2026 年 5 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中不断出现。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 5 月，全球新增的双重勒索软件有 Mortar、CmdOrganization、0daySyndicate 家族，传统勒索软件家族新增 LaliaLocker、LQTOREQ、BrzCrypt 等多个家族。

Sorry 勒索家族本月持续活跃。此前 360 发布深度报告预警该家族存在 Linux 版本，报告发布后不久便被境外多个安全论坛与媒体证实其 Linux 版本正利用 cPanel 漏洞大肆传播。与此同时该家族的 Windows 版本在国内也维持着高发态势，本月主要利用 Borland Socket Server（PE 版本信息中的原始文件名为 scktsrvr.exe）漏洞进行传播。该组件漏洞影响了国内多个行业头部厂商的中小微企业管理软件。据现有反馈与观察，受影响行业主要集中在医药、医疗器械、中小商贸，以及其他各类中小微企业。

本月 Weaxor 家族 rox 后缀变种持续活跃，360 同时捕获了该家族这一后缀的 Linux 平台样本，延续了该家族漏洞利用的攻击模式。而在

Windows 目标下，仍在通过持续多轮更换远程下发的 BYOVD 驱动以对抗安全软件。另外，该家族还迅速将开源情报披露的一款联想漏洞驱动迅速武器化发起攻击，被 360 安全大脑及时拦截。

LockBit 家族本月再度通过 Phorpiex 僵尸网络进行批量下发，相关反馈的攻击时段集中于 5 月 26 日后。这些受害者中招前均未安装有效的安全软件进行防护，鉴于僵尸网络的内网传播与持续潜伏特性，受害者需主动与所在机构与单位沟通并及时进行内网安全扫描与加固。

**以下是本月值得关注的部分热点：**

**① Sorry 勒索软件大规模利用 cPanel 漏洞发起攻击**

**② 富士康证实 Nitrogen 勒索团伙声称的网络攻击**

**③ 网络犯罪服务利用微软平台签名恶意软件的行为被拦截**

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超过十年，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 58.94%，**未正常启用** 360 安全软件的设备占比 19.94%，安装了其他安全软件的设备则占比 21.11%。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。

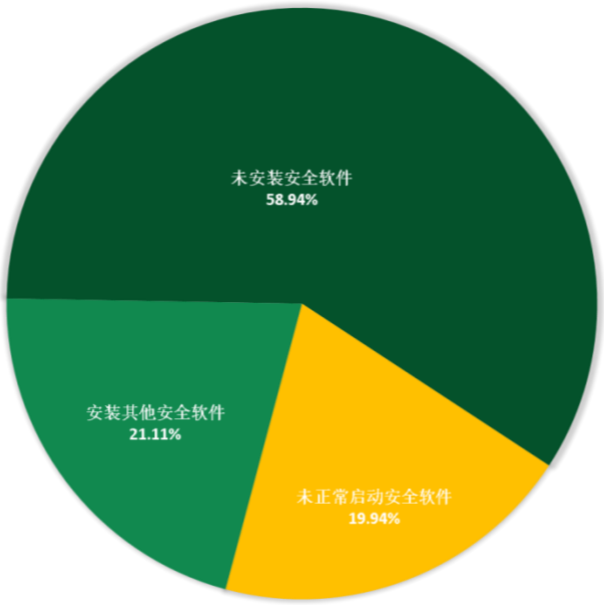


图 1. 2026 年 5 月勒索软件中招设备中安装的安全软件占比

# 感染数据分析

针对本月勒索软件受害者设备中病毒家族进行统计：Weaxor 家族占比 26.72%，居首位；第二的是 Wmansvcs，占比 23.71%；Sorry 家族以 14.66%的占比位居第三。

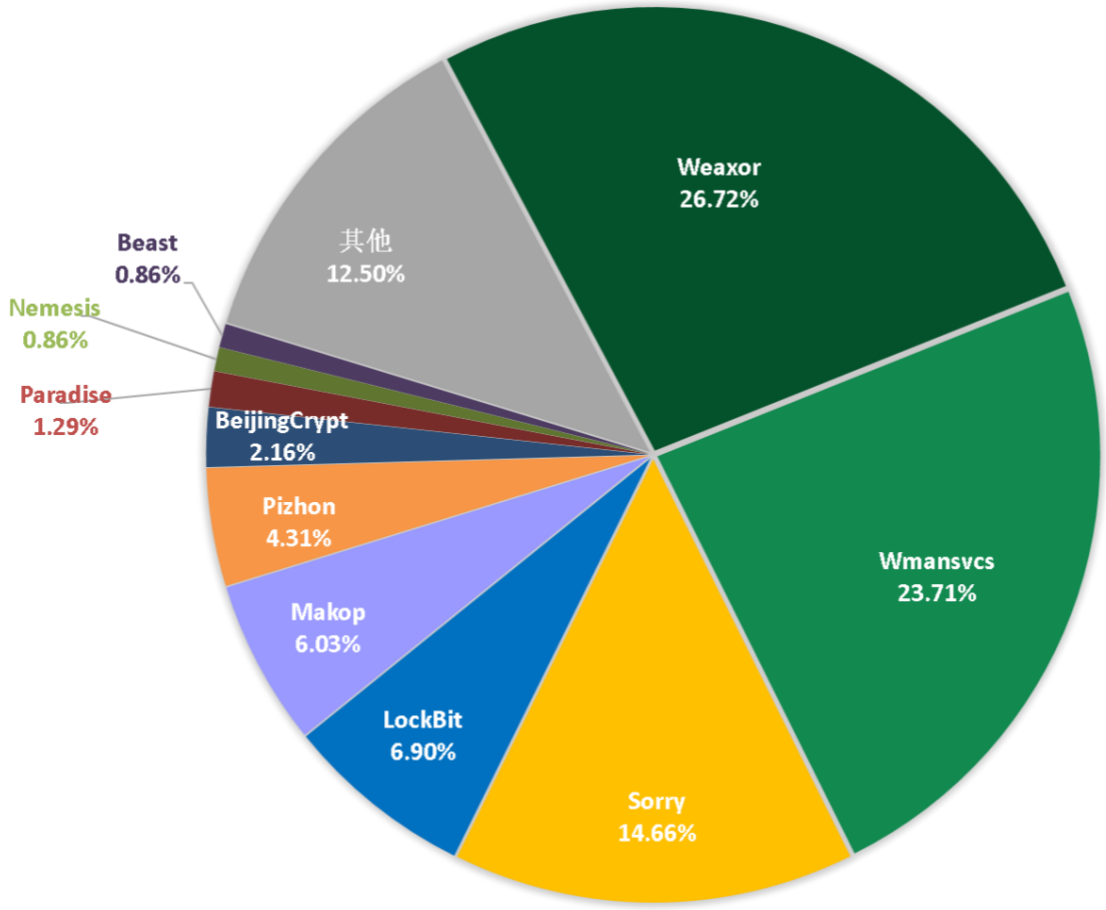


图 2. 2026 年 5 月勒索软件家族占比

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

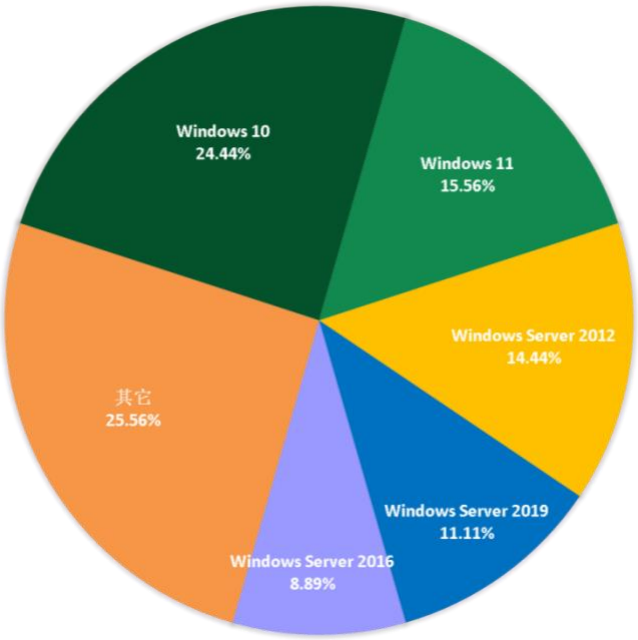


图 3. 2026 年 5 月勒索软件入侵操作系统占比

2026 年 5 月被感染的系统中，从桌面系统、服务器系统占比来看，服务器数量领先于桌面 PC，Nas 平台攻击行为有所增加。

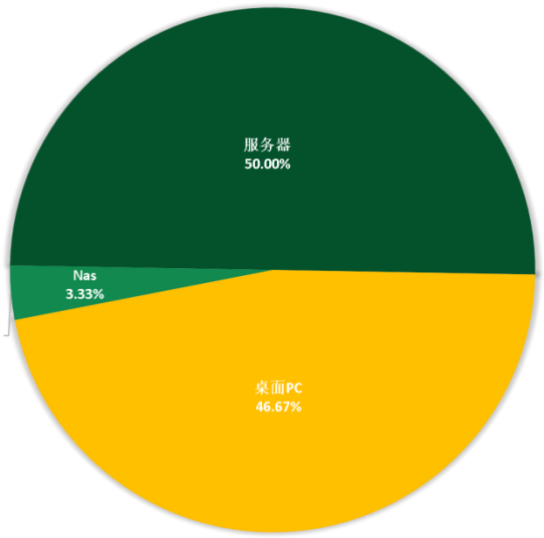


图 4. 2026 年 5 月勒索软件入侵操作系统类型占比

# 勒索软件热点事件

## Sorry 勒索软件大规模利用 cPanel 漏洞发起攻击

本月初，Linux 主机管理面板 WHM/cPanel 被披露存在严重身份验证绕过漏洞 CVE-2026-41940，攻击者已大规模利用该漏洞入侵服务器并发动“Sorry”勒索软件攻击。官方本周紧急发布安全更新修复漏洞，但安全研究人员发现，该漏洞实际上早在 2 月底就已被当作零日漏洞利用。互联网安全机构 ShadowServer 表示，目前已有至少 4.4 万个运行 cPanel 的 IP 地址在持续攻击中遭到入侵。

攻击者利用该漏洞获取服务器控制权限后，会部署基于 Go 语言开发的 Linux 版“Sorry”勒索软件，对网站数据进行加密。已有大量网站受到影响，部分受害站点甚至已被 Google 索引。该勒索软件会给加密文件追加“.sorry”扩展名，并在每个目录中生成名为 README.md 的勒索说明，要求受害者通过 Tox 联系攻击者协商赎金支付。所有受害者收到的 Tox ID 均相同，说明此次攻击活动可能由同一团伙统一实施。

技术分析显示，“Sorry”勒索软件使用 ChaCha20 流加密算法加密文件，并通过内置 RSA-2048 公钥保护密钥。若没有对应的 RSA-2048 私钥，几乎无法恢复被加密的数据。此外，本次“Sorry”勒索软件与 2018 年曾使用 HiddenTear 加密器、同样附加“.sorry”后缀的旧攻击活动并无关联。

## 富士康证实 Nitrogen 勒索团伙声称的网络攻击

电子制造巨头、全球最大电子产品代工厂富士康证实，其位于北美的部分工厂遭遇网络攻击，目前正逐步恢复正常运营。公司表示，事件发生后已立即启动网络安全应急机制，并采取多项措施保障生产与交付持续进行。富士康在全球 24 个国家拥有超过 240 个园区、约 90 万名员工，2025 年营收超过 2600 亿美元，同时为苹果、英伟达、英特尔、谷歌等大型科技企业生产电子产品。

此次事件源于“Nitrogen”勒索软件组织的公开声明。该组织声称已窃取富士康约 8TB 数据和超过 1100 万份文件，其中包括苹果、英特尔、谷歌、英伟达、AMD 等客户的“机密指令、项目与设计图纸”。富士康随后向媒体确认遭受攻击，但未透露更多受影响细节。

报道指出，Nitrogen 勒索软件组织最早于 2023 年出现，其早期恶意加载器曾部署 BlackCat/ALPHV 勒索软件，之后又基于泄露的 Conti 2 代码开发了自己的勒索软件。不过安全研究人员发现，其针对 VMware ESXi 环境的加密程序存在严重编码错误，可能导致文件被不可逆损坏。虽然 Nitrogen 并非最活跃的勒索软件团伙，但自 2024 年以来已陆续公布数十名受害者。

此外，富士康此前也多次遭遇勒索软件攻击，包括 2024 年的 LockBit 勒索软件事件，以及 2020 年 DoppelPaymer 勒索软件针对其墨西哥工厂的攻击，当时攻击者声称加密了约 1400 台服务器，并索要

3400 万美元赎金。

## 网络犯罪服务利用微软平台签名恶意软件的行为被拦截

微软披露并联合执法机构打击了一个名为“Fox Tempest”的“恶意软件签名即服务”犯罪平台。该组织滥用微软 Azure Artifact Signing 云签名服务，为恶意程序生成短期数字签名证书，使恶意软件能够伪装成合法程序绕过 Windows 安全检测。微软称，Fox Tempest 已创建超过 1000 个欺诈性代码签名证书以及数百个 Azure 租户和订阅，并通过美国纽约南区联邦法院提起法律行动。微软随后查封了其核心域名 signspace[.]cloud，下线数百台相关虚拟机，并阻断其基础设施访问。

调查显示，该平台被广泛用于多个恶意软件和勒索软件攻击活动，包括 Oyster、Lumma Stealer、Vidar，以及 Rhysida、Akira、INC、Qilin 和 BlackByte 等勒索软件家族。微软指出，包括 Vanilla Tempest（INC 勒索软件成员）、Storm-0501、Storm-2561 和 Storm-0249 在内的攻击者都曾使用这些经过签名的恶意程序实施攻击。犯罪分子会将恶意文件伪装成 Microsoft Teams、AnyDesk、PuTTY、Webex 等合法软件安装包，诱导受害者执行后部署恶意加载器、Oyster 木马以及 Rhysida 勒索软件。

微软认为，Fox Tempest 通过盗用美国和加拿大身份信息，绕过签

名服务身份验证，并专门使用仅 72 小时有效的短期证书以降低暴露风险。该平台还向客户提供预配置云虚拟机用于自动化签名服务，并通过 Telegram 频道“EV Certs for Sale by SamCodeSign”公开招揽客户，收费高达 5000 至 9000 美元比特币。微软表示，该组织已从相关非法业务中获利数百万美元。

# 黑客信息披露

## 本月收集到的黑客邮箱信息如下

| | | |
|---|---|---|
| taskt001@tutamail.com | god8damn@cyberfear.com | logoplus@cock.li |
| hacklogic@mailum.com | yourquickunlock@mailum.com | hunter505@cock.li |
| heizenberg@cyberfear.com | yourquickunlock@cyberfear.com | supp_brz@tutamail.com |
| heizenberg@onionmail.org | datahelper@cyberfea.com | Crypter008800@fonix.email |
| encryptedfile1@outlook.com | ginesomna@outlook.com | sthipade@tutamail.com |
| encryptedfile1@hotmail.com | vvvnet396@gmail.com | sthipade@cyberfear.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）。

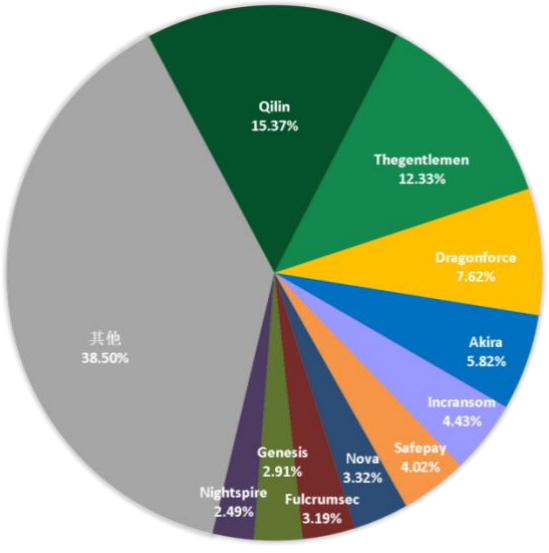


图 5. 2026 年 5 月通过数据泄露获利的勒索软件家族占比

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 773 个组织/企业遭遇双重勒索/多重勒索攻击，其中包含中国 15 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 14 个组织/企业未被标明，因此不在以下表格中。

| | | |
|---|---|---|
| Grupo Mau á | shougang.com.pe | CCD Interiors |
| MERCOR | centralromana.com.do | Shipping Services |
| MAPFRE ASSURANCE | TSG Enterprises | Calidra |
| Lake Washington School District | Barclay Damon | CMC Expertise Comptable |
| tulipmediworld.com | Zuther Hautmann | Exco Technologies |
| Cavalier Flooring Systems Inc. | RADWAG | Imex International |
| Wentworth | ROTH-TECHNIK AUSTRIA | R é seau Radiologique Romand |
| Green Resource | SARL CANIS EVENTS SÉCURITÉ PRIVÉE | Acros Sport GmbH |
| Cedar Street Capital | nacs.com.hk | Ashtech Infotech |
| A Roettgers | mindmastersg.com | Zojirushi |
| Siveco - | Landeshauptstadt Stuttgart | Greenwoods Dental Centre |
| Openmind networks | Veda Consulting Company | Desysweb |
| Pragmatic Solutions | Tang Seng Nitrogen & Pump Systems Pte. Ltd. | PennEastern Architects |
| Indiana Mills and Manufacturing | Elohim Law Corporation | cmswpc.com |
| UEI College | Kabushiki Gaisha Hodozuka Setsubi | autorisk.org |
| STAREMPIRE | Nordfjord Hotell | earthsystems.com.au<br>earthsystemseurope.com |
| LTI Services and Larick Towing | Asian Lite International | egnyte.com |
| Lee Law Offices | harrisoncountywv.com | Trellix (McAfee & FireEye) |
| BC3 Tecnologia | printroom.co.uk | K & E Distributing |
| Plexsupply Inc | hautarzt-budihardja.de | Accessoires Outillage Ltee |

| | | |
|---|---|---|
| SIRILAK SEAFOOD (PW) LTD. | mediafrance.de | EMA Engineering & Consulting |
| Apex Maritime Co., Inc. | Gartengestaltung Muller eU | Stuf Storage |
| ecci-srl.com | RCR Industrial Flooring | Soprolux |
| www.labexpress.com | ashleytimber.co.uk | Rehab Clinics Group Ltd |
| Daegu University AI Department | adlan.com | Sylvania |
| VODAFONE | Vantage Energy LLC | Norcal Training Center |
| Shoreline Sightseeing | Internal Medicine | Elia Law Firm |
| AcademyHealth | Polyrack | rjrgleanergroup.com |
| Commune De Camiers | Internet Technologies Designs | de.yangming.com |
| Capital Family Physicians | E-Control Systems | anser-coding.com |
| Schacht Law Office | DEVO-Tech | rhactushotel.com |
| Badan Pangan Nasional | Modern Display | Jacobs Doland Beer |
| Braincell | University of Finance and Administration | Grau GmbH |
| BCD Travel | Huse Incorporated | Excel Healthcare Receivable Management & Consulting |
| Interstate Roofing | TAKOSAN OTOMOBIL | pvdd.ca |
| SOMAFIX | Mezta Corporativo, S.A. de C.V. | datasavior.com |
| Healthtrax Fitness &Wellness | Abp Autoricambi Srl | kbtoys.com.au |
| Shanpoornam Metals | DFI AMERICA, LLC | alge-stop.dk |
| Restorative Therapies, Inc. | CRIT Tunisie | smp.cat |
| Asopagos S.A. | Groupe CRIT SA | gingerichtrucking.com |
| E P M | ETM-ELECTROMATIC, INC. | jmige.com |
| belimed.com | Quahe Woo & Palmer LLC | Inox Market Service SpA |
| powerhousenow.com | Berlinmobil.de | BMTP |
| entransinternational.com | Vacu - Lug | Laclinic-Montreux |
| Peña & Bromberg | Healthtrax Fitness & Wellness | Complastex.com |
| American Battery Factory | Stonehenge Therapeutic Community | Farella Braun + Martel LLP Information |
| Mayelia Automotive | Design Engineering & Consulting | Sandberg Phoenix Information |
| Techmar | Jazz Hipster | id-s.de |
| Grupo Premier | MSC Group | mbk-gmbh.de |

| | | |
|---|---|---|
| Fonderia Corra | Tr é sor Public | ettp.be |
| Heartland Growers | bergen1.net | studioubertazzi.it |
| Corporacion Prokompra | challenge-mfg.com | globalmerchservices.com |
| Fox Rothschild LLP | wtitransport.com | soavegel.it |
| Spedition Kern | cstindustries.com | Houk Air Conditioning |
| Advanced Psychiatry Associates | fallprotect.com | Panal Seguros S.A. |
| Sidra Kuwait Hospital | Salter HealthCare | Time-Cap Labs |
| VVO Finance | Majlis Perbandaran Alor Gajah | Asphalt Specialists |
| AKM | Monir Precision Monitoring | Le Maire de QUIBERON |
| Sinomax USA | Buckeye Paper | Clinical Registry Solutions |
| Mindpath College Health | Mus é e du Bas-Saint-Laurent | SDK Environmental |
| Carton Craft Supply | Fruits Queralt | Nrt India |
| Gallun Snow Associates | The Taylor Provisions | Da Guan Technology |
| Kennedy, McLaughlin & Associates | BAUM Games | Riggotts |
| HumanEdge | Don Bosco Technical Institute of Makati | IPE |
| Providence Medical Group | dosocho.es | Gator Cases |
| Tripod Farmers | soft-inc.com | DATAMATIC |
| Jens Jensen | Plan | C2O Architects |
| Osool Poultry | psbsementi.it | FMS |
| Martinez & Shanken | grupo55.com | Clark Fixture Technologies |
| TransferZ | Ingelan | Manhattan Fire Safety Corp |
| L&P Aesthetics | Holy Name of Jesus | Worralls |
| GS Yuasa Lithium Power | URG OEM | Mundo Amtae |
| General Doors | PNSB Insurance Brokers Sdn Bhd | Aerodiagnostics |
| Alpine Aerotech | metaval.com.au | Moorman Harting |
| Maschinen-Stockert | Comercial Echave Turri Limitada | ABI and Ideal Tape |
| Hospice Savannah | Trivantage | Heinrich Kopp |
| xgenize.com | Parle Agro | Nostrum |
| gokids | RAMAR FOODS INTERNATIONAL | MIMS |

| | | |
|---|---|---|
| dxon.com.br | Ross Yerger Insurance | IT Management |
| xl africa group | CLINICA AVELLANEDA MEDICAL CENTER | Colegio Notre Dame Campinas |
| lawants | Transitions Pro Centre Val de Loire | Beaconhouse School System |
| casasafer | AdvancedHEALTH | Heatherwood Golf Club |
| Otthon Centrum | Turner Supply | ACFA Regionale de Calgary |
| President Container Group | Zywave | Fabritius |
| motofrenos.com | Grafana | Forsheda Stlverktyg |
| smile-siam.com | B.Care Medical Center | Magisterial Service |
| sterlingindustries.com | NR Engineering Co., Ltd. | Kınık Gross |
| My English House academy | Australian College of Business Intelligence | Arcelik |
| William Davis Homes | Generation Life | Media Consulting |
| Mainstreet Organization of REALTORS | Menzies Group | Keretapi Tanah |
| Shocco Springs | LeRoy Surveyors & Engineers | Triquim |
| Roofing Solutions | Raise the Bottom | Engineered Advantage |
| fabbricausa.com | Tower View Primary School | The Modern Flour Mill |
| erh.co.uk | Common Part Groupings | East |
| waypointsolutions.com | Foot Solutions | Millennium Partners |
| profundo.nl | Advanced Medical Consultants | Ontario Physiotherapy Association |
| jcripberger.com | Fox Valley Tax Solutions | Levante Living |
| pieralisi.com | wwag.org | Kasapreko |
| nemd.com | McCarthy Inc | Marutake |
| practicus.co.uk | defenseisready.com | Mediaplex [Redirect attivo su digiplex.it] |
| refreshmentsystems.co.uk | lafj.org | Diviso Grupo Financiero |
| ksmart.ca | WholeHealth Chicago | La Kaffa International |
| dunasgroen.nl | Instituut voor de Nederlandse | Farmers Association of Iceland |
| northbridge.com | Grupo Alvorada | WOHA |
| wsm.co.uk | Ponisch Abogados | ttt.vn TTT Corporation |
| jichasa.com | Digiprint | Sysco |

| | | |
|---|---|---|
| FWMK Law Offices | United Quality Cooperative / www.uqcoop.com | Ropers Majeski |
| Ramos Rheumatology | Houston Eye Associates | Scales and Associates Inc |
| Northwest Woodworks | PowerCampus | Elken Sdn Bhd |
| EXCEED Energy | Ellucian PowerCampus Warning (Contact Us) | Bandeirante Supermercados |
| Gone Fishin' Marine | Stride Learning | Strategic Imports |
| hbroch.com | Amplify Technology | Magnolia (Israel) |
| Distrigaz Vest S.A. | University Of Georgia | Trimble Inc / Gerrard Inc |
| duboisag.com | Hotelogix | Atencio Engineering |
| qlslogistics.com.au | Schulte-Lindhorst GmbH & Co. | SIT Group / Robusta |
| dentonfirm.com | Fab-Masters | Desert Christian Schools (DCS) |
| Greenway Technologies | technic.com | CourtSmart |
| Delbrook Capital Advisors | Goodstone Group | ActionAid / TACOSA |
| WG Neukölln | BAYTECH A/S | Palmers Relocations |
| Ridge Law Firm | Ira & Larry Goldberg Coins & Collectibles | Académie de Montpellier / CSJM |
| Gestordes | dsdlawfirm.com | Colegio María Inmaculada (CMI) |
| Textile Testing Services of America | vspsolutions.com.au SAMPLE-FREE 20GB | CEAGESP / Netfeirasp |
| Hamister Group | John G Yphantides A Professional Law | Raycolighting |
| Sunrise, Toscana Country Club,Andalusia Country Club. | Brand X Hydrovac Services | ovextech.com |
| ctps.tp.edu.tw | LTJ Industrial Services | Cazh.id |
| sandox info | Johnson Carter Architects | Positiwise Infotech Pvt |
| Eriell | One Legal | Celeris Networks |
| H-W-G & Acros Sport | Silergy Corp | Bay State Land Services |
| Filabé | Spirit Medical Transport | Unre3d |
| Hunter | Mayer | Maximum Mold |
| BASE SPA | Bluize | Punch & Associates Investment Management |
| basatamfi | Domaine Des Tournels | Ahorramas |
| PILLER AIMMCO | MicroMarketing | GRANDHOME |

| | | |
|---|---|---|
| GW Mechanical | Pamil Modulsystem | EXPEDITOR |
| NL Fisher | Tricon Infotech | brittanyresidential.com |
| Round Hill Country Club | Belz Institutions | Adelante Soluciones Financieras (Addi.com) |
| Legend Networking & Telecom | Institute of Private Enterprise Development | Erla Technologies SAS |
| MyPillow | Allele Diagnostics | sanver.com.mx |
| Open Door Health Center | Buenos Aires Software | childplace.org |
| De Waard Transport | Gorey Community School | foodsmart.com.do |
| eitecpro.co.jp | Inteceng.com.my | Studio Marchi - Studio Professionale Associato |
| tme-rusta.de | A.R.Ge.Co | hokuyo2006.co.jp |
| cyuou.com | NTN Bearing Corporation of America | bootstransport.ca |
| vdmtrucking.com | The Gravity Group | dahlgrenscement.se |
| North Dallas Shared Ministries | Porter Wright | maiadouro.pt |
| IDS Group | Marshall Dennehey | zonaovest.to.it |
| sphvalue.com | SHERIFF | fital-treppenlifte.de |
| ennsco.ca | Infoworld Membership Systems | Seagate Capital Construction |
| arsenalscaffold.com | Town Car International | Law Office of Steven R Smith |
| rolser.com | Northern Mechanical Contractors | Foxstone Financial |
| epbinsurance.com | ACC Construction | Lexus |
| jakn.com | IWC Food Service | Rizzuto Law Firm |
| allianceadjustment.com | Ashcroft Homes | General Hardware |
| xtr-global.de | DURAND-WAYLAND | Morning Star Tours |
| saver.nl | Bestat Pharmaservices Corp. | Cushman & Wakefield |
| vegfresh.com | Focus Design Partners | vacaero.com |
| ggroupcpas.com | Shajarpak Securities | www.cswindustrials.com |
| businessrecord.com | Qatar National Broadband | Lonestar Truck Group & Tag Truck Center |
| Meirc training and consulting | Electroban SAE | City of Sandstone |
| Adensa Teknoloji | Oriental Diamond | Standard Bank Group |

| | | |
|---|---|---|
| SECONT Secretaria de Controle e Transparência | SETCAR | Cult Wines |
| Alpha Group Holdings | Value Exchange International | Johnson & Johnson Innovative Medicine |
| Alpert Slobin & Rubenstein | Dodson & Horrell | Luna Group |
| P & G Trading | Amstel Securities | ROYAL M HOTEL BY GEWAN FUJAIRAH LLC |
| Sponseller Group | GeTeCe | www.wilkemgroup.com |
| Branded Products | dentoncalvary.org | emtco.com |
| ExpoCredit | Mediapost Spain | it-freitag.de |
| Global Retool Group | Taylor Clay Products | manateeair.com |
| Red-Line | Kaplan Companies | Cushman & Wakefield Inc. |
| la familia adualt day center | Manhattan Broadcasting | Fiserv |
| Bresme Madrid S.L. | Vision 3 Architects | or-technology.com |
| Papa John's Egypt | Avanti Windows & Doors | FANASA.COM |
| Rawaj Consumer Finance | NaRaYa | cgcsa.co.za |
| Ueno Fine Chemicals Industry | Saharuang | Photonic |
| Heartland Growers | Startec Group of Companies | Standard-Examiner |
| HELIX INTERNATIONAL | NorthWest Handling Systems | North Star Signs |
| Prologic Construction | Rivadeneyra Treviño | Armstrong George Cohen Will Ophthalmology |
| Artso International, Inc. | SmilePoint Dental Group | LSM Lee |
| Seeley Office Systems | Pequod Associates | Star Precision |
| Le Perreux sur Marne | rbh aerospace inc | Beyond Measure & Associates, Inc. |
| Sanatorio Delta | Bideawee | JG Stewart Construction |
| Hussey Seatway | Casino Gaming Commission | Cytek Biosciences |
| Caka Grup Lojistik | Fargo Moorhead West Fargo Chamber | Zampell |
| TRANSSYSTEM Group | Integrated Process Engineers & Constructors. | Minidoka Memorial Hospital |
| ACAM Systemautomation | Ben F. Barcus and associates pllc | Grupo EBD |
| Koa Glass | Palo | Shenzhen Gongjin Electronics |
| Openmind Networks | HostBooks (HOT!) | Compass Housing Alliance |
| Emek Elektrik | arc-reins.com + fidelityunited.ae UPDATE-FULL DATA DUMP | Tuopu |

| | | |
|---|---|---|
| vspsolutions.com.au FULL DATA DUMP | AppDirect | arc-reins.com + fidelityunited.ae |
| Salvation Army | Arwini | Site Design Group |
| bangkok.go.th | Ayuntamiento de Valdemoro | Symcor |
| Mecanizados y Montajes Aeronáuticos | lalsgroup.com | TSYS |
| University of Valencia | Advanced Software Products Group | Epiq Global |
| Mopas Online Supermarket | Keller Williams Real Estate - Exton | northshoreenv.com |
| Baker Distributing Company | International Customer Care Services | energyaction.com.au |
| Charter Communications, Inc. | Pangolin Editions | hpk.hamburg |
| DentaQuest.com | Forestdale | bomuhospital.org |
| lasevillanita.com | Depósito Dental Universitario | Avnet |
| AMACCAO | Sistemas Electrónicos y de Telecomunicaciones | Lena Health |
| Hoy Construction | First United Methodist Church Boerne | Woundtech |
| BMJ Paperpack | ice.org.uk | youX / Drive IQ |
| Semgrep | Kent District Library | LexisNexis |
| tkgm.gov.tr | Park Dental Research | MCO |
| Gitis | Waterford Hotel Group | ReFocus AI |
| Function Enterprises | Jozef Stefan Institute (IJS) | Hatica |
| Buffalo Niagara Convention Center | Alpinion | Analog Gold / Prospector |
| Cablematic Dos Mil SLU | Tab Service | SMTA Sherwood Mutual Telephone Association |
| Karlin Foods | Cass information Systems | Ceywater Consultants |
| minsa.com.mx | Clarkson Walsh & Coulter | Peyton Law Firm |
| threadinnovations | Circle U Foods | Accurate Nursing Services |
| tvnmedia.com | Nijborg Staal | Nordstern Technologies |
| Le Pain Quotidien US | FOXCONN | ParkEngage |
| Vernon & Ginsburg | Accretech America Inc. | Saleskido |
| ROTO Immobilien | st-annes.uk.com | Interzero |
| Snyder Packaging | lifelongaccess.org | IMEVI |

| | | |
|---|---|---|
| alkaloid.com.mk | bayareaherbs.com | Raptor Supplies |
| narit.or.th | jacksoncountyin.com | Rotary Club |
| grupopetersen.com.ar | ossistemes.com | JOT |
| sheppadviser.com.au | csb-battery.com | BookBlock |
| Softseba | funkychunky.com | Crank Communications |
| ungererandcompany.com | Langenberg, Strubberg, Arand & King, LLC | CrediElite |
| G Theodor Freese | www.kurita.eu | Fashinza |
| A-Sonic Logistic Solutions | https://sibillacapital.com/ | wyomingcountyny.gov |
| Internal Medicine and Pediatrics of Cullman | lopezlawfl.com | sequoiadental.com |
| Robinsons | ams-group.co.uk FULL DATA DUMP 33GB | townofnorwell.net |
| Grupo Pasquel | Arup Group | curedentalbeltontx.com |
| MBM Corp | eclagestio360.com | austinplasticandreconstructivesurgery.com |
| YMCA of Columbia | CarePoint Health | hsjlawyers.com |
| Hotelogix Company | The American Board of Preventive Medicine | bun.nl |
| StarBucks Company | Prescott & Holden | aceforwarding.com |
| Hamer Childs | Van Atta Engineering | ic-controls.com |
| Porter W Yett | Rain Makers Solutions | Medical PAY |
| WNS Lowery | DermaPharm | orekait.com |
| Cz Collections | Hillside Lumber | gursoygrup.com.tr |
| CJ Architects | DEVCO | irestal.com |
| Air Conditioning Florida & Mrdsllc & RTE Stucco & MR Drywall Services | Arizona Professional Painting | ritta.co.th |
| Vial Agro | McCarthy | Winona County |
| Sid Harvey's | VeriCon | Roger D. Mason II, P.A. |
| Pro Farm Group Inc | KUPER | Kinsmen TeleMiracle |
| Fana Jewelry Inc | TDS | Mesquite Plumbing Inc. |
| Indian Creek Valley Water Authority | Misr Chemical Industries | Fox Broermann Pediatric Dentistry of Tulsa |

| | | |
|---|---|---|
| Exchange Group | vp-brands.com | flbgroup.com |
| Vega | Office Furniture Group | kisnet.co.jp |
| olipes.com | Calsoft Inc | nwlr.ca |
| ZFG ALTHERM Engineering | mrs holdings | liteline.com |
| TAURUS INVESTMENT HOLDINGS | CF Evans Construction | westonconsulting.com |
| Nothing | Lindabury | exceldor.ca |
| Wysza Szkoa Biznesu National Louis University | DL Cohen Construction | soundinsurance.ca |
| Acton Electrical | Ruiz Barbarin Arquitectos Slp | endeavourautomotive.co.uk |
| jec.co.id | Fogel Capital Management | eworldme.com |
| santoinacio-rio.com.br | Neurotrials Research Inc | bridgeway-consulting.co.uk |
| lbreng.com.br | CAD-IT UK | The Country Club of Darien |
| stahlwille.nl | Advanced Laundry Systems | Colorado Dental Wellness Center |

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。

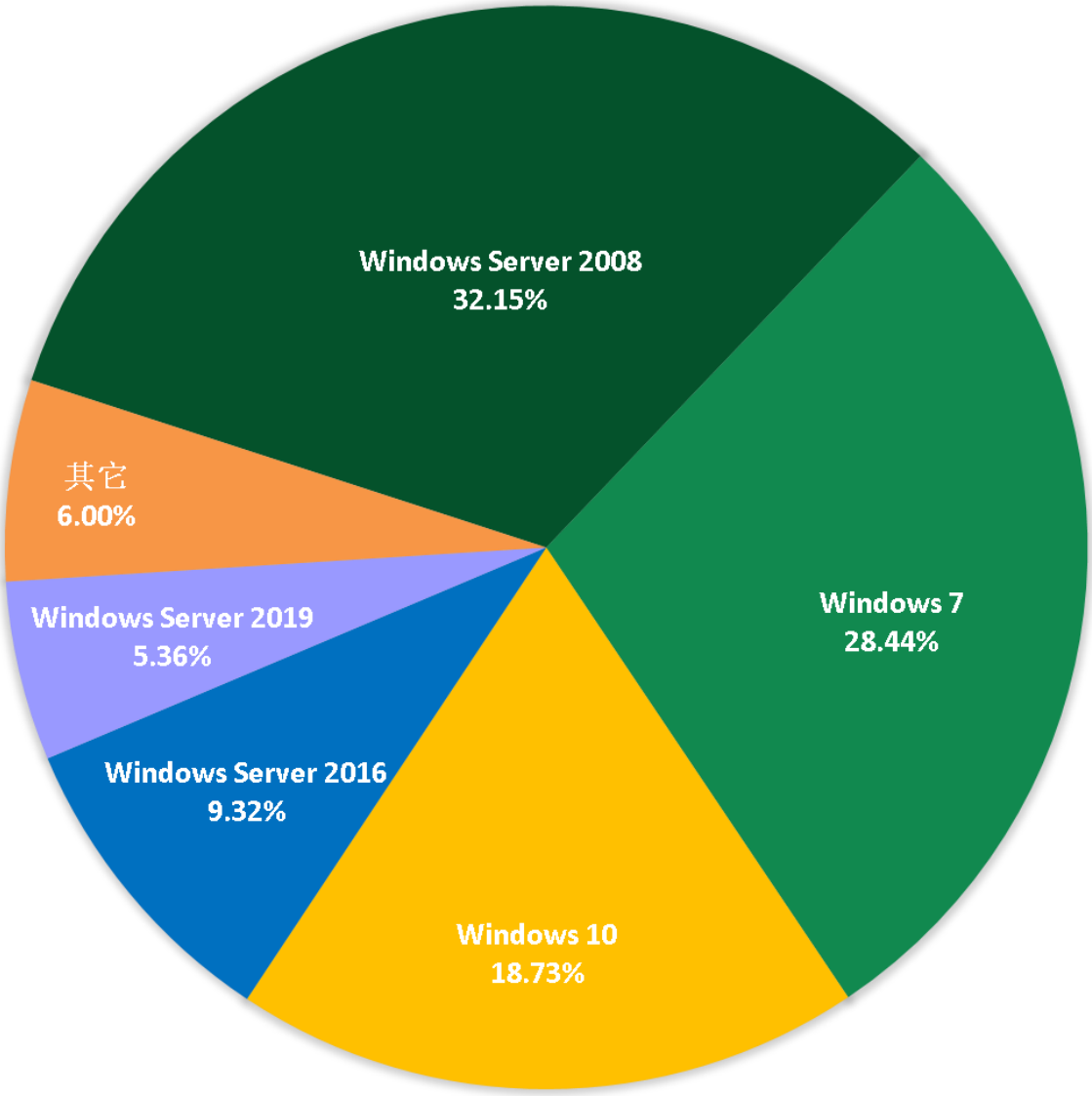


图 6. 2026 年 5 月受攻击系统占比

对 2026 年 5 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。

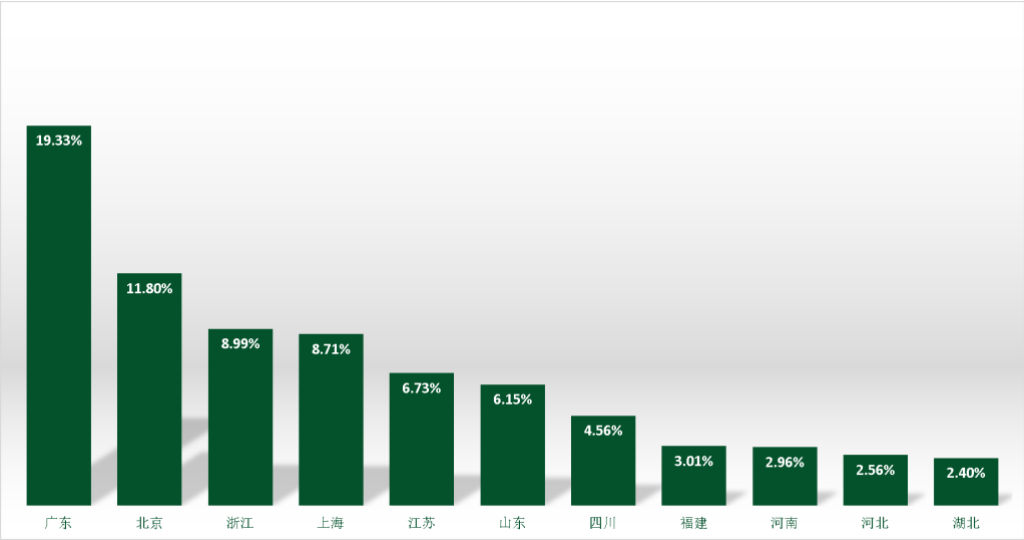


图 7. 2026 年 5 月国内受攻击地区占比排名

通过观察 2026 年 5 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。

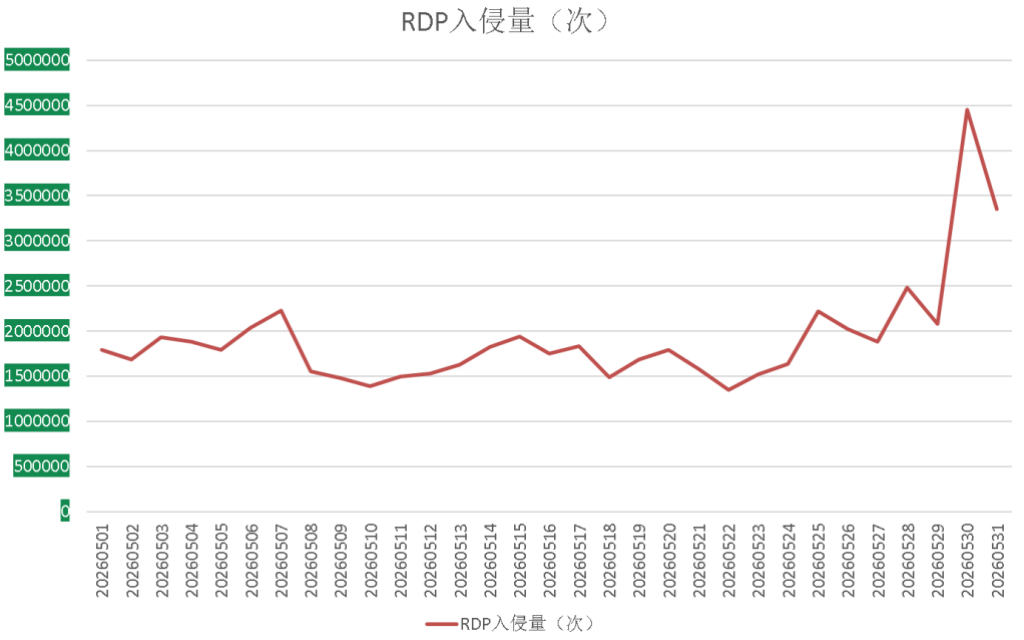


图 8. 2026 年 5 月监控到的 RDP 入侵量

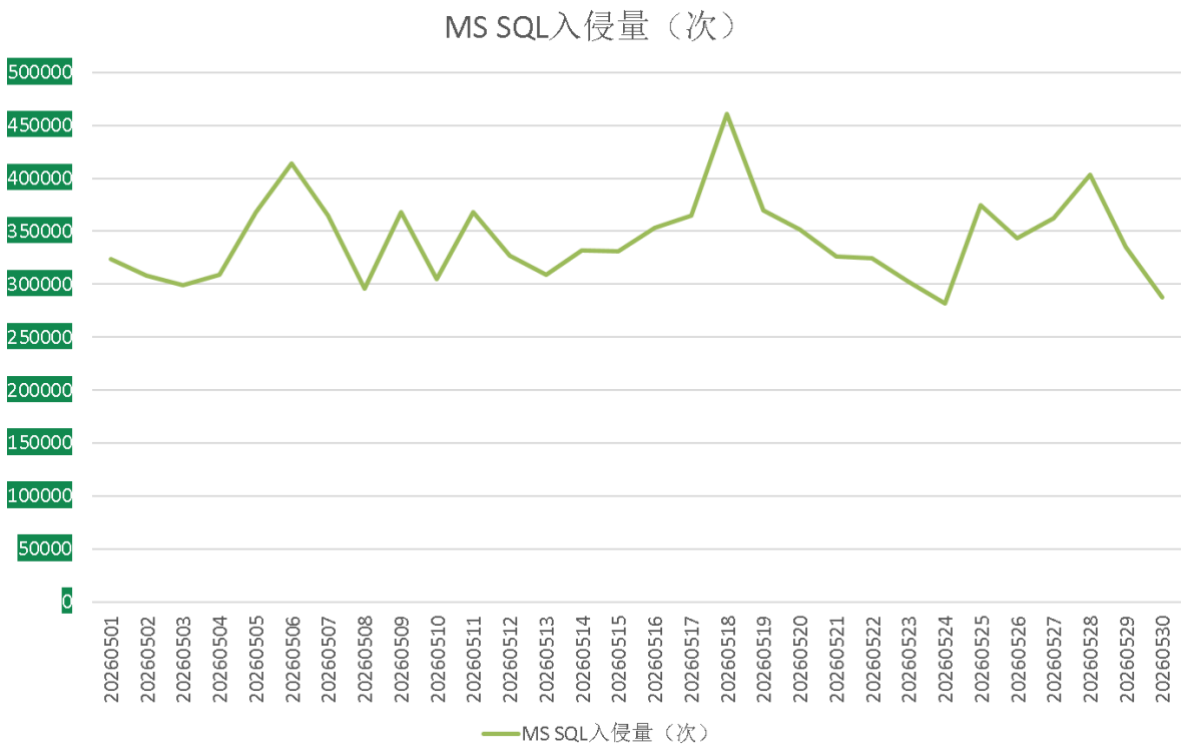


图 9. 2026 年 5 月监控到的 MS SQL 入侵量

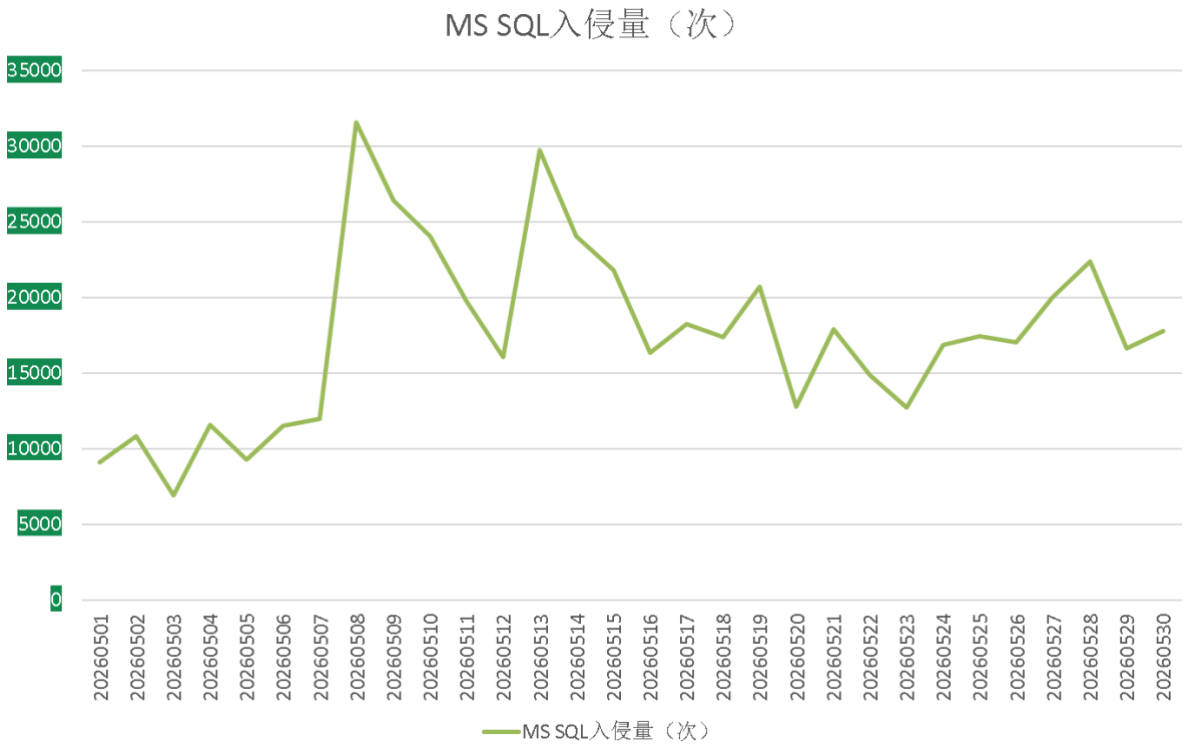


图 10. 2026 年 5 月监控到的 MYSQL 入侵量

# 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

属于 Sorry 勒索软件家族,该家族善于利用各类漏洞发起勒索攻击，同时覆盖 Windows 与 Linux 跨平台环境。

✧ wman

属于 Wmansvcs 家族，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。360 反勒索团队已支持解密。

✧ n83x0bngh

属于 LockBit 家族，攻击方式包括网络钓鱼、僵尸网络、远控投毒、远程桌面暴破登录等。本月主要通过僵尸网络下发投毒。

✧ piz

属于 Pizhon 家族，加密器包含自删除代码。攻击方式主要为远程桌面暴破登录或数据库暴破，登录后植入远控软件进行投毒。

✧ 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。

✧ live

属于 Live 勒索软件家族，已不活跃。相关搜索以安全相关从业者测试为主。

✧ ku13pcxzi

同 n83x0bngh

✧ beaf

属于 Beaf 家族，已不活跃。主要通过远程桌面暴破登录手动投毒。

✧ peng

同 wman

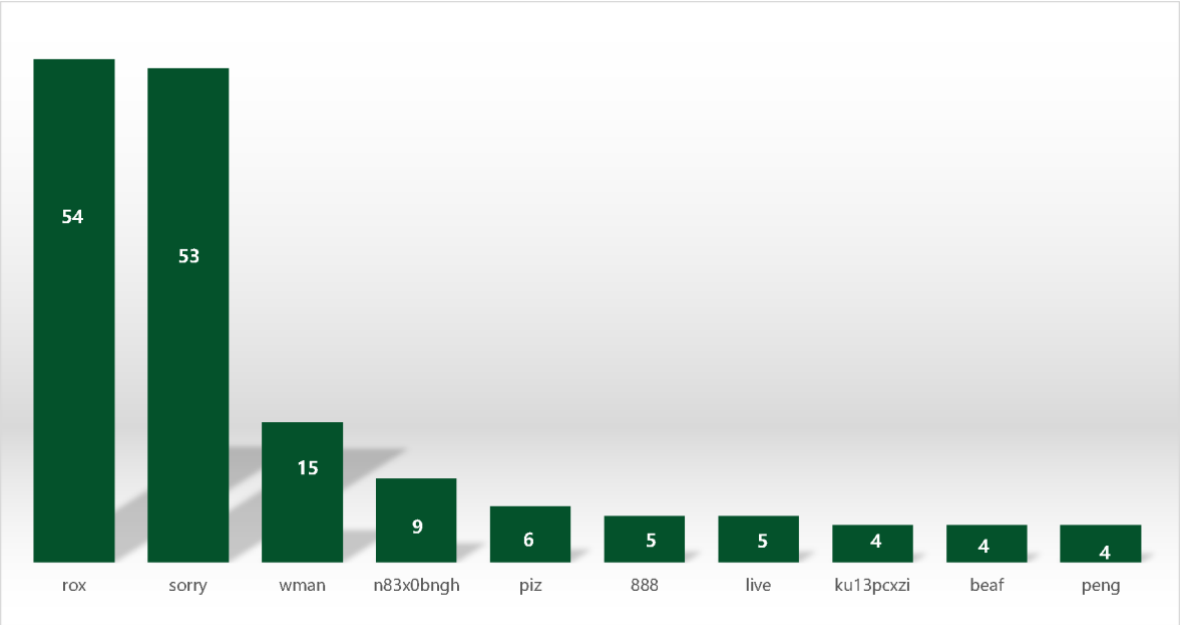


图 11. 2026 年 5 月反病毒搜索引擎关键词搜索排名

# 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 FreeFix。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。

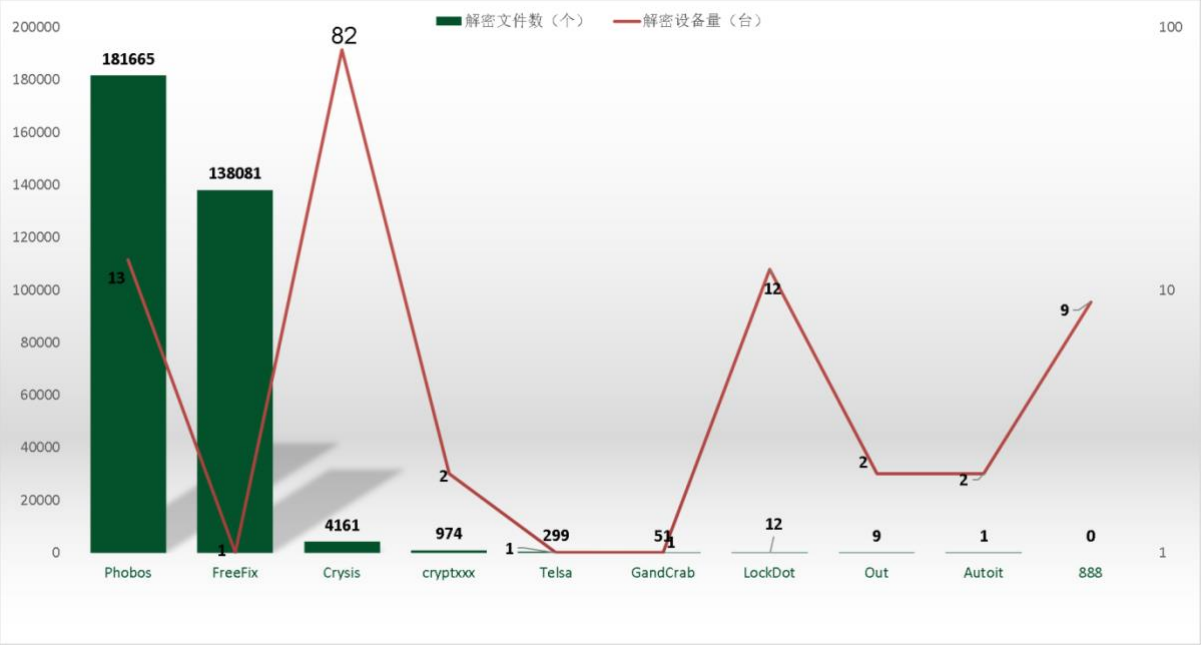


图 12. 2026 年 5 月解密大师解密文件数及设备数排名