

2026 年 4 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 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 4 月，全球新增的双重勒索软件有 HYFLOCK、Audit、TiMc、BlackWater、Aur0ra、M3rx 家族，传统勒索软件家族新增 TorBrowserTor、NBlock、JanaWare 等多个家族。

Sorry 勒索家族本月持续活跃。利用 Web 漏洞在周末时段发起攻击，目标覆盖 Windows 与 Linux 双平台。自 2026 年 3 月首次爆发以来，快速成长为国内的头部高危勒索软件家族。此外，该家族本月新增了对某企业级远控软件的漏洞的大批量利用。360 安全大模型已第一时间捕获相关攻击，并支持拦截。

以下是本月值得关注的部分热点：

- ① 360 成功破解国内顶流勒索软件 Wmansvcs 家族
- ② 360 发布 Sorry 勒索软件分析报告
- ③ Rockstar Games 的被盗数据被敲诈团伙泄露

基于对 360 反勒索服务数据的分析研判，360 数字安全集团高级威胁研究分析中心（CCTGA 勒索软件防范应对工作组成员）发布本报告。

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 61.07%；未正常启用 360 安全软件的设备占比 20%；安装了其他安全软件的设备则占比 18.93%。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。

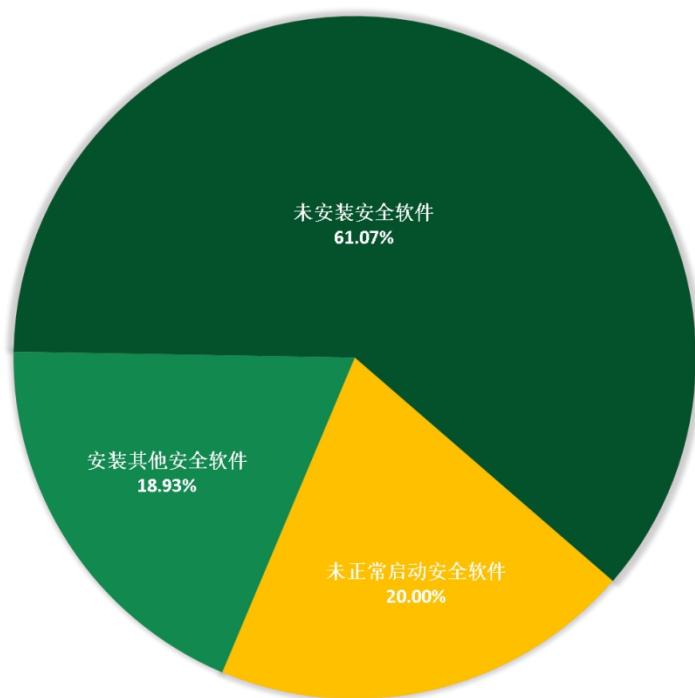


图 1. 2026 年 4 月勒索软件中招设备中安装的安全软件占比

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 25.26% 居首位，第二的是 Wmansvcs，占比 22.68%，Sorry 家族以 20.62% 的占比位居第三。

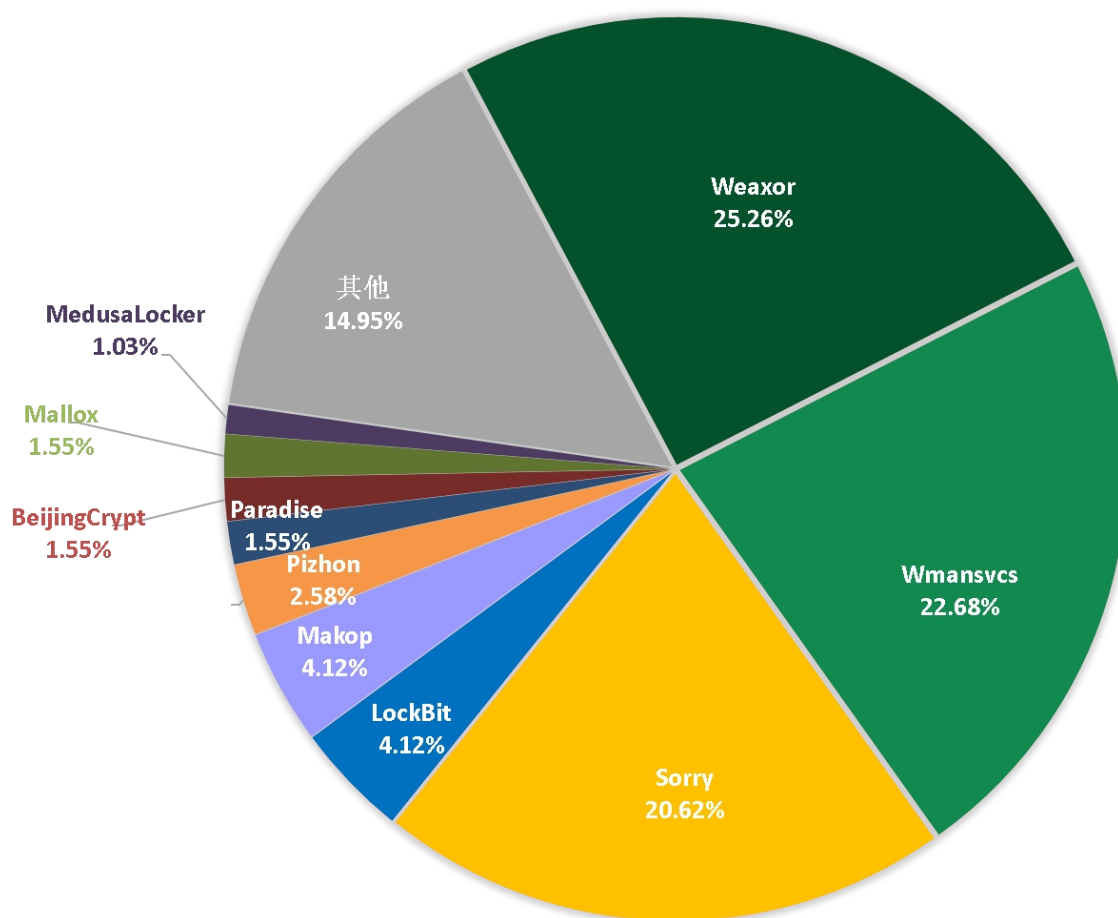


图 2. 2026 年 4 月勒索软件家族占比

对本月受害者所使用的操作系统进行统计，位居前三的是：
Windows 10、Windows Server 2012 以及 Windows Server 2019

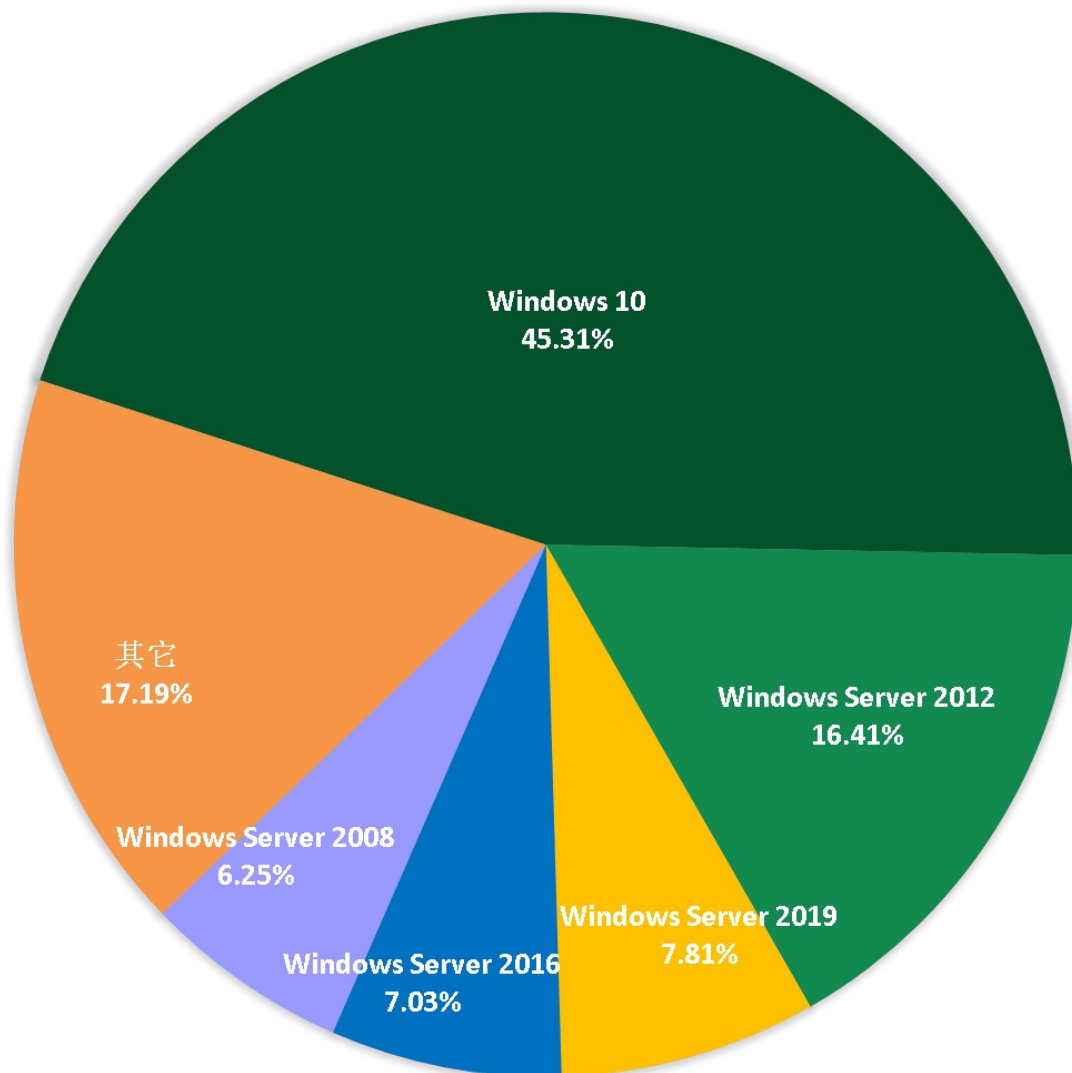


图 3. 2026 年 4 月勒索软件入侵操作系统占比

2026 年 4 月被感染的系统中,桌面系统和服务器系统的占比显示,受攻击的系统类型以桌面 PC 为主, Nas 平台的攻击行为有所增加。

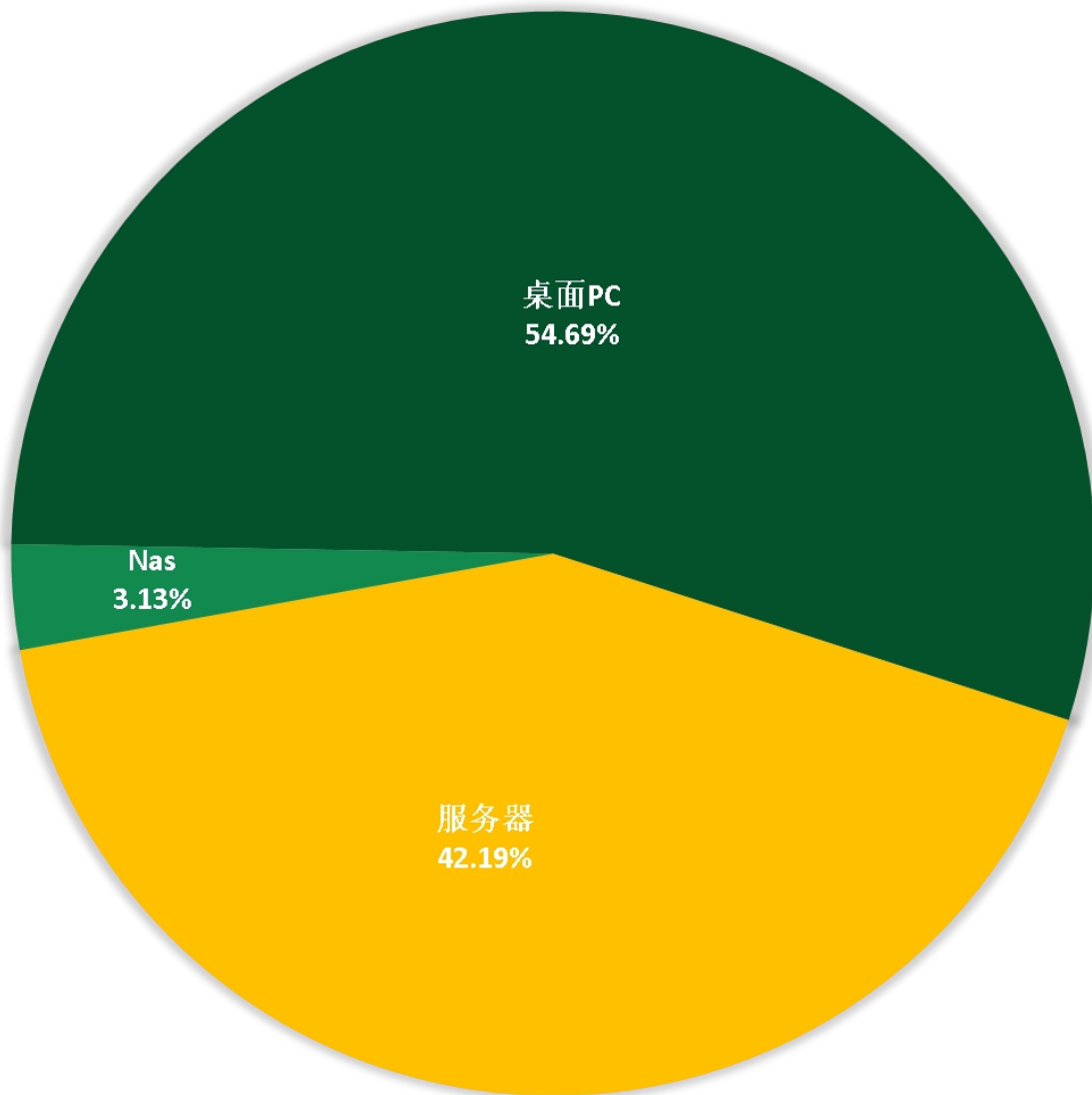


图 4. 2026 年 4 月勒索软件入侵操作系统类型占比

勒索软件热点事件

360 成功破解国内顶流勒索软件 Wmansvcs 家族

自 2025 年 6 月首次现身以来，Wmansvcs 勒索软件便迅速跻身国内最为活跃的勒索软件之一，其感染量更是长期稳居前二。在传播中，该团伙展现出了高度明确的攻击意图。其高度聚焦国内用户，通过远程桌面协议（RDP）弱口令手段，对特定 IP 进行长期定向投毒与横向渗透。该家族目前主要演化出“.peng”与“.wman”两个后缀分支。

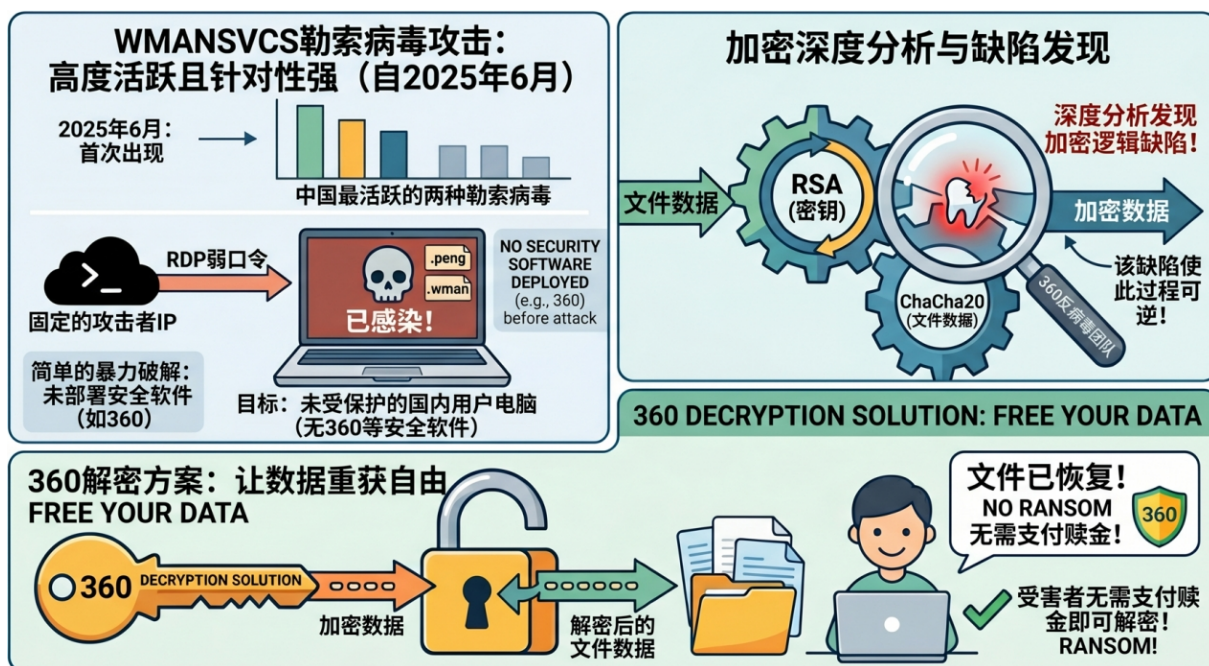


图 5. Wmansvcs 勒索家族已支持解密

360 依托反勒索服务多年的技术积累，成功解密此家族现有全系统变种。目前已经为众多受害者提供免费的技术解密服务。鉴于此家族尚处在活跃期，为了防止灰产中间商不当牟利暂不提供独立工具，并推迟解密方案在 360 解密大师中的集成。

完整分析报告参见：

<https://news.safe.360.cn/n/12998.html>

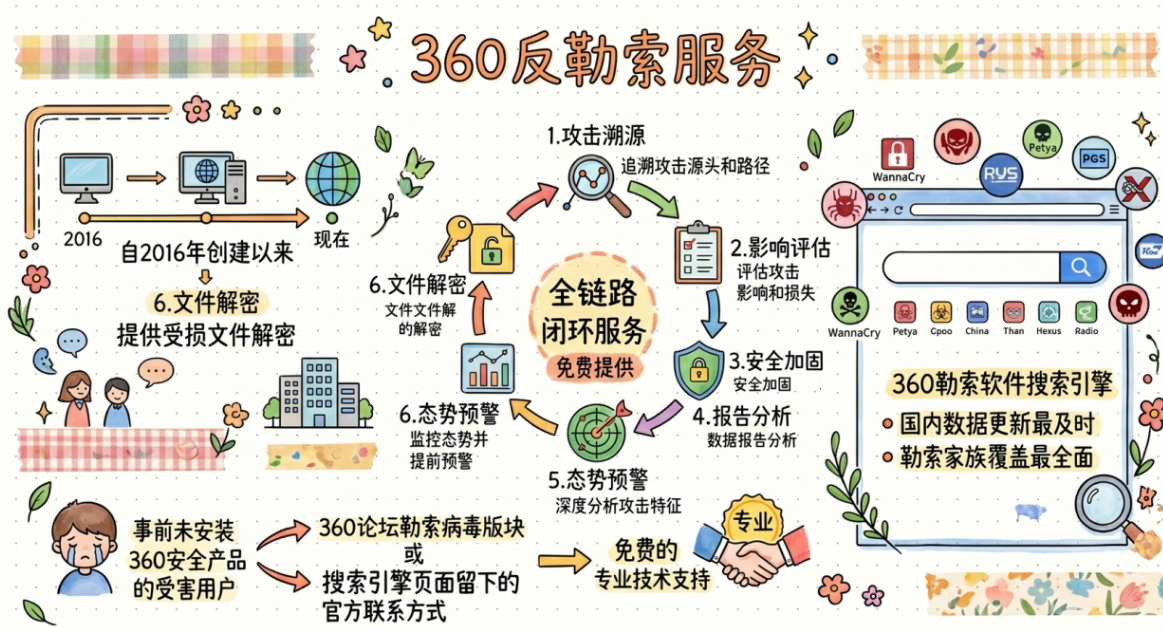


图 6. 360 反勒索服务简介

360 发布 Sorry 勒索软件分析报告

Sorry 勒索软件自今年 3 月现身以来，利用各类常见企业软件漏洞发起攻击，能够远程加载攻击载荷，并展现出跨平台的勒索攻击能力。

本月 360 反勒索团队对这一新晋高危勒索家族进行了深入分析，对该家族在国内投毒活动进行了全面解析，为相关企业快速响应这一新增安全威胁提供了技术指引与参照。

完整分析报告参见：

<https://www.360.cn/n/13006.html>

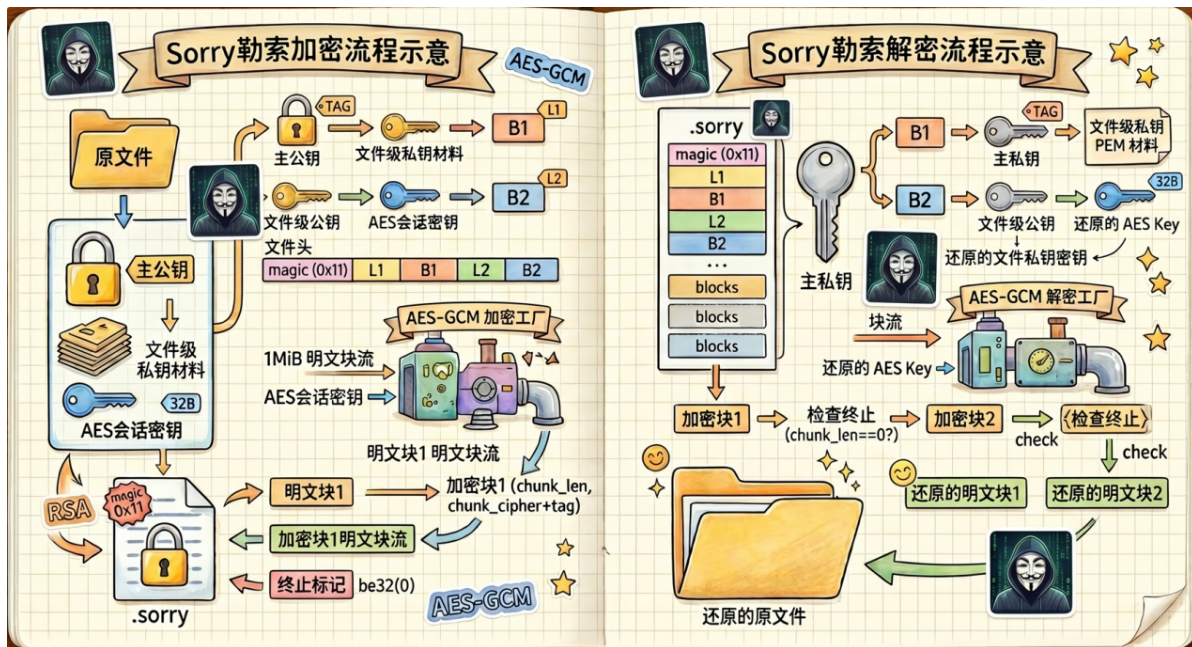


图 7. Sorry 勒索家族流程图示

Rockstar Games 的被盗数据被敲诈团伙泄露

Rockstar Games 因第三方数据分析公司 Anodot 近期的安全事件而遭遇数据泄露，幕后为 ShinyHunters 勒索组织。攻击者称其通过窃取认证令牌，入侵相关 Snowflake 环境，获取并泄露了超过 7860 万条数据记录。目前这些数据已被发布在其泄密网站上。

Rockstar 方面回应称，此次事件仅涉及少量“非关键性公司信息”，不会对公司运营或玩家造成影响。但攻击者表示，泄漏数据主要为内部分析信息，包括用于监控在线服务的指标、客服支持数据，以及《GTA Online》和《荒野大镖客 Online》的收入数据、玩家行为分析和游戏

经济相关内容。此外，数据中还涉及欺诈检测系统及反作弊模型测试信息。

该事件属于更大规模攻击行动的一部分，源头是 Anodot 集成服务被入侵。攻击者利用窃取的认证令牌访问了与之连接的云平台，如 Snowflake、Amazon S3 和 Kinesis 中的客户数据。Snowflake 已确认检测到异常活动，并对受影响账户进行封禁和通知。ShinyHunters 称其通过该手段已窃取数十家公司数据。值得注意的是，Rockstar 此前在 2022 年也曾遭遇与 Lapsus\$ 组织相关的数据泄露事件。

黑客信息披露

本月收集到的黑客邮箱信息如下

| | | |
|-----------------------------|-----------------------------------|--------------------------------|
| GregoryFowler82@outlook.com | prince1990905@gmail.com | standardbankcc@cock.li |
| NeonGPT@Cyberfear.com | dheNwbxZhdfjEw@mailum.com | ncsofficial@usa.com |
| beta-air-com@proton.me | cyberuncle@cyberfear.com | support@3dsservice.com |
| derckader2026@gmail.com | cyberuncle@tuta.io | support@gneeher.com |
| derckader2026@outlook.com | tengunlocker@cyberfear.com | God8Damn@hotmail.com |
| sqlerp@outlook.com | tengunlocker@onionmail.com | zeoticus@protonmail.com |
| Tooll@mailum.com | limeline-team@outlook.com | zeoticus@aol.com |
| Enigma_2@aol.com | rosepipkins@tutanota.com | scammers.zeoticus@tutanota.com |
| thegentlemen@onionmail.org | murphy0401@protonmail.com | spectre_support@protonmail.com |
| thegentlemen@2mail.co | restoreyoursystem23@onionmail.org | lokbt9@onionmail.org |

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）。

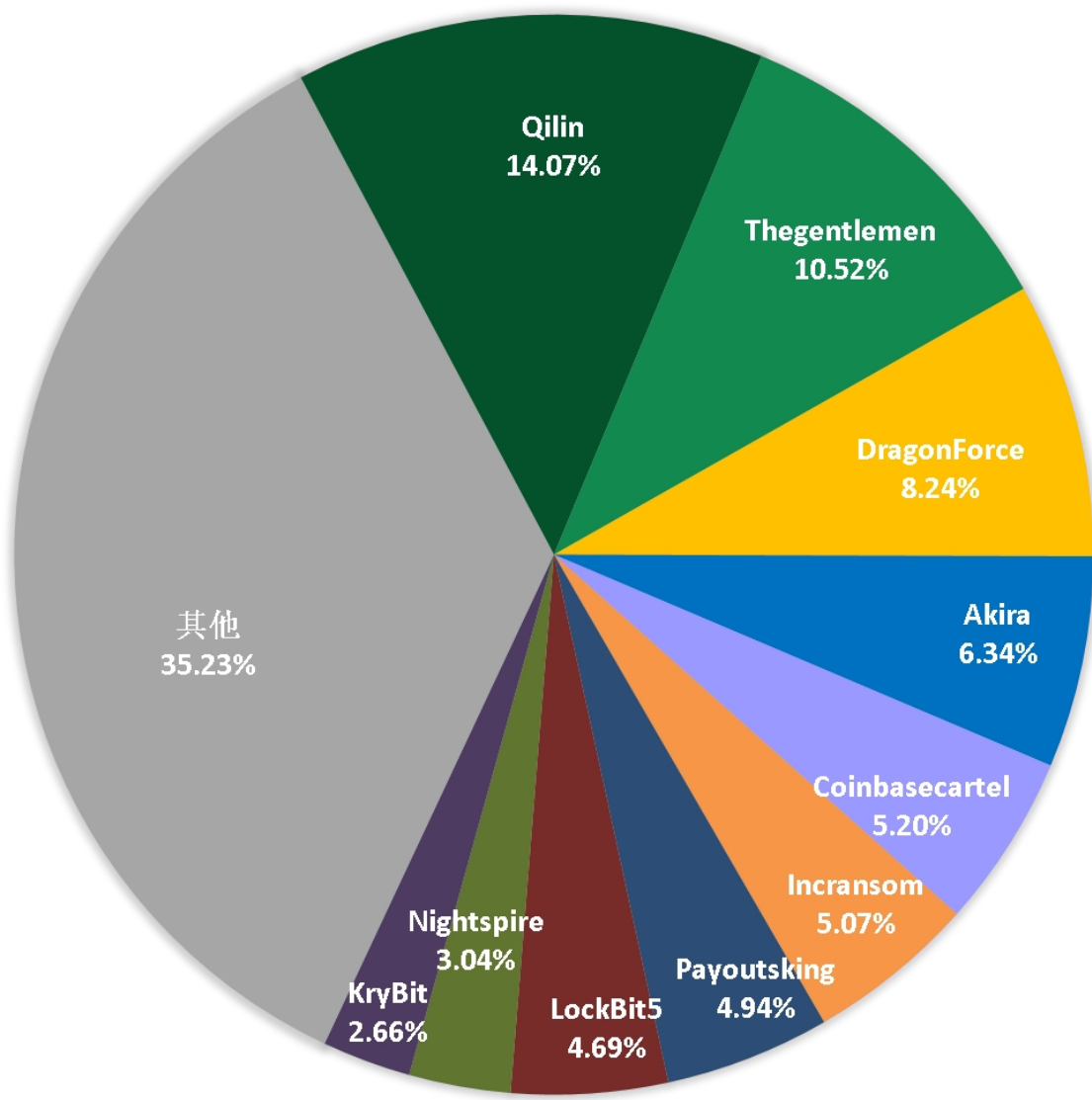


图 8. 2026 年 4 月通过数据泄露获利的勒索软件家族占比

以下是本月被双重勒索软件家族攻击的企业或个人。若未发现数据存在泄露风险的企业或个人也请第一时间自查，做好数据已被泄漏准备，采取补救措施。

本月总共有 789 个组织/企业遭遇双重勒索/多重勒索攻击，其中包含中国 23 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 21 个组织/企业未被标明，因此不在以下表格中。

| | | |
|---|---|---|
| Paramount Health Services & Insurance TPA Pvt. Ltd | Roman Catholic Archdiocese of St John | Alvi Associates |
| The company MST | Samuel I. White, PC | martek co ltd. |
| E-CON Packaging Private Limited | ViaQuest | Goulston & Storrs |
| Heng An Standard Life Insurance | polycorp.com | Kannarr Eye Care |
| Carrera Casting Corp. | Hoeren Gartencenter GmbH | Chalmers & Kubeck |
| Bohmler Einrichtungshaus GmbH | B&e Juice | Guerin Glass |
| TOWERPOINT WEALTH, LLC | ATKINSON RITSON SOLICITORS LIMITED | HIGASHIYAMA INDUSTRIES Co.,Ltd. |
| Follett Software LLC | SafeRain | megasurf.co.za |
| McKay | Nordenta (a daughter company of LIFCO) | Cox, Castle & Nicholson LLP |
| Silfab Solar | rheem | South Florida Injury Centers |
| Zinkan & Barker Development | SIG.biz | Sonn Law Group |
| Apothebeauty | Commscope | TIS |
| MES Hybrid Document Systems | Playmates Toys | Alamo Heights School District |
| The Switch Enterprises | Engie | SAAM Towage |
| See's Candies | SEL (Safety Engineering Laboratory) | Autogalerie Heister |
| Jayeff Construction | JOH Investments Limited | egov.sc |
| Progressive Oral Surgery & Implantology | City'Pro | Siegel Lewitter Malkani |
| Liberty Mutual Insurance | GUEGUEN Avocats | Family Psychological Associates |
| weiss-pm.de | The Go Solution | Powell, Powell & Powell, P.A. |
| Bimtrazer | Cooperativa de Hospitales de Antioquia - COHAN | The McLamb Group, Inc |
| ATF Aerospace | imbrieffamilylaw.com | United Medical Doctors |
| Abazia SpA | Jesin Group | oncologica |
| Reschio | Integra Architecture | Seidor |
| Philex Mining | Better House | Debene S.A. P á g i n a P r i n c i p a l |

| | | |
|------------------------------------|---|--|
| Jgb | Al Sulaiti Law Firm | asunim.co |
| Morae | Nutrabio | ImageMaster |
| Arban & Carosi | Umiles Group | MN Health Insurance Network |
| Caunton Engineering | Complete Aircraft Group | Nan Liu Enterprises |
| V. FRAAS | Tokoparts | Shingle & Gibb Automation |
| Bespoke Home Interior Design Group | Citizens Bank | Sehlmann Fensterbau |
| Vortex Companies | Frost Bank | Newman & Marquez |
| Telia Norge AS | Aman Resorts (aman.com) | Signature Healthcare |
| Prater Engineering Associates | The Canada Life Assurance Company (canadalife.com) | A Roettgers |
| ESENTIA Energy Systems | Pitney Bowes Inc. (pb.com) | Balfour Beatty |
| Del Monte Foods | 7-Eleven, Inc. (7-eleven.com) | KEB |
| UFP Technologies | Carnival Corporation & plc (carnivalcorp.com) | Correios |
| Aero-Coating | Zara (zara.com) | EasTech |
| Peachtree Group | Alert 360 Opco Inc. (alert360.com) | irmler.org |
| Ash & Lacy Holdings | Friktimporten Stockholm | inatech.com |
| Maderas del Alto Urgel | Sgt | nepgroup.com |
| Eyemart Express | SYSTHERM INFO | aviwest.com |
| Sofinter S.p.a | Cosmo Group | ACNHealthcare |
| Grant Production Testing Services | Sunspray Food | Sajet Products |
| Kichler Lighting | Americo Advogados | StrongLink |
| Powell Electronics | CH Express | Network Technology Services of New Jersey |
| Central National Gottesman | Casa Andina | rxm.com.au |
| Florida East Coast Railway | Jati Tinggi | Marlborough Partners - 1 TB data |
| Blanchard | Greenpharma | Scholle IPN - 1.7 TB Data |
| Grace Design Studios | Disk Precision | Idera - 1.5 TB data |
| TESSCO | IC Partners | Mabetex Group |
| Englewood Lab | Marchesi di Barolo | Deaconess Health System |
| Lc Industries | El Ordeno | Frontier Financial Group |
| SCS Engineers | Bmtp | El Ezh Building Contracting LLC |

| | | |
|--|------------------------------------|--|
| Epcn Communities | Laborat ó rio Santa Luzia | Thai Petroleum & Trading Co., Ltd. |
| Data Exchange Corporation | Jumbo Transport | Grupo PyD |
| SunSource | Philip Lee | Ipiranga Cont á bil |
| Color Communications LLC | Jean Cultural | NeoDerm |
| Iowa Spring Manufacturing & Sales | Suma Sklep | INCARFE S. L. |
| Karl Chevrolet | Anderlues | Eric Davis Dental |
| Bentley Capital Ventures | Teleos Systems | Ventilaciones Nerual, S. L. |
| PROM (Peakside Ros Outlet Management) | The Marton Agency | Envy Recycling |
| zsilife.co.zm | The Great Cookie | VINTAGE HOMESTEAD GmbH |
| Advanta Genetics LLC | Nanometrics | Diamond |
| Baresque Group | Henley | ASPShips |
| Cheval Blanc Randheli | ASTM Group | triotech.com.sg |
| Law Offices of Michael A. Freedman, P. A. | HS Technology Group | bkksky.com |
| Atlas Metal Industries Inc | Securitevolfeu | KUKJE PHARM CO.,LTD |
| Costa Solutions, LLC | Altpro | Kawasaki Motors Philippines Corporation |
| Bayou Title, Inc. | McCuaig and associates Engineering | joycity |
| Eduporium | Evict them for me | Aichi Electric |
| Probity Contracting Group | SOGO Auction | Tapon Corona |
| Metro-ILA Funds | rhode-hv.de | Test Rite |
| Edenshaw Developments | Winnitex (Americas) Limited | Ravands Plastech |
| Antica Sartoria | Mag. F ü nder Hausverwaltungs GmbH | Gesvalt |
| planetsport.ma | Strata Republic | DYSA |
| pricon.com.ph | alupco.com | Synergy France |
| instapack.es | Millennium Dental Technologies | Metropolitan Pediatrics |
| stllc.org | bbalawgroup.com | Burning Rock Biotech |
| dmschweiz.ch | firstcambodia.com.kh | Thai Rung Union Car |
| anvilarts.org.uk | cheeky.com.ar | Structures Stucco |
| primeproperties.com.au | abfall-kreis-kassel.de | Thai Special Gas |
| airdriephysio.com | genealogysa.org.au | ACE Consulting Engineers |

| | | |
|--|---|--|
| rainforestclean.com | lynxprecast.co.uk | Optima Servicios Financieros |
| rotak.it | thruwayplumbingservice.com | Hospital del Sur |
| osoftec.com | favellefavco.com | Ciarus |
| boxtopia.co.uk | st-bernards.bham.sch.uk | Mahyco Pvt |
| Mediaworks Kft | putzbaer.berlin | Innovision Holdings |
| fulcrumre.com | Fagen Friedman & Fulfrost LLP | Win Academy |
| nbd3pl.com | treelawoffice.com | DGS |
| Indonesia's Customs Analytics Platform | bgcsnv.org | EMCO Holding |
| cadencepetroleum.com | Qatar Biomedical Research Institute (QBRI) | Adaptavist Group LTD |
| Nephrology Associates | Law Offices of JamesC Shields | Gerald Zisser GmbH |
| Basch & Keegan | Pharmathek | El Wastani Petroleum Company (WASCO) |
| Silicon Alley | R Roesse Contracting | www.bnc.com.ve |
| KarmaData | medicalnetworks CJ GmbH & Co. KG | pacifiwestinjury.com |
| TYLin International Group | HBX Group | Noble Inc. |
| Construction Sciences | GoTip | www.smithdollar.com |
| INJURYLAWYERS.COM | Empower Group | CMD Outsourcing Solutions |
| DIME Distribuidora | Franziskusschule Wilhelmshaven | Research & Planning Consultants |
| Carma Packaging | Marino Food Products Pvt | AnchorsGordon |
| Intikom | Sunlight Express Airways | Bit-Wizards |
| moser-spiel.at | orientalweavers.com | Star Fuels |
| www.durable-tech.com | TFE Group | Accent Dental Center |
| Vimeo, Inc. | Biotechnos | fraper.com |
| Super AI | Harris Beach Murtha | School Health |
| sumacinc.com | FriendlyCare Pharmacy | Adrian Jules |
| Cybersecurity Vendor | Clearwater Marine Aquarium | ARC Dialysis LLC |
| Lifeline PCS | Limkon | Cabinet d' Étude en Sécurité Pyrotechnique |
| Birtcher Anderson & Davis | Uniwersytet Warszawski | Brooklands of Mornington |
| Leone Film Group SpA | S&PGLOBAL, LiteLLM/Trivy campaign (TeamPCP) | academyhealth.org |

| | | |
|--|---|--|
| Floyd Skeren Manukian Langevin, LLP Information | guesty, LITELLM/TRIVY CAMPAIGN (TEAMPCP) | Crystal Point |
| medikaplaza.com | Truckload Carriers Association | Morphosis |
| jpgpetrucci.com | Gruppo ICM SPA | Aqua-Serv© Engineers |
| providentgh.com | UOM University | Gauthier Connectique |
| Promotion AB | Vluznet | AKM Consulting Engineers |
| Stelia North America | Epoch Times | Operinter |
| TokyoHosoKogyo Corporation | Superintendency of territorial planning | Muller Technology |
| ibswebsite.com | GL Steel | Pacific Building Solutions (PBS) |
| delonhampton.com | Wayne Brothers Construction | International Business Solution de México |
| aotco.com | Questivity | fastindustria.com.br |
| wmsopko.com | Millenium Packaging | gas.mercedes-benz.com.eg |
| andrewtjohnson.com | Kemenpppa | abuhatim.com |
| fatbrands.com | Rogiken / institute of Science Tokyo | milanocavi.com |
| mopec.com | La Maison Bleue France | zsfh.cz |
| avalonflooring.com | Sampol | contrar.it |
| gelatissimo.com.au | Astreya | awvgrazerfeld.at |
| rosehillgardens.com | Cognizant | douglasstruckbodies.com |
| massdevelopment.com | CIR Realty | mesto-jemnice.cz |
| Raich Sp. z o.o. | INDESMALLA | mezyietp.com |
| grupo-principal.com | Fletcher Chrysler Products | pegasussrl.com |
| cofaco.com | VOLTERRIES | villa-romane.fr |
| dunav.com | Curtis Design Group | vitropor.pt |
| BELFOR | McCOR | defcon5italy.com |
| Selex - Gruppo Commerciale | bela - pharm | vitexpharma.com |
| algoaibi-gtb.com | Flash Charm INC - (IDERA) | seleniaravenna.it |
| alx-pc.com | Stonehenge | aplast.ro |
| arrawdah.org.sa | LACROIX | shunhinggroup.com |
| ldisolutions.com | Gastroenterology & Hepatology of CNY | earthprotect.co.jp |
| Inspira | Apply Capnor | wibeats.it |

| | | |
|--|------------------------------|---------------------------------|
| Rural Municipality of Gimli | D-Troy Logistics | Aculab |
| RT Software | coastappliances.com | Tesla Systems |
| Narteks Tekstil A.S | itc-group.com | CCCKeito.edu.hk |
| MTCI | tremcar.com | Carmelo Candy Inc |
| reddycardiology.com | imadesign.com | M&K Foam Koło |
| Synmosa Biopharma | advprograms.com | Pemerintah Kabupaten Bojonegoro |
| Longwood Engineering Company | novafp.com | Innovision Holdings |
| A & A Building Material | ppiplastics.com | AXCERA.IO |
| Exclusive Networks | je-nyc.com | UNIV LILLE |
| Istarpal | breslinbuilders.com | ASTRAZENECA CORP |
| Walman Optical | tulsachamber.com | VirtaHealth |
| EEC Group | CSA SpA | AIRCOS |
| Coralina | La Tuilerie | Zanzi |
| Lawson Software | milliondollarbabyco.com | Das Labor |
| Suzhou Yike Kejian | graphicinfo.com | GCA Professional |
| bladex.com | gtlcompany.com | GCA Group |
| heinrichs-logistic.de | asesoriauriel.com | Gaposa |
| merlo.de | unipest.co.th | alloha.com |
| CHECKMARX | palladium.gen.tr | Medici Group |
| Chase Cooper Limited (RiskLogix Solutions) | secran.com.br | Terminal 21 |
| Apple Film Group | ServiceMaster Clean services | UCPS |
| LA Woodworks | BK Tomorrow | Dreamtoy |
| Buckley Powder | R L Larson Excavating | Zamek Namest |
| Cahbo Produkter | WEDA ROBOTICS | Equity Life |
| Leistritz Turbine Technology | comunidadandina.org | jrk.com |
| Dillon Family Medicine | fondonorma.org.ve | Siam Okamura International Co |
| KEMBA Indianapolis Credit Union | cegasa.com | AUG Pharma |
| SanCor | nucleodiagnostico.mx | Vietnam Fortress Tools JSC |
| First County FCU | marti.do | Barnes Solicitors LLP |

| | | |
|---|--------------------------------------|---|
| Chelten House | decatordiagnosticlab.net | Sokolin |
| Woodfields Consultants | PsychPlus | G Plants |
| Travel Expert | UK Electronics | EMCO Electric International |
| Mid Florida Dermatology & Plastic Surgery | Intra | Kopran |
| Swansea Ambulance Corps | GEM Terminal | Shine Aviation |
| Malaysian NPK Fertilizer Sdn. Bhd | Brand Collective | lkc.ac.bw |
| krauseundco | Cleor | Community Connections |
| Point Four EPoS Solutions | Harlem Stage | Advanced Vehicle Assemblies |
| Denso | International Maritime Hospita | coronapa.com |
| Marc Cain | Double C Farm | Infonet Media d.o.o. |
| Progressive Propane | BRC Biotechnology | BJ Grupo |
| Priests for Life | NSOFT | kramer-nsc.at |
| Flipo Group | Verzinkerei Rentrop | whiskey.co.jp |
| Grupo ABC | Hangzhou Industrial | Jordan India Fertilizer Company |
| METO Systems | Caja De Seguro Social | Harman Fitness |
| tlctrialteam.com | Asaniverko | Nippon Medical School Musashi Kosugi Hospital |
| Rockville Fuel & Feed | Ultimate Metals | Shiraume Hospital |
| Star Energy Geothermal Salak | JM Bozeman Enterprises | GEG Telecomunicazioni |
| Dorotea Sweden | Indigo Group | Seoyon E-Hwa Summit |
| Lessard Dental | Richmond Plywood Corporation Limited | BERGE-BAU GmbH & Co. KG |
| Udemy, Inc. (udemy.com) | Mike Brandner Law | Bo.. and Br..e |
| ADT, Inc. (adt.com) | GRUPO RONDA | Westamerica Communications |
| Chartwell Law | IPARBILBAO ABOGADOS - ROCA JUNYENT | Charles River Insurance |
| Mother's Market & Kitchen | cwwcontractors.com | Community College of Beaver County |
| B to B Visions | Jersey Fabrication Group LLC | Woodland Trade |
| Manulife Wealth | sentrydynamics.com | American Vintage Home |
| The FAFS | Gauthier Tissus | Southeastern Conference of Seventh-day Adventists |
| Clearview Intelligence | CNAOC | Dubosson Fr è res SA |
| City of Napoleon, Ohio | FILAIR | Siena Construction |

| | | |
|---------------------------------------|---|--|
| Peroni Sosa Tellechea Burt & Narvaja | Beaver Engineering | PARS AR-GE |
| meditron.com.ve | ClientSolution EFO Service Srl Logitech Srl Safety | Neptune Mechanical, Inc. |
| b3-bruck.at | Servetto Srl | TTAF Defense |
| caravaningcity.com | International Assistance Sdn | Association OCACIA |
| Alkegen | The Seacare Hotel | roodtrucking.com |
| 1st Solution CTC | Pullen Moving | Berning & Söhne GmbH |
| Gumpp Kunststoffe | Colorado Pulmonary Intensivists | Piet Vijverberg |
| Virginia Health Services | J Brand | artmotion.net |
| Kementerian Pertanian | PGDIS. PAPETIQUE PRO | asseco-ce.com |
| Sea Telecom Br | Alternativa de Moda SAS | Asmar Schor & McKenna |
| Precision Coating | Frutcola Olmu é | United Finance Egypt |
| Integer Holdings | Basalt Dentistry | Tscherne Consulting Steuerberatung GmbH |
| Sanna Web | Colonial Presbyterian Church | Faulkner County Sheriff's Office |
| Peru LNG (Hunt LNG Operating Company) | Herth+Buss | Wolf Technology Group |
| Aptim | Despr é s Mé canique Mobile | VLawyers |
| SmartSystems | Northeast Missouri Rural Telephone | project1631.com |
| Champion Homes | T. t Ste. .ius & Ho. i. ter LLP | National Aerospace Fasteners |
| Euro Creations | ifmis.go.ke | singita.com |
| Uniview Technologies | whessoe.com.my | cesimaging.com |
| Tractial | olpro.com.my | Serap |
| Marnell Financial Services | DeMera DeMera Cameron | The Center for Hearing & Speech |
| trugreen.com | phb.com | jbrand.co.uk |
| teamster773.org | edtg.com | acmealliance.com |
| Jackson Lewis | Travel of America | northstarmetal.com |
| INCYTE | Lift | kleankanteen.com |
| Gregory Jewellers | rudolf-med.com | bunch.ca |
| alexandergroup.com | www.sistemigestioneintegrata.eu | sutex.com |
| krwlawyers.com | Transaction Packing Inc | Katcon Global |
| S4K Entertainment | K Subsea Group | Industrias Guerra, S.A. |

| | | |
|---|---|---|
| Kubiak Melton & Associates | bdac.com.au | fhw-neukoelln.de |
| Equatorial Coca-Cola Bottling | Affordable Oil | greenwayfence.com |
| studiopiu.net | Helzberg | congoleum.com |
| murni.co.id | Ralph Lauren | atpkg.com |
| bardehle.com | Carters | TouchSource |
| erstransportes.com.br | dencom.co.nz | irpea.it |
| The Galliher Law Firm | Straten & Kollegen | Ph..s |
| Primius Law Firm | medical-park | Neurologic Associates Of Central Brevard |
| PremCom | Rockstar Games | CHEK News |
| Rutan & Tucker, LLP | Abrigo, Inc. | jursaconsulting |
| K2 Electric, Inc | Marcus & Millichap, Inc. | Die Linke |
| Kolin Turkey | Kemper Corporation | Fountain |
| Sea Air International Forwarders | Ryan, LLC. | Elara Engineering |
| Huonker GmbH | McGraw Hill, Inc. (mheducation.com) | blossmangas.com |
| PTS Office Systems | National Railroad Passenger Corporation (amtrak.com) | Lincoln Property LLC |
| Industrial Carrocera Arbuciense | Mytheresa | State Road and Tollway Authority |
| Heartland Steel Products | mastercom.com.au | Swagelok |
| Jiangsu Zenergy Battery Technologies Group Co., Ltd. | morgancountyga.gov | Builrite |
| Ferguson Timar | Sahara Air Products | Plunkett Cooney |
| Safety Engineering Laboratories | conrepsa.ro | AMBAU Personalservice |
| ruskcountywi.us | www.campbell.edu | Alamo Heights School District |
| Avitrans | Hofland | First Trinity Financial |
| STERIMED | Peuker & Alexander | Tange , Mann & Garza |
| Salimetrics | Sadtek | Starr Insurance |
| Alva Manufacturing | wright-ryan.com | SAYEGH |
| MAC Construction & Excavating | T..t Ste..ius & Ho..ter LLP | Alliance Roofing |
| GGI | Turbo International | Publishers Clearing House |
| Arctic Home Living | Arkansas Oral & Maxillofacial Surgeons | Notre-Dame du Grandchamp |

| | | |
|-------------------------------------|------------------------------|----------------|
| CHARLES CONSEIL COORDINATION (3CCC) | Colonial Presbyterian Church | Ghazi Brothers |
| Champion Homes | Netgain Networks | The GMP 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 Server 2008、Windows 7 以及 Windows 10。

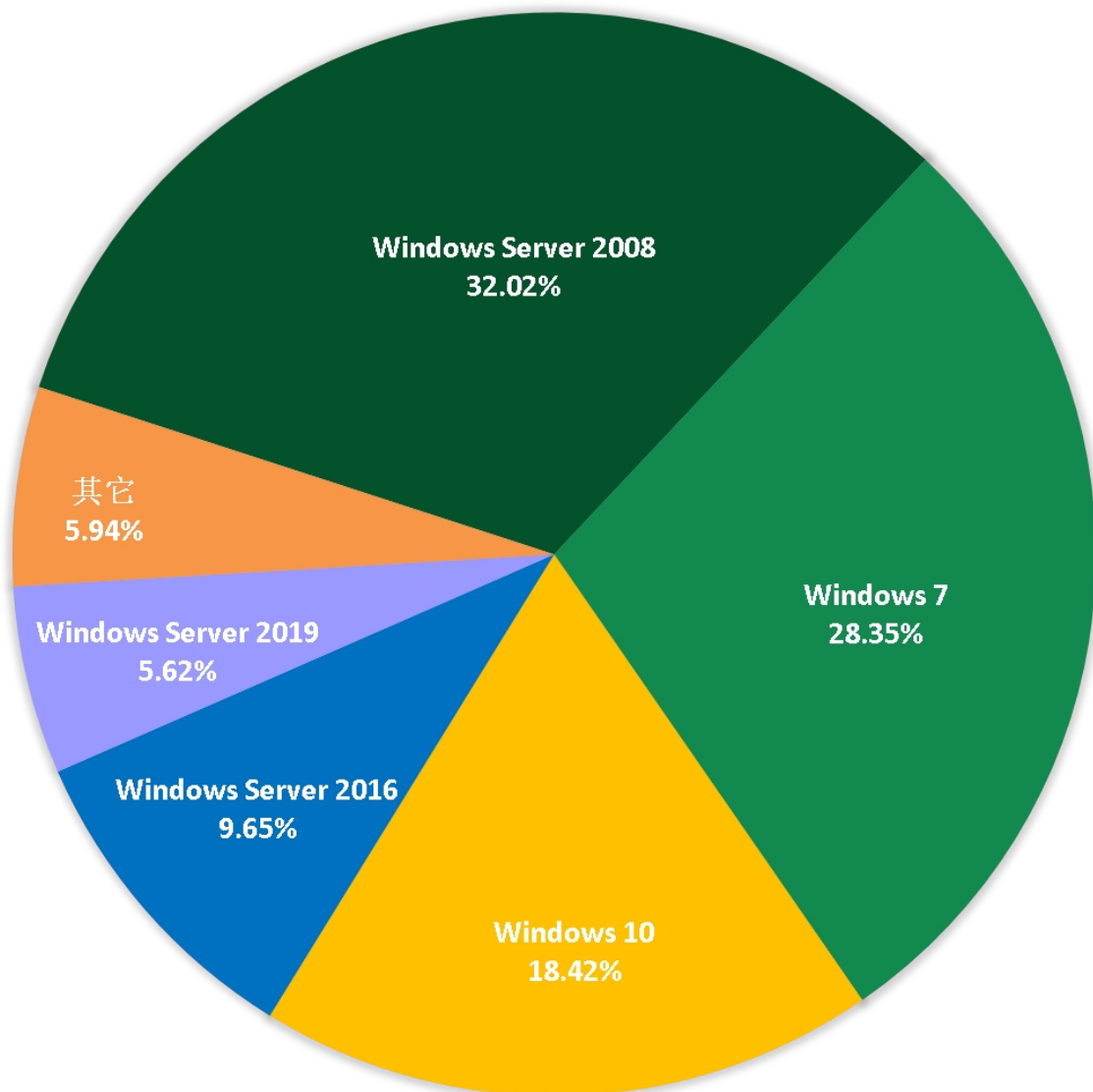


图 9. 2026 年 4 月受攻击系统占比

对 2026 年 4 月被攻击系统所属地域统计发现，与之前几个月采集

到的数据进行对比，地区排名和占比变化均不大。数字经济发达地区仍是受攻击的主要对象。

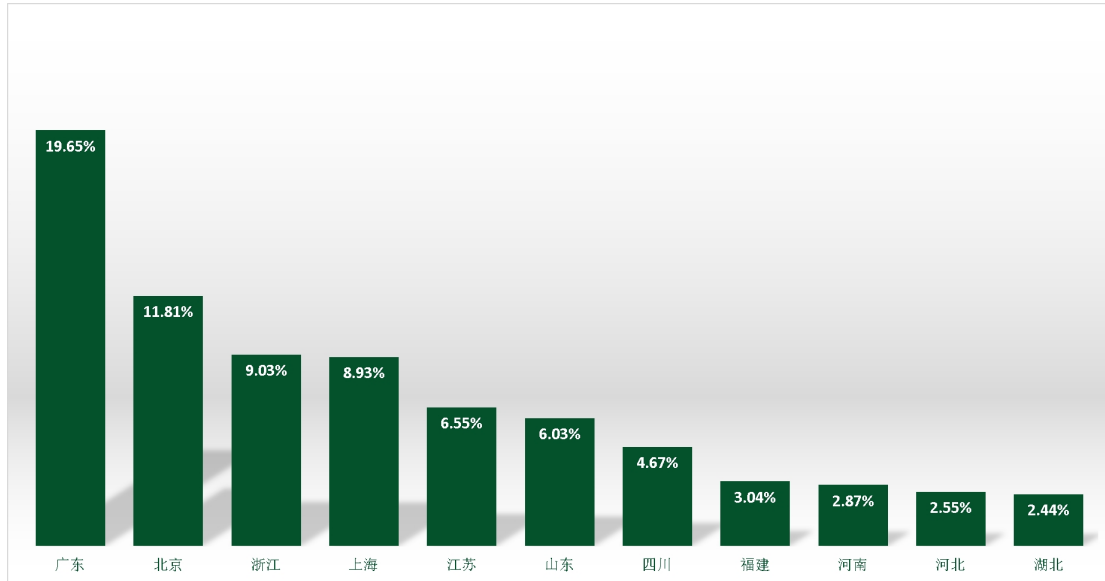


图 10. 2026 年 4 月国内受攻击地区占比排名

通过观察 2026 年 4 月弱口令攻击态势发现,RDP 弱口令攻击、MYSQL 弱口令攻击和 MSSQL 弱口令攻击整体无较大波动。

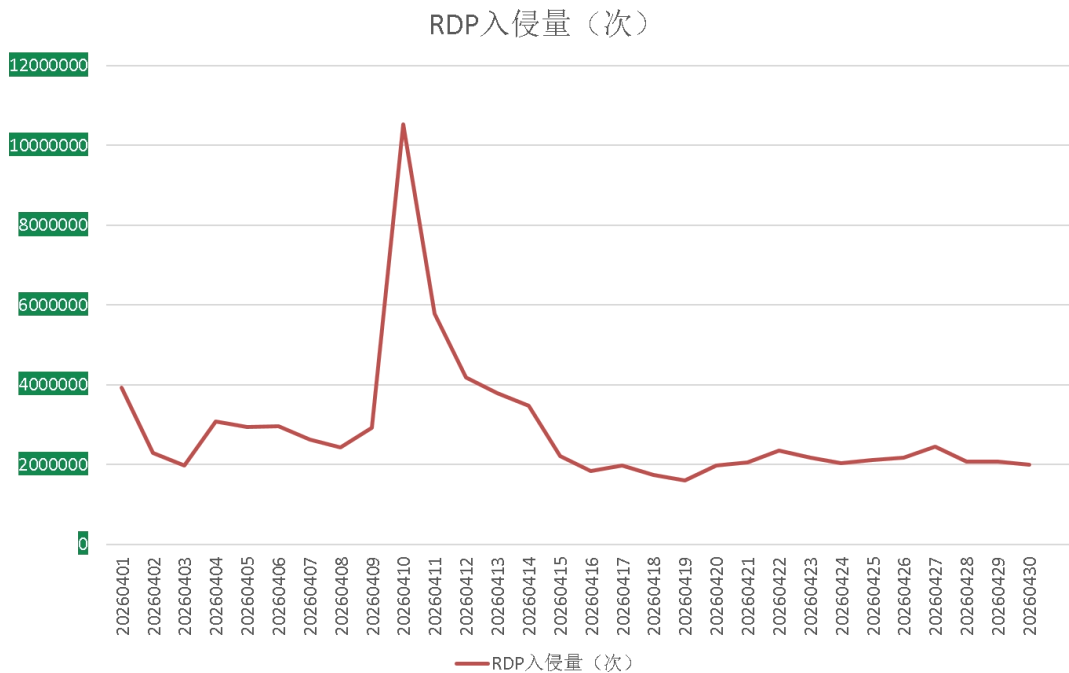


图 11. 2026 年 4 月监控到的 RDP 入侵量

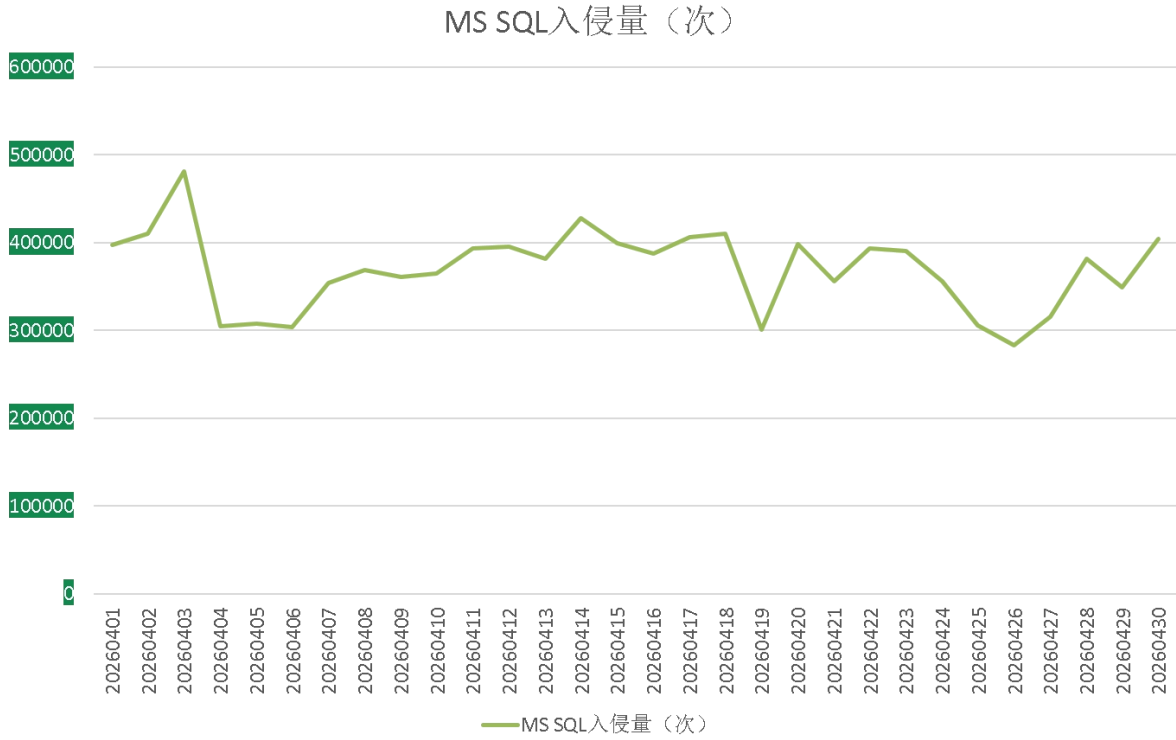


图 12. 2026 年 4 月监控到的 MS SQL 入侵量

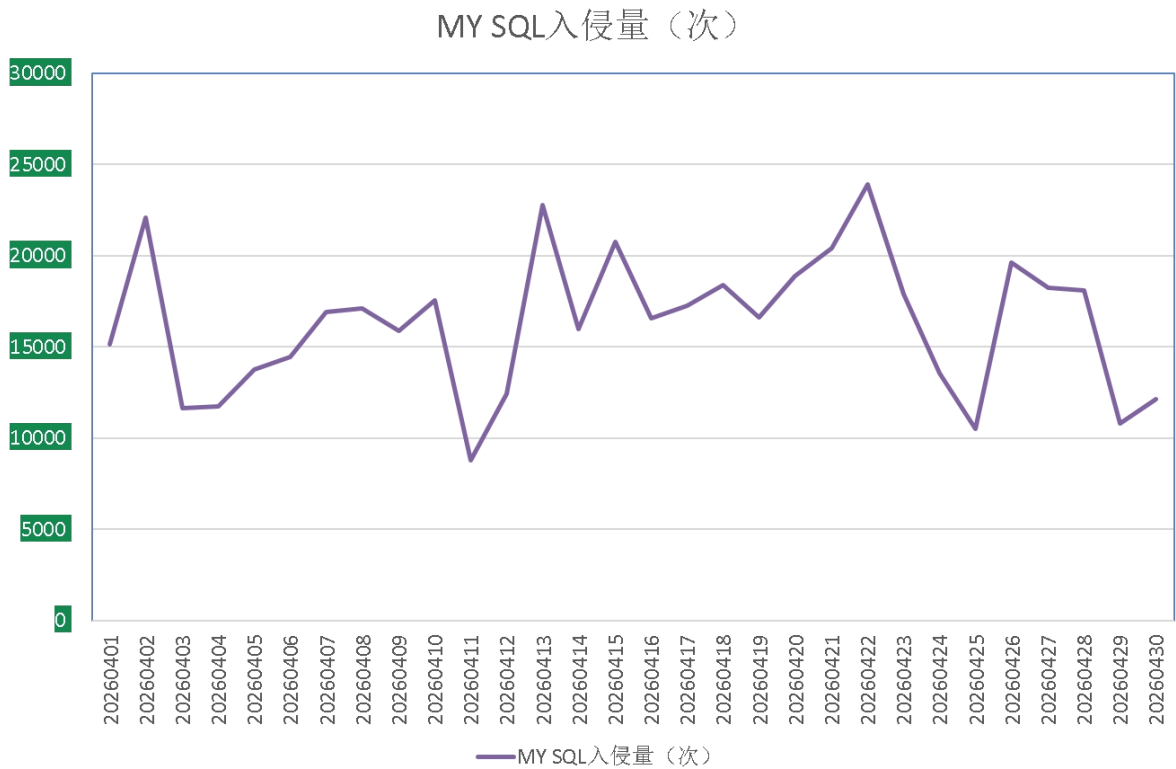


图 13. 2026 年 4 月监控到的 MYSQL 入侵量

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。

◇ 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。

◇ 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。

◇ 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。

◇ bixi

属于 BeijingCrypt 勒索软件家族，由于被加密文件后缀会被修改为 beijing 而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令与数据库弱口令成功后手动投毒。

✧ **baxia**

同 bixi。

✧ **snowsoul**

属于 SnowSoul 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 Web 漏洞进行投毒。

✧ **weaxor**

同 rox。

✧ **mallox**

属于 TargetCompany (Mallox) 勒索软件家族，由于被加密文件后缀会被修改为 mallox 而成为关键词。主要通过暴力破解远程桌面口令成功后手动投毒和 SQLGlobeImposter 渠道进行传播，后来增加了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。

✧ **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。

✧ backups

属于 Proton 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。

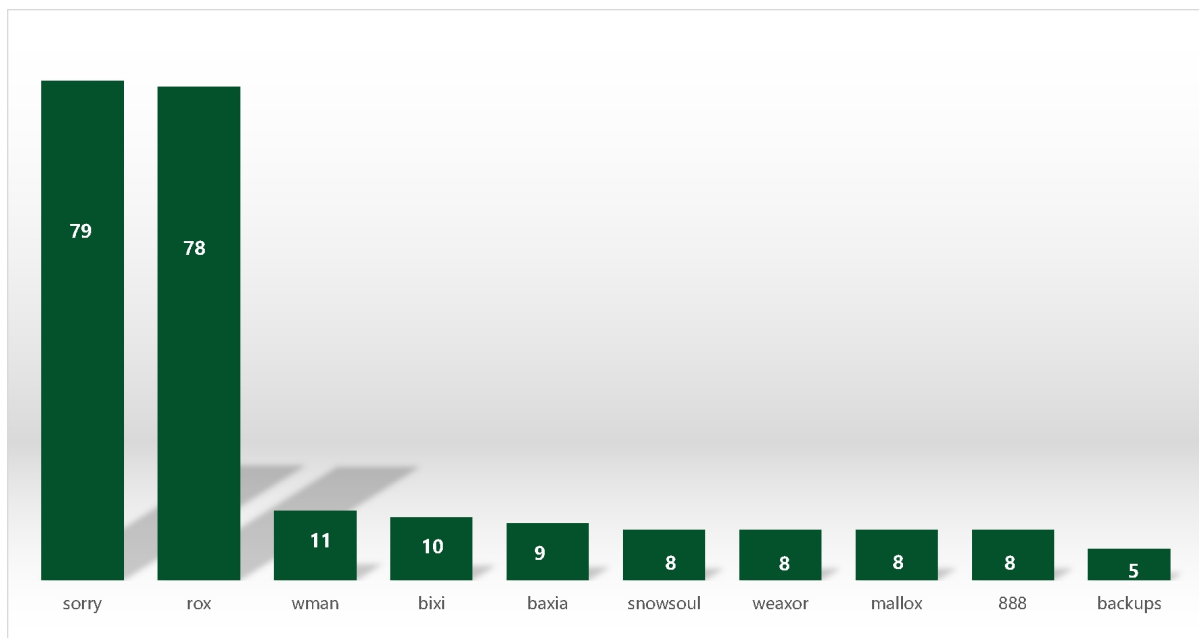


图 14. 2026 年 4 月反病毒搜索引擎关键词搜索排名

解密大师

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

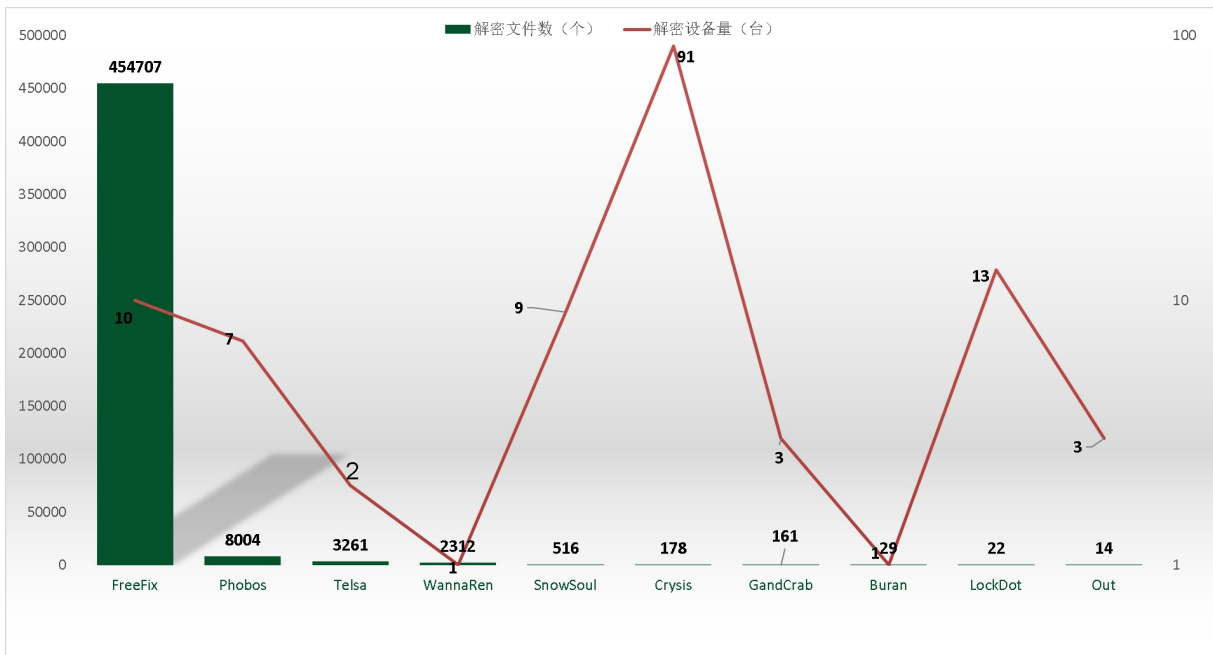


图 15. 2026 年 4 月解密大师解密文件数及设备数排名