

勒索软件流行态势分析

2025 年 5 月



三六零数字安全科技集团 | 高级威胁研究分析中心

勒索软件传播至今，360 反勒索服务已累计接收到数万次勒索软件感染求助。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上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，危害也越来越大。360 全网安全大脑针对勒索软件进行了全方位监测与防御，为需要帮助用户提供 360 反勒索服务。

2025 年 5 月，全球新增的双重勒索软件有 J、Datacarry、Worldleaks 等多个新增家族。传统勒索软件家族新增 Bert、Kalxat 家族。

本月 360 反勒索服务团队接到数起关于 Kalxat 勒索软件攻击的反馈。经分析发现，这种新型勒索软件拥有非常高效的文件加密机制，并可以多级动态调整加密策略，具备大量配置与扩展属性，属于新一代的先进勒索软件。根据受害者反馈，Kalxat 会在系统中悄然加密各类文件，并将其扩展名修改为“.kalxat”，同时留下勒索信息，要求支付赎金以获取解密工具。

在入侵传播方面，Kalxat 则表现出了明显的定向攻击特征。该勒索软件主要针对 Windows 服务器发起攻击。其加密策略也是针对服务器上的关键数据——如数据库文件，进行完整的全量加密。而对于其他非关键文件，其采用部分加密策略，以加快整体加密速度。此外，该勒索软件还会执行一系列系统操作，包括大量修改注册表项、禁用 Windows Defender、清除系统事件日志和安全日志等，以规避安全检测并确保攻击成功。

Kalxat 采用了高度模块化设计：勒索信内容、加密文件扩展名、RSA 公钥等关键参数，均通过独立的配置文件进行配置。这也使攻击者可以轻松地为不同目标定制不同版本进行攻击，同时也增加了安全研究人员的分析难度。这种设计使得 Kalxat 具有较强的变种生成能力，各个攻击实例可能展现出不同的行为特征，并且采用了双重 RSA 架构。这些操作表明，Kalxat 是一款精心设计的、针对企业服务器环境的高级勒索软件。

以下是本月值得关注的部分热点：

- 1** VanHelsing 勒索软件生成器在黑客论坛上泄露
- 2** 员工监控软件 Kickidler 在勒索攻击中被利用
- 3** 勒索软件团伙越来越多地利用 Skitnet 投放恶意软件

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。

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：Weaxor 家族占比 28.27%居首位，第二的是 RNTC 占比 16.23%，BeijingCrypt 家族以 10.47%占比位居第三。

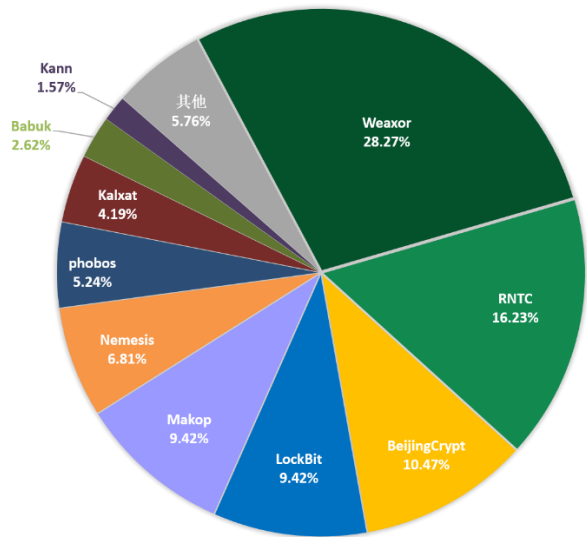


图 1. 2025 年 5 月勒索软件家族占比

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 Server 2012 以及 Windows 11。

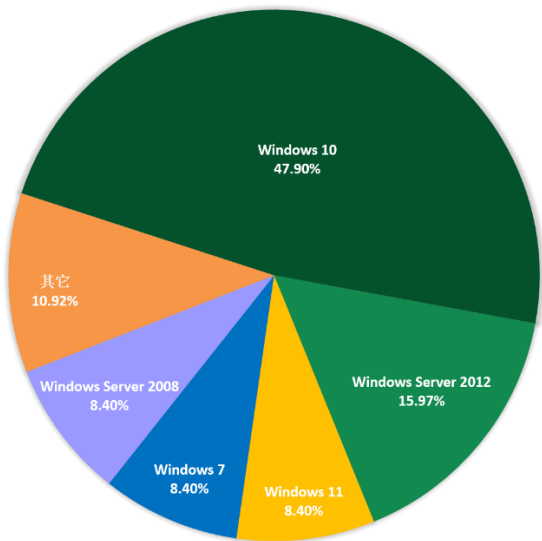


图 2. 2025 年 5 月勒索软件入侵操作系统占比

2025 年 5 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。

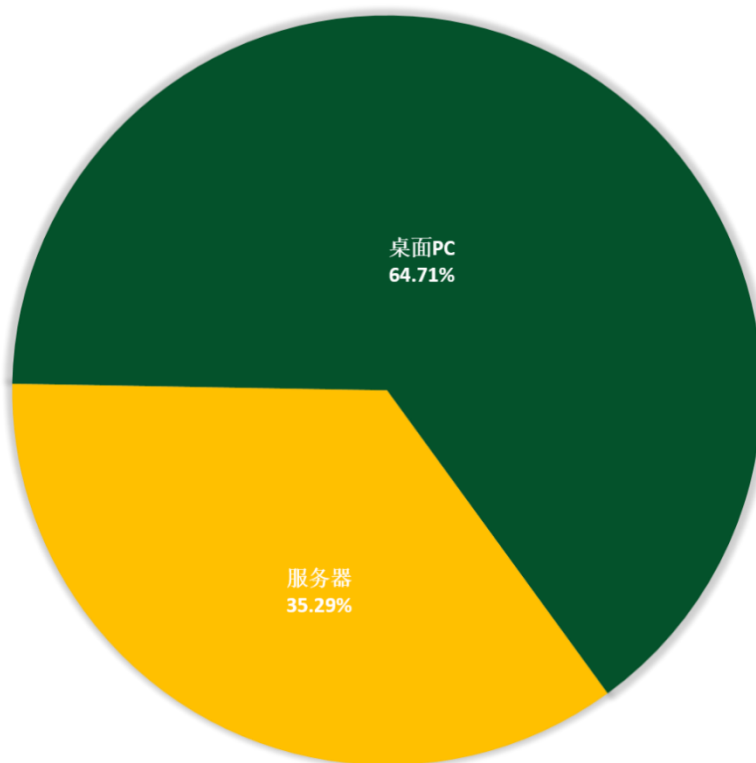


图 3. 2025 年 5 月勒索软件入侵操作系统类型占比

勒索软件热点事件

VanHelsing 勒索软件生成器在黑客论坛上泄露

2025 年 5 月 20 日，一个别名为“th30c0der”的用户在 RAMP 论坛上提出以 10,000 美元的价格出售 VanHelsing 的源代码，并公布了对“TOR 密钥+管理员的 Web 面板+聊天+文件服务器+博客包括数据库所有内容”的全面访问权限。该卖家还详细介绍了勒索软件的多平台功能，声称可以针对 Windows、Linux、NAS 系统以及 2.0 到 8.0 版的 ESXi 环境进行勒索。

作为回应，VanHelsing 官方运营商发布了部分源代码，声称 th30c0der 是“开发团队的老成员，他试图通过出售旧代码来欺骗人们”。

泄露代码的真实性已被验证，其中包括 Windows 加密程序和管理工具的组件。此事件加入了越来越多的勒索软件源代码泄露清单，这些泄漏有可能扩大网络攻击影响。

而有安全研究人员表示，泄露的存档包含真实但杂乱无章的代码，Visual Studio 项目文件错误地放置在通常为编译后的二进制文件保留的“Release”文件夹中。其 Windows 加密程序构建器连接到 IP 地址为 31.222.238 的附属面板。208 用于构建数据，从而为潜在用户造成技术障碍。

代码中的另一个重要发现，揭示了 Van Helsing 为有效负载分配生成临时路径的能力。这显示了恶意软件如何使用 PsExec 设置横向移动功能。

员工监控软件 Kickidler 在勒索攻击中被利用

勒索软件正在使用合法的 Kickidler 员工监控软件进行侦察，跟踪受害者的活动，并在破坏其网络后收集凭据。

近期，有网络安全公司发现 Qilin 和 Hunters International 勒索软件下属组织安装了 Kickidler，这是一种员工监控工具，可以捕获击键、截取屏幕截图并创建屏幕视

频。攻击始于攻击者在用户搜索 RVTools 时投放了 Google 广告。受害者一旦点击了此类广告，便会访问一个虚假的 RVTools 网站，最终下载一个伪装成正常程序的钓鱼木马程序。受害者下载的这个恶意软件加载程序，可下载并运行 SMOKEDHAM PowerShell 的 .NET 后门，最终在受害设备上部署 Kickidler。

此类攻击针对的是企业管理员，他们的账户通常会在被入侵后，为攻击者提供特权凭证，安全人员分析认为攻击者可能已经保持了对受害者系统的访问权限数天甚至数周，以收集访问异地云备份所需的凭证而不被发现。此外，安全人员还发现 Hunters International 使用的部署脚本利用了 VMware PowerCLI 和 WinSCP Automation 来启用系统中的 SSH 服务，便于部署勒索软件并在 ESXi 服务器上执行。

虽然员工监控软件不是勒索软件团伙的首选工具，但他们多年来一直滥用合法的远程监控和管理软件。最近，有人发现攻击者以易受攻击的 SimpleHelp RMM 客户端为目标，创建管理员账户、安装后门，并可能为 Akira 勒索软件攻击铺路。

勒索软件团伙越来越多地利用 Skitnet 投放恶意软件

一些勒索软件攻击者正在使用一款名为 Skitnet 的恶意软件作为工具来窃取敏感数据，并建立对受感染主机的远程控制。

据安全公司分析，Skitnet 也称为 Bossnet，是一种多阶段恶意软件。该恶意工具的一个值得注意的方面是它使用 Rust 和 Nim 等编程语言，通过 DNS 启动反弹 shell 并逃避检测。它还包含持久性机制、远程访问工具、数据泄露命令，甚至可下载用于提供额外有效负载的 .NET 载荷程序，这让其成为一种多功能恶意工具。

Skitnet 于 2024 年 4 月 19 日首次发布，并作为由服务器组件和恶意软件组成的“捆绑包”提供给潜在客户。该基于 Nim 的二进制文件进一步启动多个线程，每 10 秒发送一次 DNS 请求，读取 DNS 响应并提取要在主机上执行的命令，最终将命令执行的结果传回服务器。这些命令通过用于管理受感染主机的 C2 面板发出。

下面列出了一些受支持的 PowerShell 命令：

- Startup: 通过在受害者设备的 Startup 目录中创建快捷方式来确保持久性
- Screen: 用于捕获受害者桌面的屏幕截图
- Anydesk/Rutserv: 部署合法的远程桌面软件, 如 AnyDesk 或 Remote Utilities (“rutserv.exe”)
- Shell: 用于运行远程服务器上托管的 PowerShell 脚本并将结果发送回 C2 服务器
- AV: 用于收集已安装的安全产品的列表

早在 2025 年 2 月, 便有分析人员发现该工具一直处于活跃状态。它包含三个组件, 一个下载器、一个后门和一个用于后门的专用加载程序, 使攻击者能够在受感染的系统中, 部署包括勒索软件在内的各类恶意程序。本轮攻击中比较典型的勒索软件包括 BlackBasta 和 Cactus 等。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

charlestate@tuta.com	sembekker@aol.com	Safelife@tutanota.com
nnaseygoody@2mail.co	roks@keemail.me	zen_crypt@tuta.io
monvernalle@onionmail.org	dashboard487@onionmail.org	zen_crypt@cyberfear.com
jessikachumamo@web.de	dashboard487@cyberfear.com	playsourse@zohomail.eu
anarchyransom@proton.me	govmail@usa.com	caremastub@proxy.tg
helpreserve@onionmail.org	gouv@usa.com	datafiles78@tuta.io
helpreserve@cyberfear.com	ventutusa@gmail.com	datafiles78@cock.li
spyhunter5s@aol.com	ExDevilCorp@proton.me	devman@cyberfear.com
TDVP7boZDZDE4GYWA3qW@protonmail.com	backlock@waifu.club	james.shaw.junior@gmail.com
pluransom@tutamail.com	redfox@mailum.com	ziqbwnscvbsj@proton.me
traverse_politely673@aleeas.com	xtjdjfbxix@mail.ru	asdcspocnsdke@proton.me
grumble_monastery519@8alias.com	digitalbro@onionmail.org	tfefwapyasd3@proton.me
bakeshop_unhappily046@dralias.com	nightspireteam.receiver@onionmail.org	restofiles@hotmail.com
lockbit3black@pressmail.ch	ownercall@tuta.io	cyberspectreislocked@onionmail.org
lockbit3black@zohomail.eu	ownercall@mailum.com	skiffdecrypt@onionmail.com
returnback24@protonmail.com	moonliga@tutamail.com	skiffdecrypt@mail2tor.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，该数据仅包含未能第一时间缴纳赎金或拒缴纳赎金的企业或个人情况（已经支付赎金的企业或个人，可能不会出现在这个清单中）。

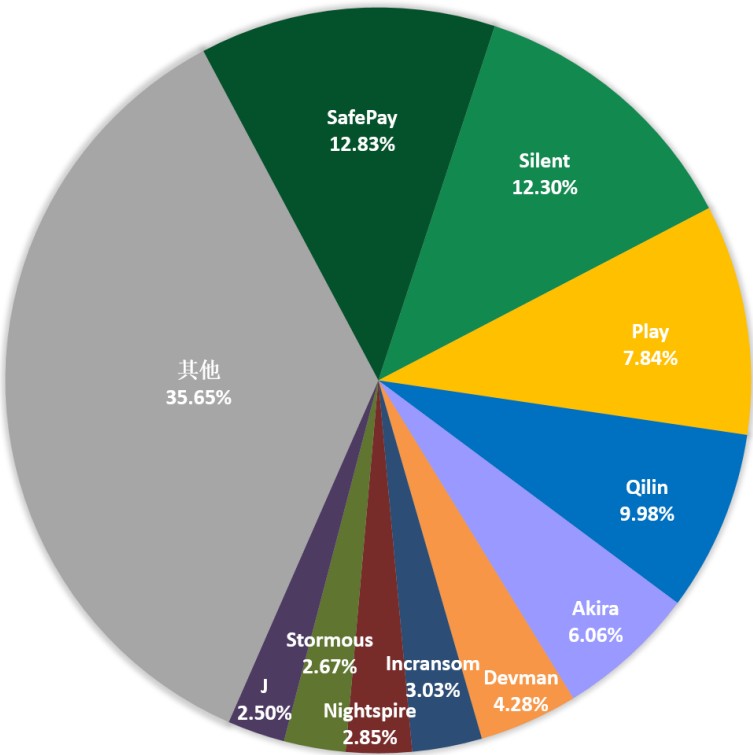


图 4. 2025 年 5 月通过数据泄露获利的勒索软件家族占比

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，做好数据已被泄露准备，采取补救措施。

本月总共有 561 个组织/企业遭遇勒索攻击，其中包含中国 11 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 4 个组织/企业未被标明，因此不在以下表格中。

universityacademy.org	The Holiday:Adult Care Community & Retirement Homes	Selenis
radicon	AttainX	novaevo+ / T. consult
lantro.com	Greater Seattle Concrete	Khidmah
ASCOMA Cameroon	notar-roemer-troisdorf.de	Kaefer
Chrisman Commercial	rgvengineering.co.uk	gmanetwork.com

Trustgrp. ae	servicedecorating.com	Amtech Software
Volkswagen Group	ctd-dortmund.de	Transport Lutztulln
Synergy Investments	planet-it-services.com	Julia Evans accountants
Terra Caribbean	dawg-dok.de	mdgny.com
Adriatic Glass & Mirrors	proctorlane.com	clinpath.com
Bin Faqeeh Real Estate	sb-p.de	gslelectric.com
Rousseau	schoene-aussicht-kassel.de	jbanksdesign.com
TDM Technical Services	Neighborhood Development Services	gates-cooper.com
mysfa.org	Anglo American plc	ehlers-inc.com
office-national	Rivers Academy West London	Langer & Langer
meeksgroup.com	JDC Air & Sea Freight (HEUEL LOGISTICS Group)	Elmore & Bunn
sfhumanesociety.org	www.seashoremotel.com	The Dominguez Firm, LLP
donowentire.com	www.wirebangkok.com	USClaims
iicil.com	www.axxoshotels.com	Dean & Fulkerson
visco.de	crystalhotels.com.tr	Pajcic & Pajcic
buechel-online.com	nirvanahotels.com.tr	Shutts
www.shautoparts.com	thewatermansarms.net	Fenwick
Tri-Point Solutions	Semple & Cooper	McLaughlin & Stern
Anchor Industries	Ertl ELEKTRO FELDBACH	Roger Keith and Sons Insurance Agency
W. E. Bowers	Valentin Hotels	Advantage Group GA
evergreen-hotel	Florida Lung	Cors & Bassett
wheel-king	Durham Arts Council	IFG Companies
STANDBYTE	Flo Components	Kisling Nestico & Redick
Canadian Rocky Mountain Resorts	Reece Noland & McElrath Engineers	NCheng
Lars Myhre Ostfold AS	tennsco.com	ADM LAW
Datatrykk	Rommel's Ac\Rommel Electric	First Financial Equity
Acorn Sales	MSM International (TOYOMI)	Barst Mukamal & Kleiner
MCM Construction	Making Tech Happen	Olinsky Law Group
Chalmers Suspensions International	The Vascular Experts	Pembroke Group
UnigazJordan	BEST VISION	Colucci Law Group
M&H Electric Fabricators	Tri State Electric	GreatFlorida Insurance Holding Corp.
Jordan Drug	Landmark Properties	Paycor
ibague.losolivos.co	Stiga.com	Baxter Baker Sidle Conn & Jones
Avance Agricola sl	Medswana	Chicago Atlantic Group
murraybuildingcompany.com	Indigo Group S.A.	Mauldin & Jenkins
sander-doll.com	K & K Fence	Miller Canfield
usmortgage.com	DMG Contractors	CRC Group
McKenzie Commercial Contractors	Strand Ag Supply	44North
eli	Miller & Stewart	EW Smith Insurance Agency
bcps.k12.va.us	RISE Racing	Anders CPAs + Advisors

personalassistants.com	Buford Ranches	Black , Bashor & Porsch
altrusses.com	EPK	Shea Barclay Group
teamhorner.com	branchcore	ATLAS CPAs & Advisors
logan.edu	NSSF KENYA	Klehr Harrison Harvey Branzburg
cpshawaii.net	edgeanalytical.com	Inspere Insurance Solutions
ccllabel.com	Williams Patent Crusher & Pulverizer Co.	Cross Valley FCU
tmcousa.com	Mantis Creative. Formerly known as WCI Rally.	Metro Public Adjustment
hallmarknameplate.com	TBD KOREA	Palomar Insurance
mhmlawgroup.com	TBD HONK KONG	Liberty Tax Service Inc
Choice AG	TBD GREECE	Kotz Sangster Wysocki
AGME Automated assembly solutions	TOHO-CO	Marriott International Inc
Termignoni SpA	piriou.vn	Cantey Hanger LLP
Del Corona & Scardigli Canada	www.atolon-parkhotel.com	JMJ Associates
ASC Machine Tools	Horecamaterialen De Meester NV	Prime Consulting Group
gruposancristobal.com.mx	Asco Tools	Ball Eggleston Law Firm
radsports.com	DSI Tech	Tetra Technologies Inc
schoenundendres.de	Termolar	Lincoln Investment Planning LLC
hennertanklines.com	Road Development Corporation	Quintairos Prieto Wood & Boyer PA
Alliance Healthcare IT	RECI SYSTEMS	Bass , Berry & Sims PLC
metromont.com	Colegio de la Compania de Maria Vigo	Essex Property Trust
Inns of Aurora	Fong Shann Printing Philippines	Davenport & Company LLC
Infinox	Grupo Boulevard	AG Adjustment
Mulia Raya	greenpac.com.sg	Jacobs Entertainment Inc
bridgecast.ca	mylikowines.co.uk	McCague Borlack LLP
codylawfirm.com	ngca.net	Lane Gorman Trubitt
spring-green.com/petbutler.com	distribution2.com	AGT Slots
paynecountyok.gov	redsquaredentalcare.com	Integrity Home Mortgage Company
SunMoon university	overheadtyler.com	Hannover Re
KDV Label	clarkmechanicalinc.com	TWFG Insurance
Eliel Cycling	prais.ro	Geocon Inc.
innovasystems.com	aplusmachining.com	Liebert Cassidy Whitmore Attorneys
Cator Ruma & Associates	MG Chemicals	Rosenbauer America
Quick Frames USA	Gearhiser Peters Elliott & Cannon	Haynie & Company PC
Neurosurgeons	diyar.com	Williams, Kastner & Gibbs PLLC
High Grade Materials	blainemn.gov	Sanchez Daniels & Hoffman LLP
Fujipoly Hong Kong Ltd	abilenetx.gov	Managed Benefits Advisors LLC
Elite Advanced Laser Corporation (Elaser)	gmb.com	Ted A Greve & Associates PA
kosmas.cz	chreynolds.com	Jardim, Meisner & Susser PC
The Salvation Army	cwcglobal.com	eu-rec.de

Lac La Biche Transport	gestionnaireimmobilier.ca	schapmann
Lasercam	compagnons-du-devoir.com	dosjm.com
Cape Robbin Inc	aldersonlaw.com	biglevel.net
Flagship Bank	scelltech.com	bloomfamilyeyesurgeons.com
TOP Ships Inc., Stock Symbol TOPS	freudenberg-cranes.com	kolpa.com.pe
Valiant Energy Solutions	Carney Badley Spellman	dreng.com
Corantioquia	zvaonline.com	mooregiles.com
iptelecom GmbH	finanzconsult-immobilien.de	Balance Diagnostics
educu	nissi-beach.com	Commune de Jemeppe-sur-Sambre
A/C Supply	alpha-steuer.de	Daniels & Taylor, P.C
Brackett & Ellis	npfy.org	NSS 長崎船舶装備株式会社
www.nexus.edu.my	www.davisdavisco.com	Rand Technology
Wrap & Send Services	ccrcda.org	Novosit
Eight8Ate Holdings, Inc	ros.eu	Marine Technical Surveyors
Centralno grijanje Tuzla	Straits Construction	Downtown Travel
crbgroup.co	Triple Jump	SNS SYSTEM
DataPost	Pacific Summit Energy	Breen Construction Services
kiwi86	Maruichi Leavitt Pipe & Tube	LGM
qualitas-pro	ALL RING TECH CO., LTD.	Alberta Construction Safety Association
SMV Thailand	south african airways	Future Association for Microfinance
Wilson International	TOHO CO., LTD.	Synthesia.com
Legal Practice Board of Western Australia	adamjeeinsurance.co	Grupo Herradura Occidente
Sylvania	olympusaero.com	Croatianmint.hr
VS One Technology	azpiaran.com	Derp.org
A M King	wnyenergy.com	Abdainsurance.co.id
Media Links	ITinSell group	Vnack.org
Laboratorios Belloch(Nelly, Yunsey, Fresh feel)	Vezina Lawrence & Piscitelli	Goodson.com
labbeemint.com	www.jparkislandresort.com	Mediprobe Research
servicecentermetals.com	MKA Accountants: Business Advisers, Moonee Ponds VIC	Trybus
ozarkah2o.com	Gloucester County Virginia	Sugar Lake Lodge
gjszlin.cz	GARDNER ORTHOPEDICS	Webcor
lrpa.com	Regal Ideas	ATI Systems
estudiolm.com.ar	Royal Chemical	Technical Die-Casting
Frederick's Machine & Tool Shop	Grafton Technologies	Sioux Chief
WAT Supplies	Av Alunitran	GPF Lewis
dmbarone.com	Murphy Pearson Bradley & Feeney	Hire Velocity (lan.hirevelocity.com)
dcbflegal.com	Franman	OeTTINGER Brauerei

rtblegal.com.au	Sao Camilo Cachoeiro de Itapemirim	https://pestbusters.com.sg/
Siena Hotel	www.cmic-cmo.com	Pulmonary Physicians of South Florida Clinics
Tan Logistics in Turkey	Kingsmen Creatives Ltd.	Bentley Industries
La Maison Liégeoise	PDI Health	Cocoon
Executive Jet Support	Dishaka	Lubiam
alles Lægehus	Nottingham Construction	NNC Firm
Mammut Sports Group	DeVita & Associates, Inc.	Defiance
FrontierCo	Superior Steel	Decoline
Étude Bordet	Precision Tax Relief	CabinC.com
ALB Forex	Nedved Architekti	TOMOKU CO., LTD.
Balcia Insurance	First Choice Courier & Messenger	valedolobo.com
Gobierno del Estado de Colima	Just Concrete & Masonry	soundtransit.org
Mediclinic Group	EIZO Rugged Solutions	ruizre.es
Department of Culture and Tourism Abu Dhabi	Overhead Door of Nova Scotia	iyca.com.co
Olho D'Água Distribuidora	Operative	edisoft.es
Carrera Chevrolet	loopergoodwine.com	ddecor.com
Antea Luce	www.circul-aire.com, www.dectron.com	Kalin Hobeltechnik
allstarflooring.com	psec.com.ar	American Eagle Logistics – Press Release
Novaria	bouygues-es.fr	Fowler Elementary School
Sama	ferretornillos.com	HCI Informatique d'entreprise
Constructive Building Solutions	ratnasagar.com	runtec.co.jp
oxparkrec.org	brdigital.net.br	[DISCLOSED] Imedexsa
Reliance Heating	Grupo Jorge Batista	Megachem Singapore
kkp.law	Trindel Insurance Fund	Jamjoom Pharma
iss-na.com	moorecoal.com	Jordan Kuwait Bank
icgad.com	igpi.co.jp	enersolcr.com
dbhcares.com	kize-weisser-stein.de	KYC UK
icmtx.com	lifesafeservices.com	Wizz Air
jastreet.com	gravelec.ch	derichsukonertz.de
neffendorfblokercpa.com	abfiad.nl	uva.edu.br
gosvt.com	join-the-quest.co.uk	ausfecl.com.au
vazirilaw.com	maxusgroup.com	rosekennedygreenway.org
www.nijar.es	hagemann-h.de	jean-petit.lu
Coweta County School System	metten-maas.de	atp.chaco.gob.ar
APH Svenska	scheuerle-stuttgart.de	l-a.com.vn
Norgeshus	gewandhaus.bayern	automobile-mueller.info
elitavia.com	morricetransportation.com	laticrete.com.cn
Anjos Ramos	tvgoiania.com.br	mygoalseek.com
Calcadawines	www.regencytorviscas.com	smvthailand.com

South Atlantic Federal Credit Union	www.regencycountryclub.com	kll-law.com
Kalamazoo Public School District	www.regencyrestors.com	arc-com.com
AKJ Energiteknik	Beaumont Products	pdcn.com
Vernon Milling	citrusmagic.com	Government of Peru
Berko İlaç Ve Kimya San Aş	statesmanbiz.com	Defected Records
Ghent Dredging	Municipality of Pisa	Chinese Healthcare Organisation
Delignit	Pienaar Brothers	Singapour Factory
www.paragonradiology.com	Victim from Japan	cobbcounty
netstar.co.za	Sweet Shop USA	Dedicated Web Consultants, Inc (USA) – dwcusa.com
West Lothian Council	Gistic Research	Custom Paper
www.bestop.com	Verrex	www.newseason.com
Simalga	EMX Enterprises	ECOM America
radiologue.paris	North Kitsap School District	Southern Fidelity
Bronx Pro Group	C. E. E. APTA	The Seydel Companies
The Haymond Law Firm	CHECKCITY.COM	Weil Construction, Inc
Professional TestingCorporation (PTC)	Lake Shore Paving	www.ancc.org
piercecountylibrary.org	Russell Child Development Center	Marsicovetere & Levine Law Group
Curewell Pharmacy & Surgicals	Bervar and Jones	Insight Pipe Contracting
Wawasan Dengkil Sdn Bhd	Klampfer Elektroanlagen	StudioVaiani
4Motive	Mountain View Mushrooms	The Saint James Hospital Group
Adria Grupa	hennessyfunds.com	Janco Steel
Coca-Cola	dailynews.co.th	maywdef
Cacspmec	101 Arch Street	South African IT firm
CNHI LLC	SHRADERLAW	South African Hr company
TeamLease	www.hcsheriff.gov	dovesit.co.za
Ecoinside	UniTrak	

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，目前已加入黑客入侵防护功能。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。

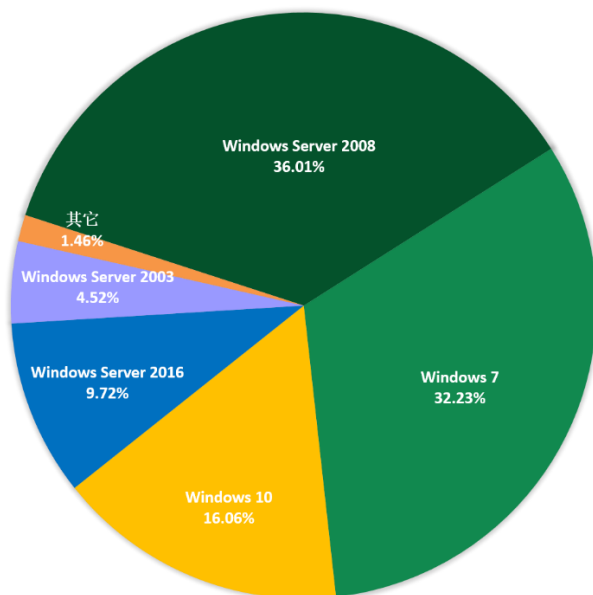


图 5 2025 年 5 月受攻击系统占比

对 2025 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被攻击的主要对象。

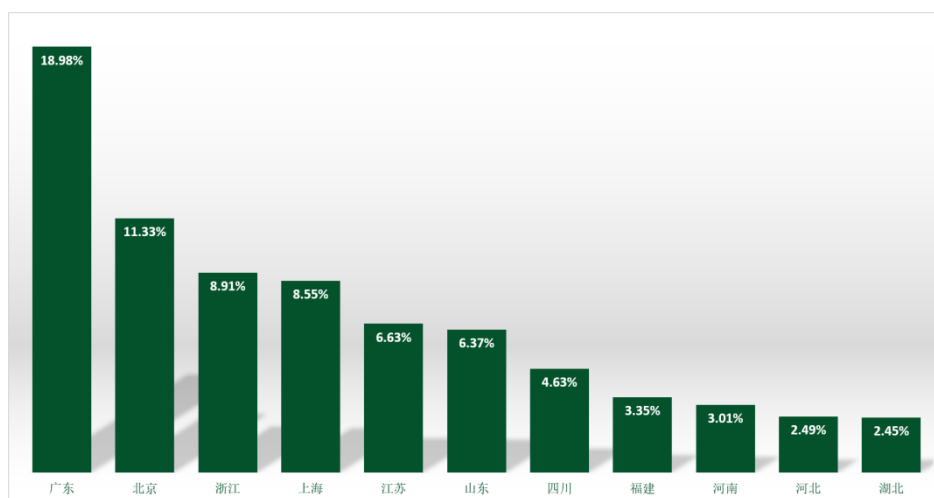


图 6. 2025 年 5 月国内受攻击地区占比排名

通过观察 2025 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。

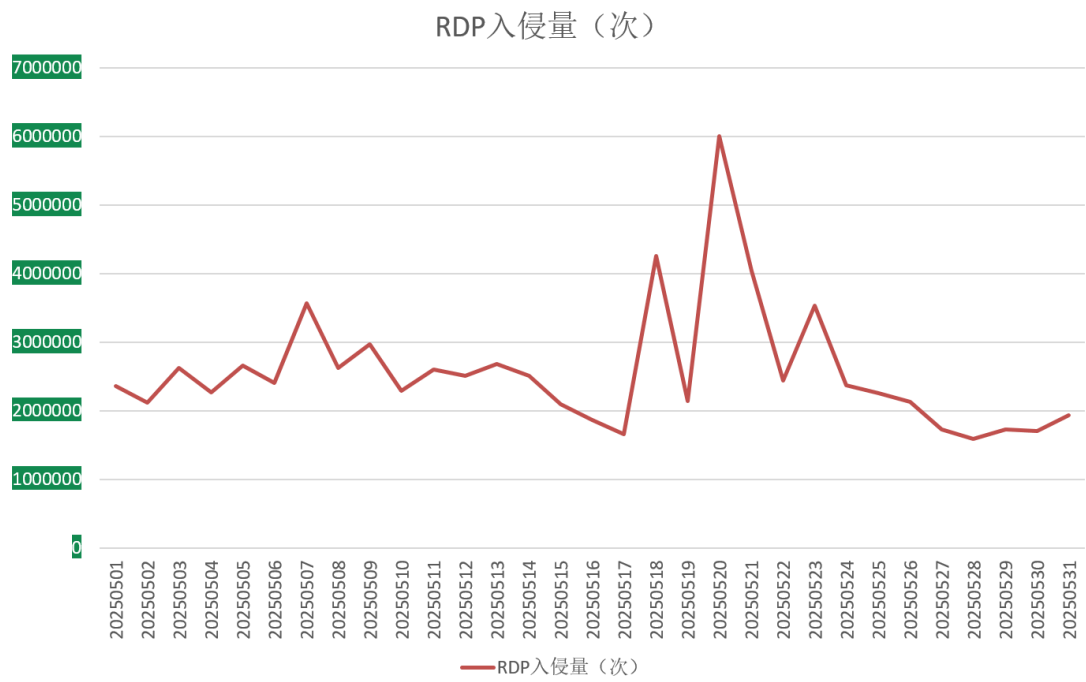


图 7. 2025 年 5 月监控到的 RDP 入侵量

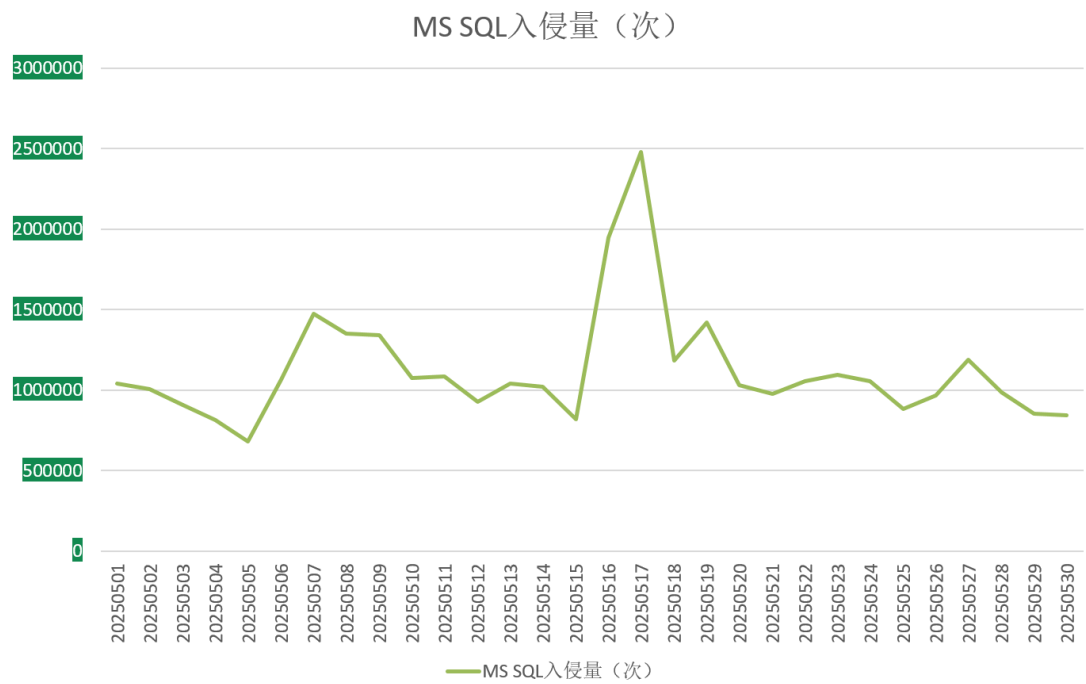


图 8. 2025 年 5 月监控到的 MS SQL 入侵量

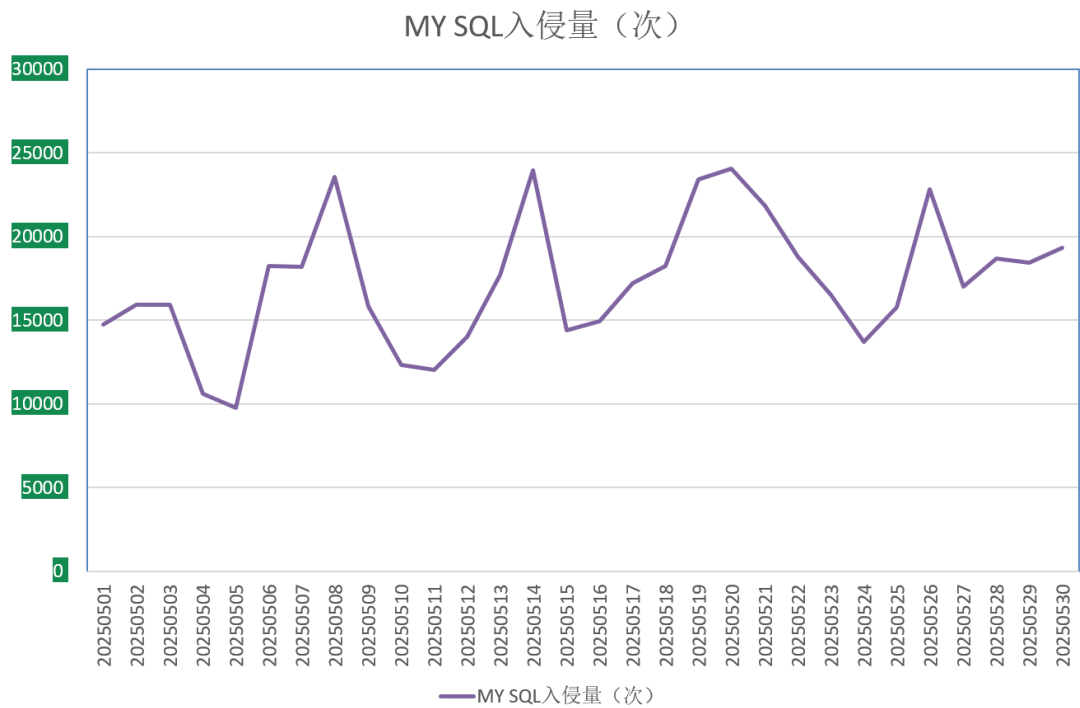


图 9. 2025 年 5 月监控到的 MYSQL 入侵量

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。

- ✧ **wxx**: 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，以及通过暴力破解远程桌面口令，成功后手动投毒。
- ✧ **wstop**: RNTC 勒索软件家族，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，同时通过 smb 共享方式加密其他设备。
- ✧ **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。
- ✧ **kalxat**: 属于 Kalxat 勒索软件家族，由于被加密文件后缀会被修改为 kalxat 而成为关键词。该家族主要的传播方式为：通过暴力破解或注入数据库，成功后手动投毒。
- ✧ **mkp**: 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。
- ✧ **baxia**: 同 bixi。
- ✧ **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。
- ✧ **weax**: 同 wxx。
- ✧ **sstop**: 同 wstop。

✧ **rw2**: 属于 LockBit 家族，以泄露的 LockBit 构建器代码创建。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。

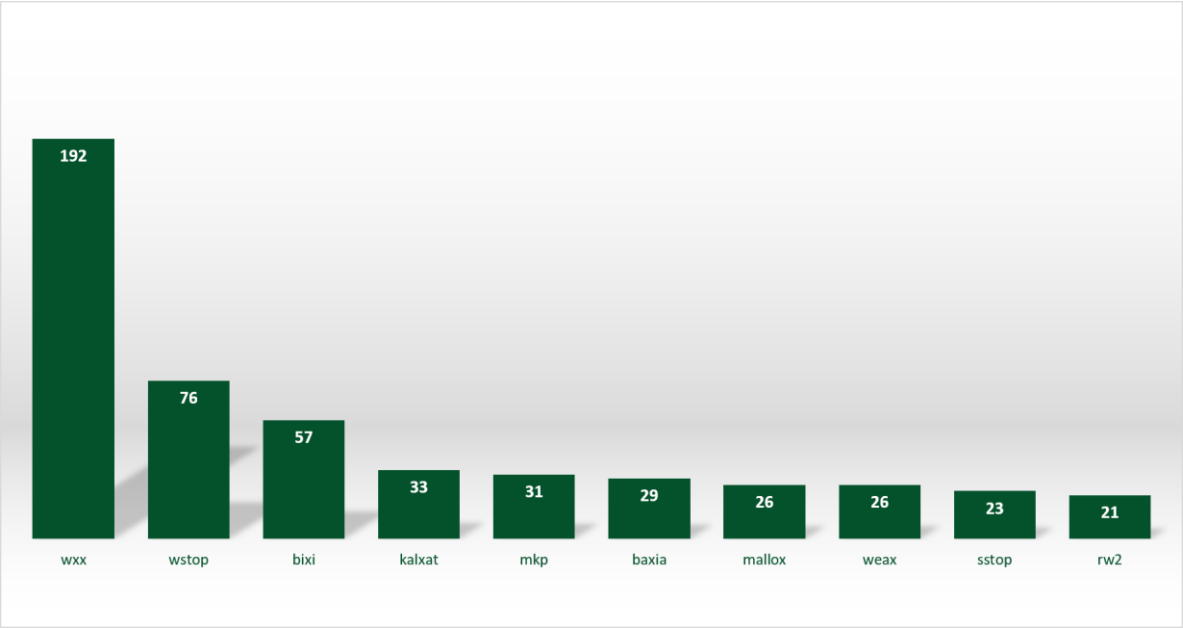


图 10 2025 年 5 月反病毒搜索引擎关键词搜索排名

解密大师

从解密大师本月解密数据看，解密量最大的是 FreeFix 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。

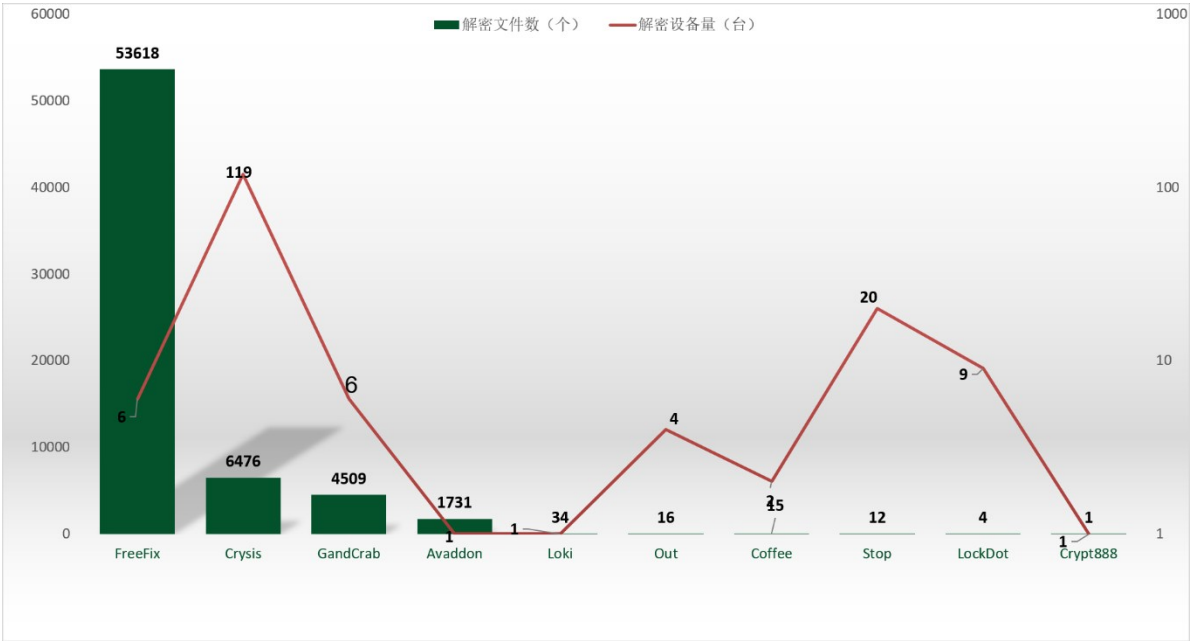


图 11. 2025 年 5 月解密大师解密文件数及设备数排名