexul Energetic Oltenia
anagnosdoor.com	Bray Whaler	Aero Fabrications
nbccministries.org	Channel Products	Apex Spine and Neurosurgery
Callagy Law Firm	Avalon Hills	Hytec South Africa
ttmet.co.th	National Waste Associates	USArt
twi-group.com	Thunder Mountain Harley-Davidson	Charles Leonard Steel Services
Match Group	Mid-park Ink	Epi du Rouergue
shawhillprimaryschool.org.uk	QFloors	Secorp Industries

newkirklaw.com	Advanced Business Equipment	Medical Asset Management
KSP TLM INDONESIA	Bikkal & Associates	Health Bridge Chiropractic
FRUIT-BONTÉ Agroalimentaire	Office for Students	baja.gob.mx
Morison Insurance Brokers	Title Guaranty	Autohaus Pichel GmbH
Gallagher Transport International	Galutti Automotive Industria Metalurgica Ltda	Due Doyle Fanning
Ashcraft	GSM PORTAL TEKNOLOJİ HİZMETLERİ TİC. LTD. ŞTİ	Mill Brothers
lenotech.com.ph	University Volkswagen Mazda	Italgrafica Sistemi
COMPAGNIE FONCIÈRE PARISIENNE	Dreher Law Firm	www.swautomation.at
skyegtours.com	Jampen Holzbau AG	Saplog Group
QualiChem Metalworking	Vietnam Airlines	www.sje.vic.edu.au
Abu Dhabi Indian School – Branch 1, Al Wathba	Balneario	www.granosycereales.com.co
Connor Co	Southern Alberta Community Living Association	www.ville-dunkerque.fr
Goodmanagement	MKC Customs Brokers International Inc.	CEIVA Logic
Global Parts & Maintenance	Nafae Sanitaire S.a.r.l	www.blackdogsalvage.com
IMA Diligence Services	Orthopaedic Specialists of Massachusetts	crawfordorthodontics.net
Sukhothai Thammathirat Open University	Cary Pediatric Center	www.stcharlesprep.org
MMD Insurance Law Advocates	anfibius.net	www.mcphillamysgold.com
The Trevino Group, Inc	ccbtr.org	www.msCorp.net
OEC Medical Systems, Inc	Ilumno	www.burdettedental.com
Panera Bread	UGS	www.tecnoelectric.com.py
freidarothman.com	Colacem	KSL Ingenieure
Uniflex Technology Inc	Laboratorios Smasac	Purcell Architects
cs.at	Fluorsid Spa	Gebrüder Bagusat GmbH & Co. KG
Tele Plus	Central Roofing South Wales	Posillico
F&B Mfg	hl.co.uk	The Lewis Bear
The Sourcing Group	comercialautomotriz.com	salcom.com

ALLMAX	ecsc.org	swdc.wa
Quantum Fuel Systems Technologies	Dongguan HYX Industrial	lauryсенkitchens.com
Aquatic Control	La Macchia Group	wildbunchdistribution.com
Christine London	Commenco	kiddsservices.com
Routten & Laster Law	MicroPrecision	hartford.fr
Joyva	DigiCOURSE	groupecho.com
www.shrimphouse.com	Industrial Rivet & Fastener Company	miltonfl.org
zHealthEHR	CFM Mozambique	www.braemac.com
sitoy.com	Grupo Roa	Triad Packaging
Prince & Schmidt LLP	JR Advertising Specialties	madisonareaymca.org
Disuelas JC SAS	Dedman Gray Property Consultants	M&M Auto Parts
premmotors.com	Upper Township	Harris Consulting Engineers
namico.go.ke	NWIMS IT Group	Krenzer Marine Overview Metrics
Jakarta Nanyang School	cirrusaviation	Lares
KREISEL	sjl-legal.com	The Boathouse on the Bay
Mills Products	PSTECHLTD	Windward Life Care
Langley Twigg Law	1171 Rue Notre Dame O	Wesley Heating & Cooling
Vitosha Park Hotel	Krez & Flores	American Health
Centrotherm International	Texas State Utilities	GreenValley International
WRENLAWFIRM.COM	Neo Group	NLFX Professional
LDHRLAW.COM	Moen	Delko
GENESYSSPINE.COM	Aero-Coating	Sva Y Tecnologia Movil De España
HILTON.COM	Bergmanis Preyra	Lampire Biological Laboratories
WEATHER.COM	Gorlick Kravitz & Listhaus	Pools by Bradley
WHISKIJACKRESORTS.COM	Paylogix	DESY
GROUPAMS.CO.UK	McAloon & Friedman	Bolttech.io
RTCCOMPUTERS.COM	depotnapoli.com	IDeaS.com
CCCM.BC.CA	vistlabs.com	Resource Corporation of

		America
TECHNIKE.LCA	Nordstrom Rack	Tommotek
KAZMILAW.COM	Kan & Krishme	Sönmezler Metal
WFRFIRE.COM	Samson Equipment	Cal Spas, Inc.
VERTIGORELEASING.COM	Vereinigte-stadtwerke	Hydrodiseno
BR-ALSETH.NO	Peugeot Motocycles	Bina Darulaman Berhad
4DITSOLUTIONS.COM	JJ White	PernelMedia
VISTA-TRAINING.COM	Soapeople	KwikLedgers
RSTR.IT	Visionwheel	Laurenzano Logistics
WILDRIDGELANDSCAPE.COM	Sanko Gosei Technology	Sunzen Biotech Berhad
MODTECH.CA	Chemirrol	Varimed Medikal
INSPYRSOLUTIONS.COM	Rameder	Youngblood Tyler & Associates
CLEARWAYGROUP.COM	Bär Cargolift	Borough of Moonachie
EXCELAS1.COM	Rogers Capital	mtspokanepediatrics.com
OKIN GROUP	Gtech	proton-system_Serbia
Şemsioğlu Uşak Ev Tarhanası	Ernest Maier	Automation One Business Systems Inc
Cytek Biosciences	Designers Mirror and Glass	UBS Office
The Successful Match	Pathology Associates Of Saint Thomas	Ellison Educational Equipment
KICKSTAGE	Lunsford Capital	Farmacia San Pablo
BIDAIK BANO S.L.	Pre-Con Builders	Jing Cheng Enterprise Co., Ltd.
Aromate Industries Co., Ltd. z	Radiant Remodeling	Sai Oral SurgeryOral
Lesk Engineers Limited	The National Auto Loan Network	mdm@NT
Golden Growth Biotechnology	Rebars & Mesh	McKenzie SewOn
MBM	ImageWorks Display	Röben Tonbaustoffe
Shiffler Equipment Sales	TruGolf	NECO Equipment
Borg Argentina	seha.org.sa	cj Global
D & D Building	Fechner Pump & Supply	Lakeside Title Company
gsglobalresources.com	H2 Builders	Wardell Builders
lcpublishinggroup.com	Copec S.A.	Garner Foods

adifse.com.ar	Adriatic Port Authority	Pewarchuk CPA
trulinemfg.com	acswinc.com	Benise-Dowling & Associates
superiordrywall.com	Hyatt Place New York	Rockport Technology Group
interr.com	AUTOCARES CARRETERO	Stoughton Steel
Herzing	Quick Safety Electric	SINBON Electronics Co., Ltd
HARTE-BAVENDAMM Rechtsanwlte PartG mbB	Merit Group	Csv Group
Gianni Botsford Architects	bellowsmfg.com	Sugawara Laboratories
LTS Group	Ju Teng International Holdings Ltd	Barnes & Jones

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。

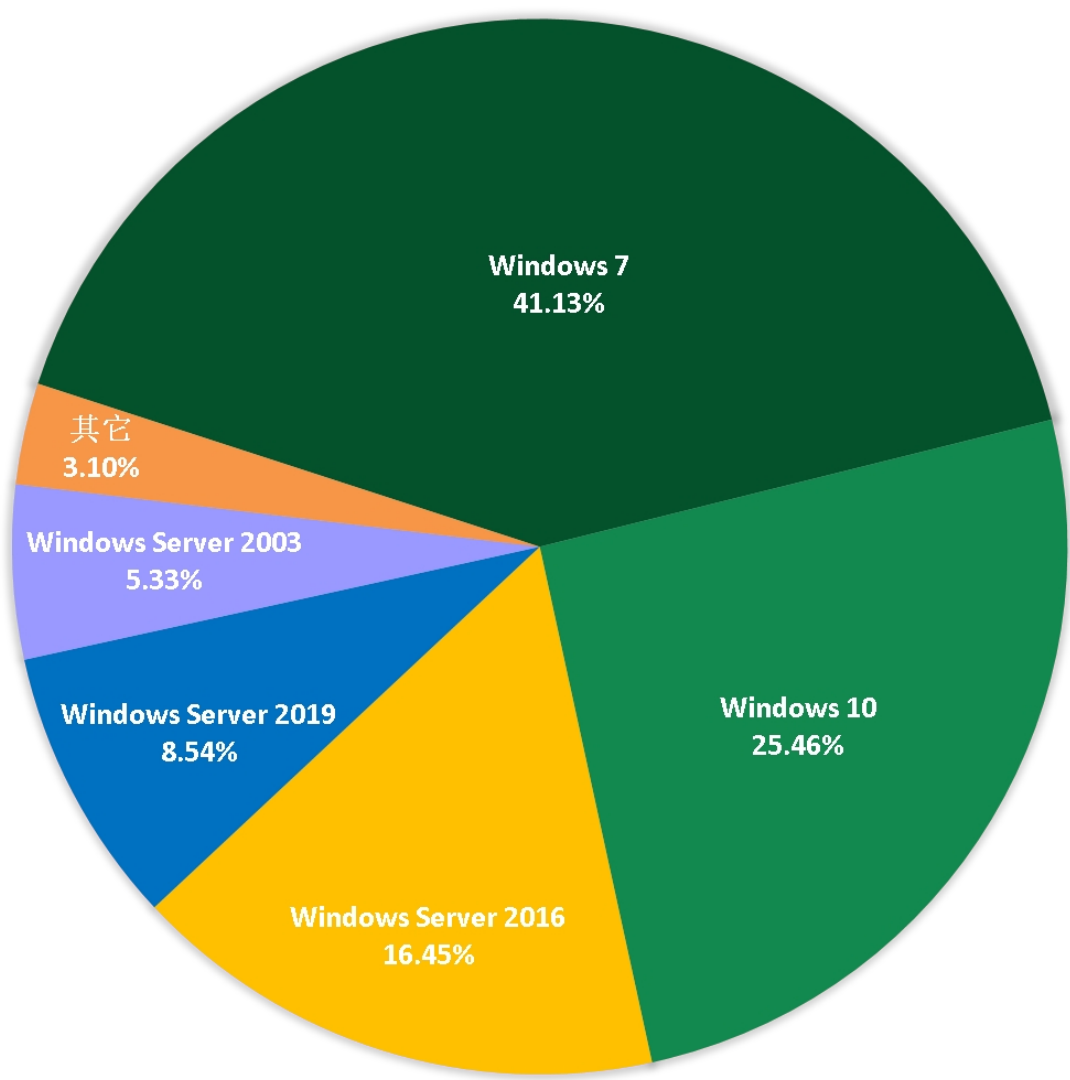


图 9. 2026 年 1 月受攻击系统占比

对 2026 年 1 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。

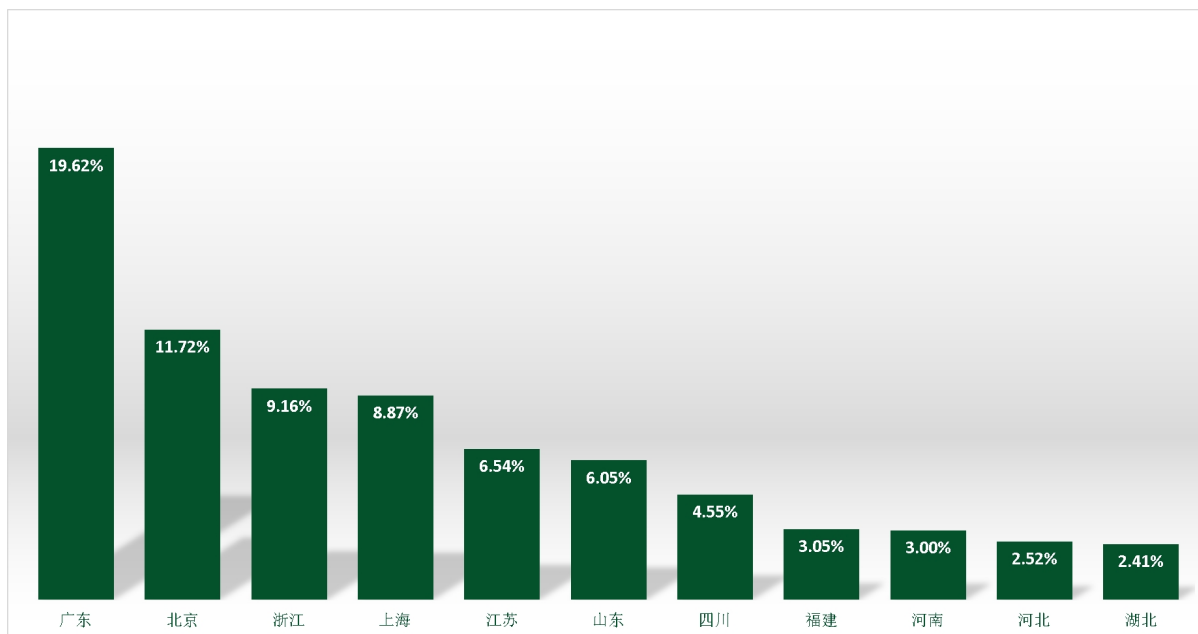


图 10. 2026 年 1 月国内受攻击地区占比排名

通过观察 2026 年 1 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。

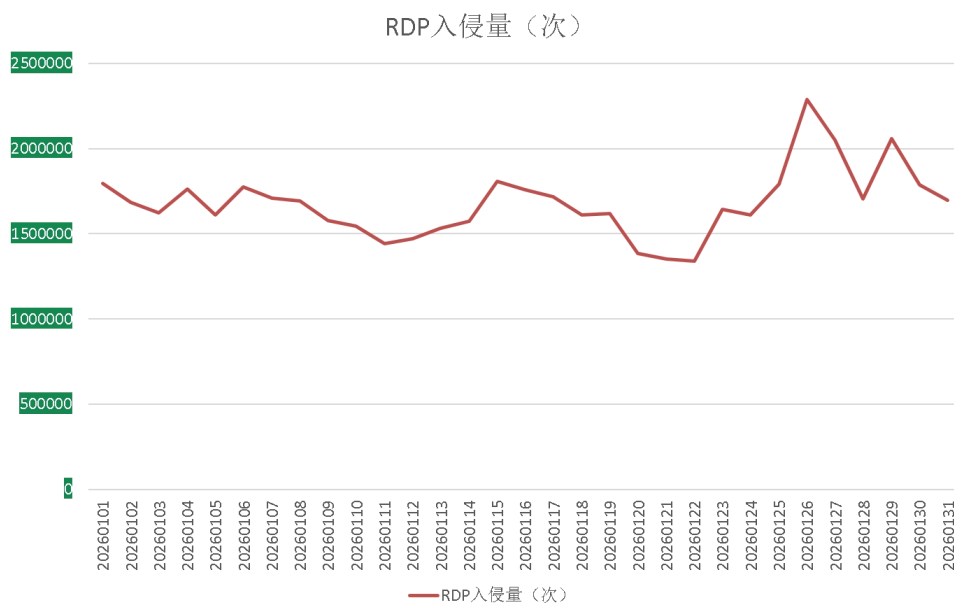


图 11. 2026 年 1 月监控到的 RDP 入侵量

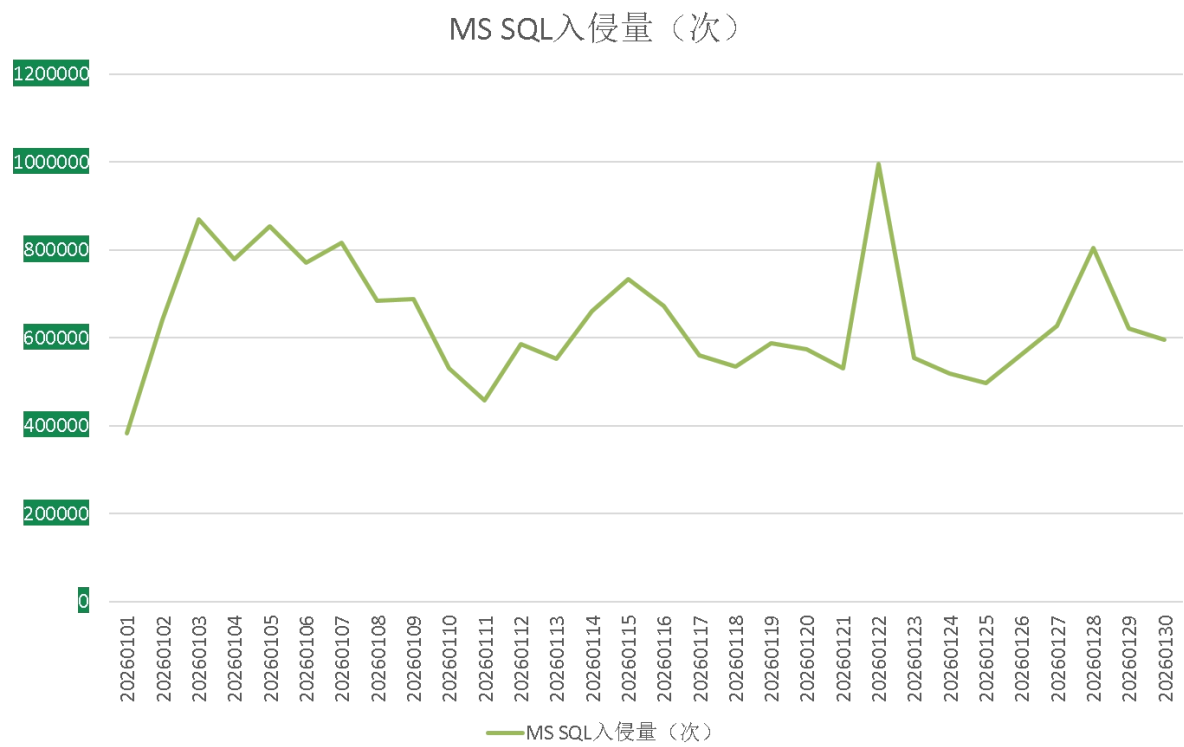


图 12. 2026 年 1 月监控到的 MS SQL 入侵量

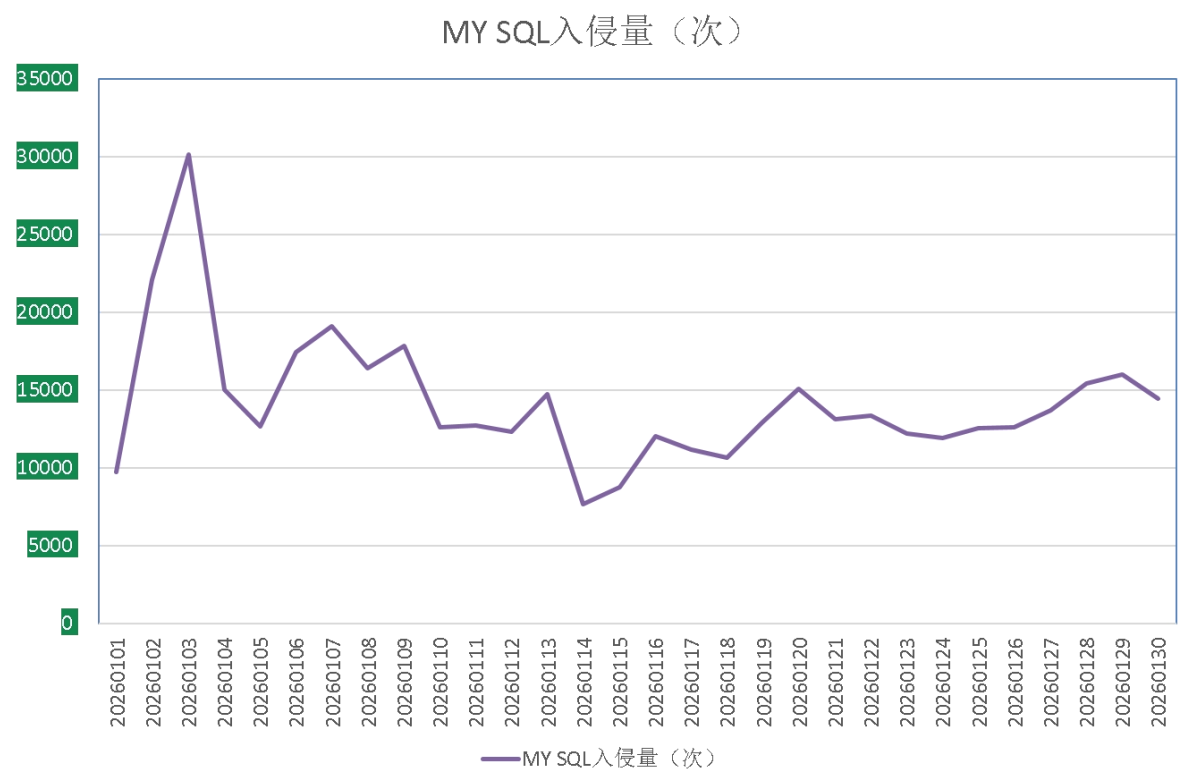


图 13. 2026 年 1 月监控到的 MYSQL 入侵量

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。

- ✧ rx: 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。
- ✧ 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。
- ✧ nezha: 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。
- ✧ 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。
- ✧ weax: 同 rx。
- ✧ lockbit: 属于 LockBit 勒索软件家族，传播方式多样。包括广撒

网与定向钓鱼、远程桌面或数据库爆破登录、漏洞利用、僵尸网络下发、远程凭据劫持等。

✧ revrac：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。

✧ 1mwillc4：同 lockbit。

✧ qrxnm74sx：同 lockbit。

✧ 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。

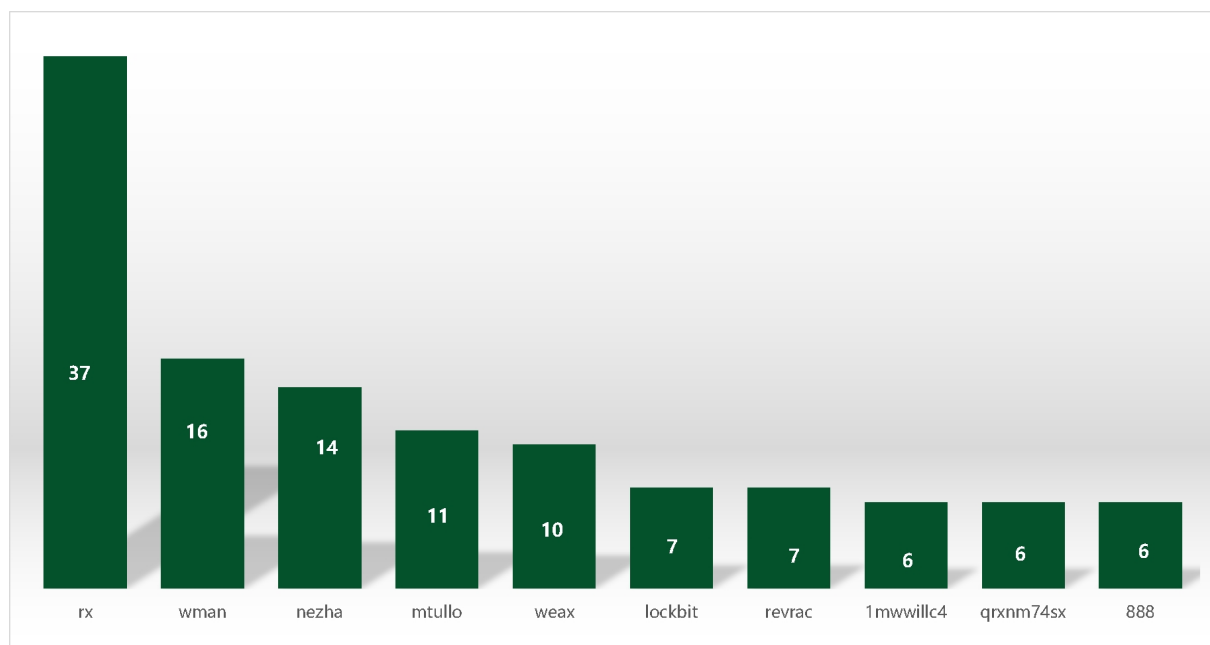


图 14. 2026 年 1 月反病毒搜索引擎关键词搜索排名

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 MiddCrypto。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。

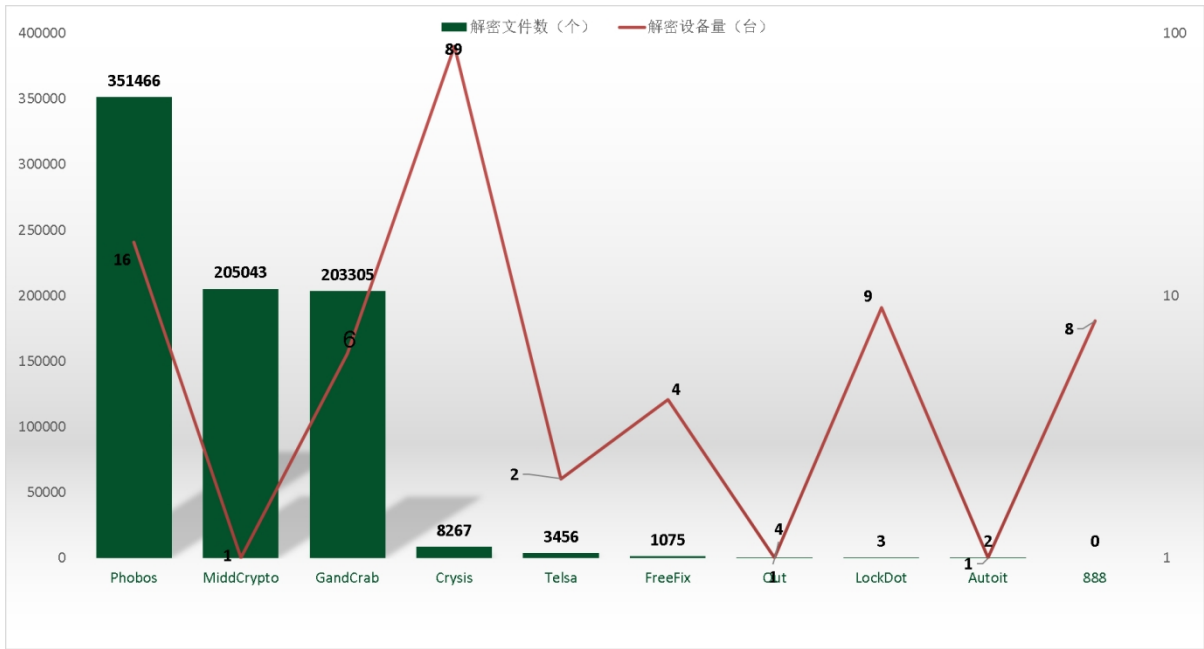


图 15. 2026 年 1 月解密大师解密文件数及设备数排名