勒索软件流行态势分析

2024 年 11 月

勒索软件传播至今，360 反勒索服务已累计接收到数万勒索软件感染求助。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 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。

2024 年 11 月，全球新增的双重勒索软件家族有 Kairos、Safepay、Argonauts、Chort、Termite。11 月新增的传统勒索软件家族有 XmrData、Frag、Triplex、Nyxe、MrBeast 等十余个家族，其中 XmrData、Frag 有监测到在国内的传播行为。

以下是本月值得关注的部分热点：

- Veeam RCE 严重漏洞现在被 Frag 勒索软件利用实施攻击
- 施耐德电器确认黑客窃取数据后开发平台遭到破坏
- 俄罗斯逮捕了与勒索团伙有关的知名开发人员

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：TargetCompany(Mallox)家族占比 22.38%居首位，第二的是 Makop 占比 15.38%的，RNTC 家族以 11.89%位居第三。

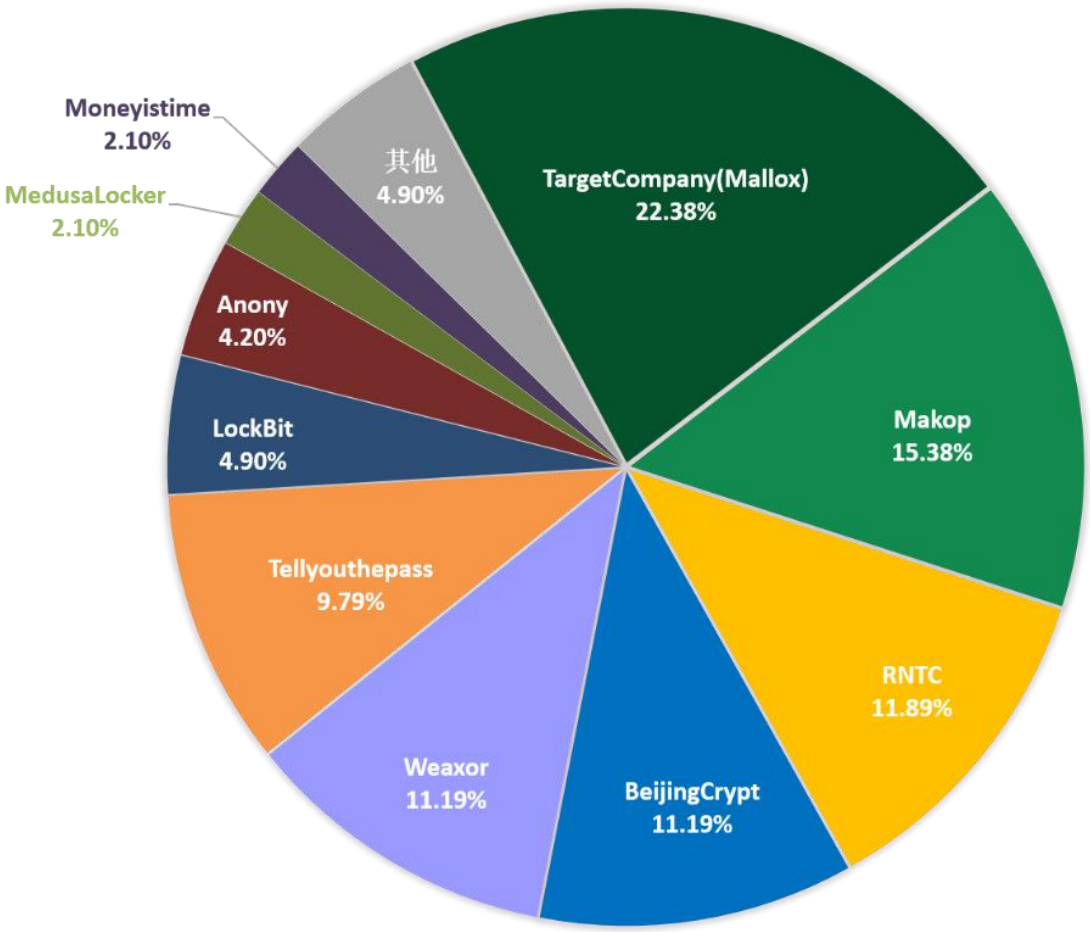

图 1. 2024 年 11 月勒索软件家族占比

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、Windows7 以及 Windows Server 2012。

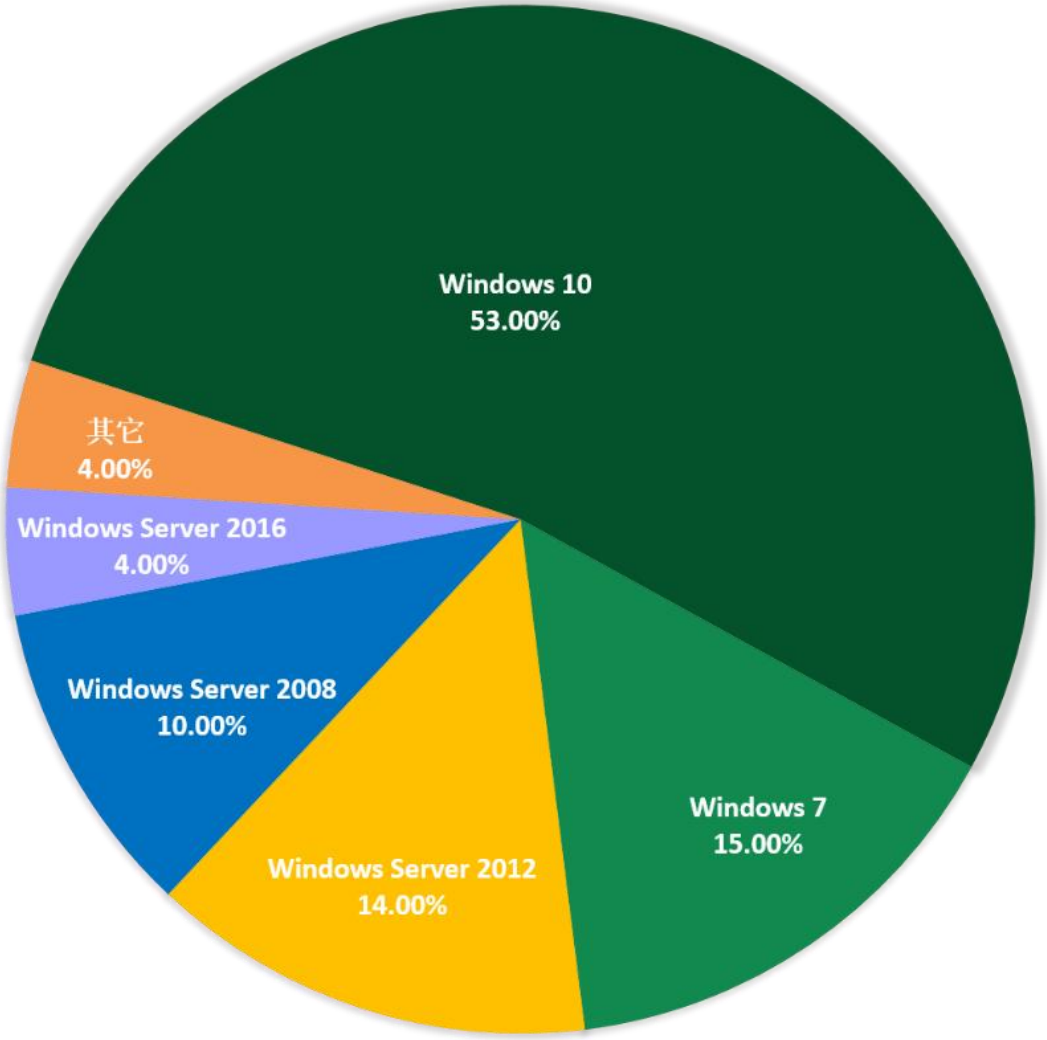

图 2. 2024 年 11 月勒索软件入侵操作系统占比

2024 年 11 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 高于服务器平台。

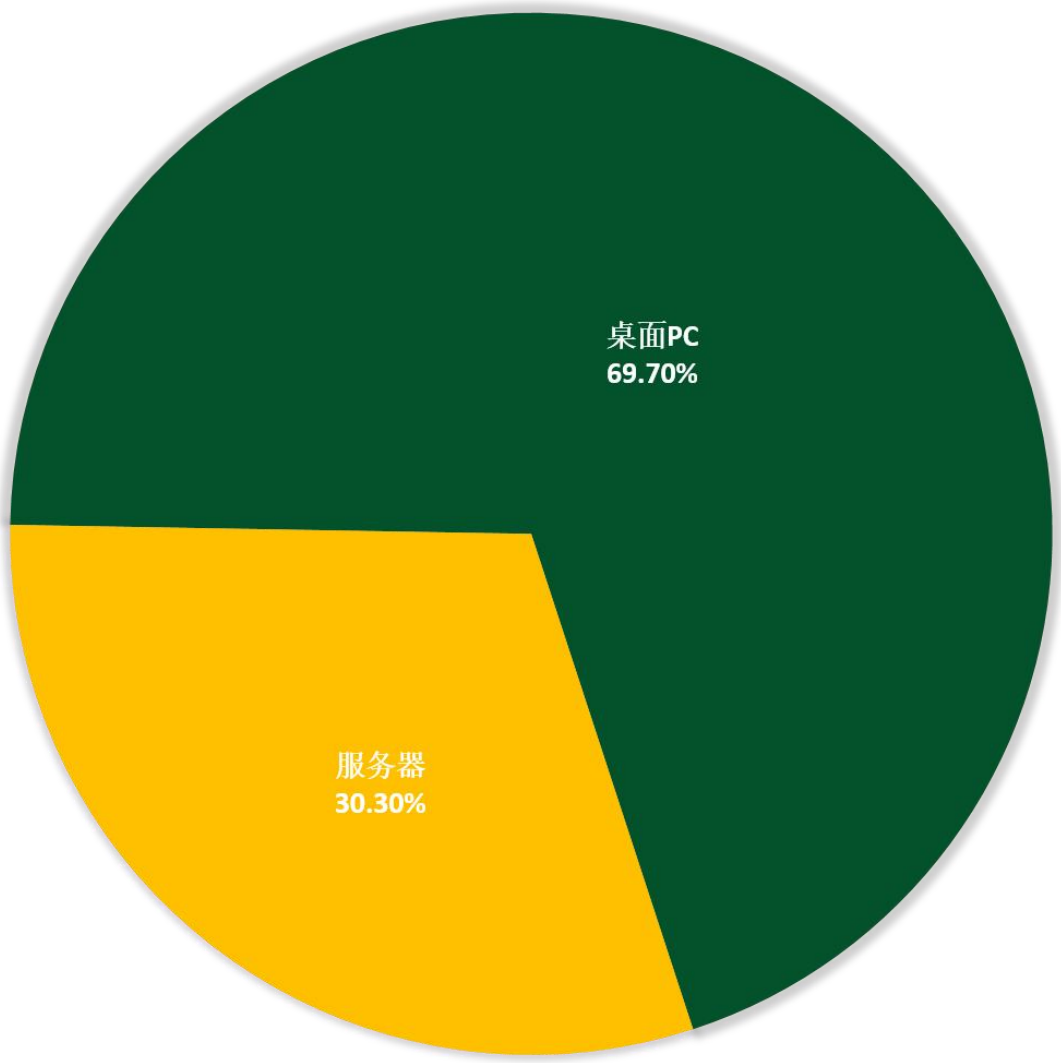

图 3. 2024 年 11 月勒索软件入侵操作系统类型占比

勒索软件热点事件

Veeam RCE 严重漏洞现在被 Frag 勒索软件利用实施攻击

在确认已被 Akira 和 Fog 勒索软件利用发起攻击后，Veeam 备份和复制（VBR）的一个严重安全漏洞最近再度爆出被用来部署 Frag 勒索软件。

安全研究员发现，该漏洞（CVE-2024-40711）是由不受信任的数据漏洞反序列化引起的，未经身份验证的攻击者可以利用这些数据漏洞在 Veeam VBR 服务器上获得远程代码执行（RCE）权限。

曾有安全实验室于 2024 年 9 月 9 日发布了有关 CVE-2024-40711 的技术分析，并将该漏洞的概念验证代码发布推迟到 9 月 15 日以便管理员有足够的时间安装 Veeam 于 9 月 4 日发布的安全更新。这一推迟也正是由于 Veeam 的 VBR 软件成为寻求快速访问公司备份数据的攻击者的热门攻击目标，而许多企业目前都将该软件视作灾难恢复和数据保护解决方案，以备份、恢复和复制虚拟、物理和云机器。

但实际上，安全响应人员发现这对延迟 Akira 和 Fog 勒索软件攻击的作用很小。攻击者依然利用了该 RCE 漏洞和被盗的 VPN 网关凭据，将流氓帐户添加到未修补和互联网暴露的服务器上的本地管理员和远程桌面用户组。

就在最近，研究人员还发现又有攻击组织（疑似是“STAC 5881”）在攻击中使用了 CVE-2024-40711 漏洞将 Frag 勒索软件部署到了受感染的网络设备上。

```
Frag is here!

If you are a regular employee, manager or system administrator, do not delete/ignore this note or try to hide the fact t
hat your network has been compromised from your senior management. This letter is the only way for you to contact us and
 resolve this incident safely and with minimal loss.
We discovered a number of vulnerabilities in your network that we were able to exploit to download your data, encrypt th
e contents of your servers, and delete any backups we could reach. To find out the full details, get emergency help and
regain access to your systems,

All you need is:

1. Tor browser (here is a download link:
2. Use this link to enter the chat room -
3. Enter a code ( <REDACTED> ) to sign in.
4. Now we can help you.

We recommend that you notify your upper management so that they can appoint a responsible person to handle negotiations.
 Once we receive a chat message from you, this will mean that we are authorised to pass on information regarding the inc
ident, as well as disclose the details inside the chat. From then on, we have 2 weeks to resolve this privately.

We look forward to receiving your messages.
```

图 4. Frag 勒索软件的勒索信息

这些攻击与 Akira 和 Fog 攻击者所使用的方法类似——他们都会在攻击期间针对备份和存储解决方案中未修补的漏洞和错误配置。

根据 Veeam 方面的数据，全球有超过 550000 名客户使用其产品，这其中甚至涵盖了全球 2000 强榜单中约 74%的公司，这一数据也说明了本次攻击事件背后巨大的潜在威胁。

施耐德电器确认黑客窃取数据后开发平台遭到破坏

施耐德电气已确认，在攻击者声称从该公司的 JIRA 服务器窃取了 40GB 的数据后，开发人员平台遭到破坏。

10 月底，一位名叫“Grep”的攻击者在 X 上嘲讽该公司，表示他们已经入侵了其系统。在与媒体的对话中，Grep 表示他们使用暴露的凭据入侵了 Schneider Electric 的 Jira 服务器。获得访问权限后，他们声称使用 MiniOrange REST API 抓取了 400k 行用户数据。Grep 表示，其中包括 75000 个唯一的电子邮件地址以及 Schneider Electric 员工和客户的全名。

在暗网网站的帖子中，攻击者开玩笑地要求 125000 美元的“Baguettes”来换取不泄露数据，并分享了有关被盗内容的更多详细信息。

Grep 进一步告诉媒体他们最近成立了一个新的黑客组织 International Contract Agency（ICA），以《杀手：代号 47》游戏命名。攻击者表示，该组织以前没有勒索他们入侵的公司。然而，在得知“ICA”名称与“伊斯兰恐怖分子团体”有关后，攻击者表示他们再次更名为 Hellcat 勒索软件团伙，目前正在测试用于勒索攻击的加密器。

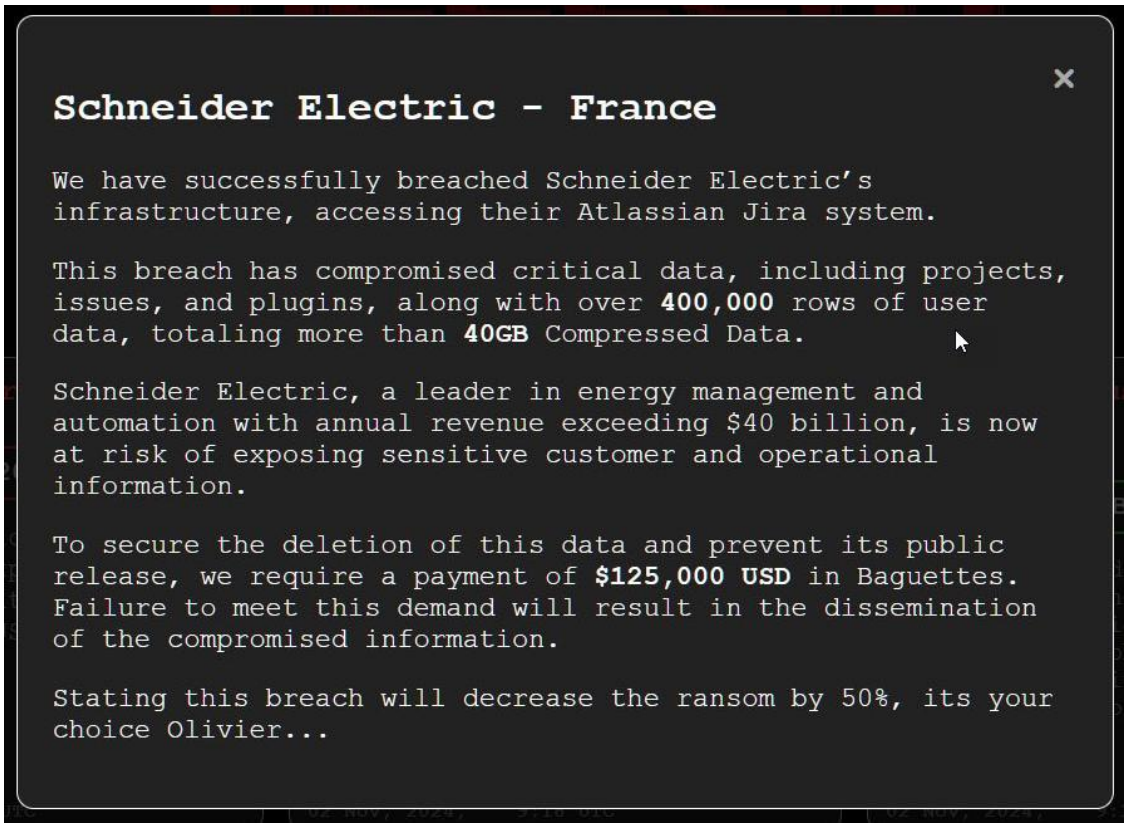

图 5. 攻击者放出有关对施耐德电器的攻击信息

俄罗斯逮捕了与勒索团伙有关的知名开发人员

俄罗斯执法部门于 2024 年 11 月底逮捕并起诉了臭名昭著的勒索攻击参与者 Mikhail Pavlovich Matveev（又称 Wazawaka、Uhodiransomwar、m1x 或 Boriselcin 等），罪名是其开发恶意软件并参与多个黑客组织。

据俄罗斯国有新闻机构 RIA Novosti 所接到的匿名来源消息称：虽然检察官办公室尚未公布有关此人身份（在法庭文件中被描述为“程序员”）的任何细节，但此人正

是 Matveev。俄罗斯内务部在一份声明中说：“目前，调查人员已经收集到足够的证据，检察官签署起诉书的刑事案件已送交加里宁格勒市中央地区法院进行审议。”

正如网络政策专家 Oleg Shakirov 首次发现的那样，Matveev 被指控开发勒索软件（检察官办公室将其描述为可以加密文件和数据的“专用恶意软件”），并称其计划使用勒索软件来加密“商业组织的数据，以便然后从他们那里获得赎金进行解密”。

去年，即 2023 年 5 月，美国司法部还对 Matveev 提出指控，称其参与开发了针对美国受害者的 Hive 和 LockBit 勒索软件。此外，他还被认为是“Orange”黑客论坛的创建者和管理员，以及 Babuk 勒索软件的最初运营者。而后者在组织成员无法抉择是否发布从华盛顿特区首都警察部队窃取的数据后分道扬镳。

图 6. FBI 对 Mikhail Matveev 的通缉信息

根据美国司法部的新闻稿和新泽西州及哥伦比亚特区的公开起诉书，可以整理出他在与三个勒索软件团伙合作时活动的大致时间表：

- 2020 年 6 月，Matveev 和 LockBit 勒索软件合谋在新泽西州帕赛克县的一个执法机构的网络上部署了 LockBit 勒索软件；
- 2021 年 4 月，Matveev 与 Babuk 勒索软件合谋在华盛顿特区大都会警察局的

系统上部署了恶意载荷。

- 2022 年 5 月，Matveev 同 Hive 勒索软件团伙成员加密了总部位于新泽西州默瑟县的一家非营利性行为医疗保健组织的系统。

- Matveev 还因对美国实体（包括美国执法部门和关键基础设施组织）发起网络攻击而受到财政部外国资产控制办公室（OFAC）的制裁。

Matveev 在网上的知名度非常高。他经常与网络安全研究人员和专业人士进行交流，并使用他的 Twitter 帐户“RansomBoris”公开讨论他的网络犯罪活动。而在受到美国制裁后，Matveev 还曾公开嘲讽美国执法部门，并在推特上发布了一张 T 恤上的通缉海报照片。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

lazylazy@tuta.com	arcustm@proton.me	prometheushelp@mail.ch
help.service@anche.no	arcusteam@proton.me	prometheusdec@yahoo.com
apexxx@onionmail.org	darksetran@gmail.com	Tiberiano@aol.com
Dismember@tuta.io	Darkset@onionmail.org	yourdata@RecoveryGroup.at
cactus@mexicomail.com	serverdatakurtarma@mail.ru	Jeremy.albright@criptext.com
Techsupport@cyberfear.com	sunucuverikurtarma@gmail.com	monster666@tuta.io
inform-hack@proton.me	lazylazy@dnmx.su	onster666@tuta.io
infrom-test@proton.me	nonamehack2023@gmail.com	recoveryfiles@techmail.info
anonymousfrance@onionmail.org	nonamehack2023@tutanota.com	steriok@mail2tor.com
taxz@cock.li	pepe_decryptor@hotmail.com	proper12132@tutanota.com
taxz@cyberfear.com	gotchadec@onionmail.org	helpunlock@aol.com
H3lp4You@onionmail.org	Yamaguchigumi@cock.li	putinubiyca@privyonline.com
Upgrade4you@onionmail.org	sendmykey@duck.com	assistant@techmail.info
cactus787835@proton.m	josephnull@secmail.pro	hakbit@protonmail.com
pbs@criptext.com	xmrdata@tutamail.com	servo99@protonmail.com
pbs24h@tutanota.de	xmrdata@onionmail.org	youranonbonzi@cock.li
stocklock@airmail.cc	fixmaster@tutamail.com	molox@keemail.me
stocklock@firemail.cc	fixMaster01@onionmail.com	muflon@tutamail.com
suppdec@aol.com	MrBeastOfficial@firemail.cc	defg@tuta.com
suppdec2@ao1.com	biobiorans@gmail.com	god1@pissmail.com

studiocp25@hotmail.com	biobiorans@keemail.me	god1@cock.li
teroda@bigmir.net	Mirex@airmail.cc	richadau@mailfence.com
BM-2cWscKHR4SVHDYp4FqVHC5D5 fJFNAWNwcc@bitmessage.ch	pussylikeashavel@cyberfear.com	hrol@tutanota.com
metro777@cock.li	discord4spamreport@gmail.com	black_private@tuta.io
Recoverysupport@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）。

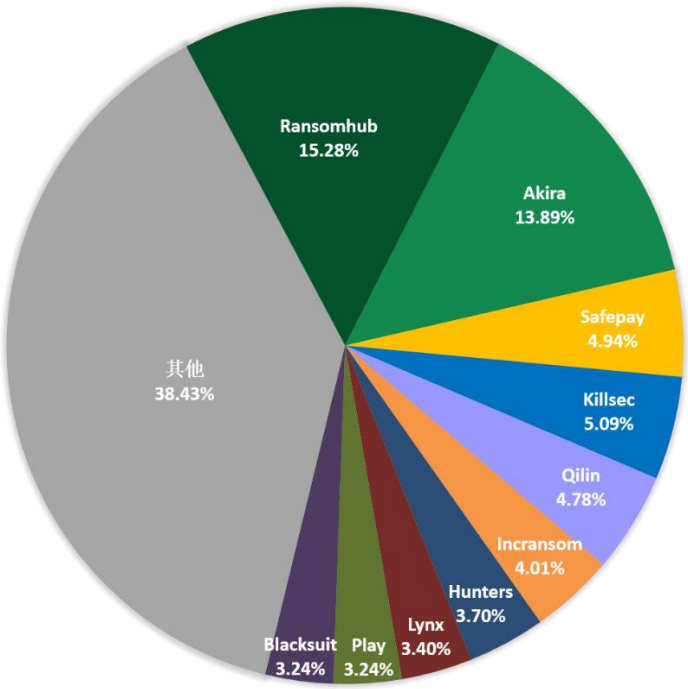

图 7. 2024 年 11 月通过数据泄露获利的勒索软件家族占比

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

本月总共有 649 个组织/企业遭遇勒索攻击，其中包含中国 12 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 10 个组织/企业未被标明，因此不在以下表格中。

www.agenciatributaria.es	Kellerhals Ferguson Kroblin PLLC	Zyloware
Mobigator Technology Group	Silverback Exploration	Pine Belt Cars
EP:Schuller	SSV Blockchain Network	DieTech North America
www.sansirostadium.com	PK Mulyo	Cottles Asphalt Maintenance Inc
Chema Per	Barneek Safety Consultancies	Herron Todd White
backyarddiscovery.com	Trust Seeds	J.S.T. Espana
Trace3	HM Environmental Services	Karl Malone Toyota
Specialty Bolt And Screw	IT Networks	Pincu Barkan, Law Office and Notary
Bendheim	www.microlise.com	ADT Freight Services Australia Pty Lt
www.aras-group.ae	James H Maloy	Kumla Kommun
Horsa	Automation Tool & Die	CP Construplan
Tillamook Country Smoker (tcsmoker.com)	Tampa State Bank	DynamicSystems
Pražské služby	Ship Services	Popular Life Insurance
Packard Machinery	Volo Internet Tech	Micon National
Brookway Landscape &Irrigation	Furniture Mart USA	Kelowna Springs
Aviosupport	PBS AEROSPACE	Dumont Printing
Co-op Agro Centre	RDS Electric	Berexco LLC
Wadsworth Solutions	Bishop Ireton High School	Intercomp
AMI Consulting Engineers	Groupe PPA- Mahe	stalyhill-inf.tameside.sch.uk
HTT Packaging & Design	Berman Law Group	Hellmich
Thomas Greg & Sons Ltda	Prime Group US	AXEON 360
Sanderson Stewart	www.ekirkpatrick.com	COOPERATIVA TELEFONICA DE CALAFATE LTD.
Touchstone Home Products	LaMear & Rapert, LLC - Accounting Firm	G-One Auto Parts de México S.A. de C.V.
Astor Chocolate	Alpha Care Medical Group	Schmack
McFarlane, Inc.	Privat Spitex	Sercomm
Summit Hosting	scalar.co.il	midstatesindustrial.com
Kay & Burton	rao.hr	sunnydayssunshinecenter.com
MSR Group	CK Power Public Manufacturing	formosacpa.com.tw
Deutsche Industrie Video System	inthinking.net	clayplattefamily.com
First Chatham Bank	Amherstburg Family Health	askyouraccountant.com
Metal Finishing	Global Results Communications	pmrcenter.com
Plastic Recycling	polaraire.com	kansasrmc.com
North Shore Systems	Département de La Réunion	Artistic Family Dental
Traffics	Oxford Auto Insurance	Value Dental Center

www.fpj.com.py	Camim	Asaro Dental Aesthetics
Weld Racing	LiquiTech	Axpr Valve Science
Colwell Colour	snowbrand.com.au	American Associated Pharmacies
Complete Control	piburners.com	Giggle Finance
Dfa Ny	tritonsourcing.co.nz	Orange County Pathology Medical Group
Cate Equipment	onnicar.it	SK Gas
CAUDURO SPORTS LTDA	kingswoodpark.ca	Medigroup.ca
Corman Leigh	incocommercial.com	steppingstonesd.org
Ilvief	euromedix.com	Hillandale Farms
Zillertal Bier	BusinessTraining.be	jst.es
Lucid Corp	ccseniorservices	jarrellimc.com
Rengo Packaging	ib-spieth.de	Banco de Fomento Internacional
Lotus Concepts Management	Safex.us	TaxPros of Clermont
4QuartersIT	millerservicecompany.com	National Institute of Administration
Snelling Paper & Sanitation	mcauslan.com	Supply Technologies
Magguilli Law Firm,PPLC	stats.gov.bb	Maxxis International
Turf Paradise	smartdimensions	potteau.be
Bennett Porter Wealth Management Insurance	westwood	Followmont TransportPty Ltd
ppotts.com	threadfxinc/bluedogmerch	dezinecorp.com
Namforce Life Insurance	Pronatec	Amourgis & Associates
brownpacking.com	Gilazo	Dietzgen Corporation
JTEKT NORTH AMERICA	OMINT	nynewspapers.com
Delmar International	NKCE Japan	comarchs.com
EQ Chartered Accountants	Richmond Hill Primary Academy	tolbertlegal.com
NHS Alder Hey	Active Cosmetic	Banco Sucredito Regional S.A.U.
Chanas Assurances S.A. (chanasassurances.com)	O'mara	OxyHealth oxyhealth.com.sa
ALLTUB Group (alltub.com)	Indesign, LLC	Immuno Laboratories, Inc
IAC	mithun.com	bitquail.com
Bedminster School (bedminsterschool.org)	mcleanmortgage.com	ATSG, Inc
WPM Pathology Laboratory (wpmpath.com)	andyfrain.com	Mizuno (USA)
visufarma.com	Henderson Stamping & Production	Palmisano & Goodman, P.A.
briatek.com.ng	Diamond Brand Gear	Karman Inc
clubfitsoftware.com.au	Dairy Farmers of Canada	Siltech (siltechcorp.local)
elwood.k12.in.us	Miller & Smith	Finger Beton Unternehmensgruppe
scottelec.com	Hive Power Engineering	emefarmario.com.br
helixbermuda.bm	CMD	Granite School District
australianhearthealth.org.au	IVC Technologies	WimCoCorp

midlandtool.com	Birdair	NEBRASKALAND
cloudofgoods.com	Vox Printing	bartleycorp.com
gehnaindia.com	Burkburnett Independent School District	interlabel.be
gajicermat.com	Valley Planing Mill (valleyplaning.com)	del-electric.com
corenroll.com	arabot.io	liftkits4less.com
www.polleninformation.at	IndicaOnline	www.lamaisonducitron.com
Contrack Facilities Management	Performance Health & Fitness	www.baldinger-ag.ch
Ventana Micro Systems	techguard.in	Marisa S.A
alleghenycontract.com	wulffco.com	www.assurified.com
tappi.org	smawins.net	www.botiga.com.uy
Grandview School District	chsplumbing.com	ottosimon.co.uk
R Pac Central America S.A. de C.V.	tempaircompany.com	Healthcare Management Systems
habeshacement.com	Anderson Miller LTD	Intermed Hospital Mongolia
ahn.org	Premier Tax Services	www.cenergica.com
times-supermarket.com	KVF	MedElite Group
Gruber Tool & Die (grubertool.com)	Southern Oregon Veterinary Specialty Center	vbuzrt.hu
ivylifesciences.com	rembe.de	nelconinc.biz
BOCCHI S.r.l.	brylesresearch.com	www.fdc.ie
contactsrl.eu	hartmannbund.de	www.bluco.com
弘潔科技股份有限公司	citywestcommercials.co.uk	Prime Hospitality Group, LLC
avisinterac.it	thinkecs.com	The Berman Law Group, LLP
藤森工業株式会社	gfemlaw.com	Lexco
AIAD.IT	instinctpetfood.com	naj.ae
crollatelecom.it	eatonmetal.com	Equator Worldwide
fitcisl	continentalserves.com	dzsi.com
NUUO	wachter.com	futuremetals.com
wheelerassoc.com	jonti-craft.com	plowmancraven.co.uk
gronercrm.com.br	isaitaly.com	europe-qualité
Signal Health Washington	rockportmortgage.com	geminiindustriesinc.com
Interior Metals	San Francisco Ballet	Winnebago Public School Foundation
bolognafc.it	kmcglobal.com	Jomar Electrical Contractors
www.bent-tree.com	rauch.de	Howell Electric Inc
facilcreditos.co	interborosd.org	ucv.es
osmedica.com.ar	Thebike.com	New Law
Vermilion Parish School System	3ccaresystems.com	Postcard Mania
formpipe.com	Equentis Wealth	www.msdl.ca
Wisconsin Lifting Specialists	Terra Energy	brandenburgerplumbing.com
Government of the People's Republic of Bangladesh	www.depewgillen.com	arcoexc.com

Fuero Militar Policial	Nations Homes Commercial & Residential Construction South Carolina	Lincoln University
SILKNET COMPANY	waive.com.au	Wholesale Fuel Distributors, Inc.
www.sella.eng.br	PC AfterHours	Cape Cod Regional Technical High School (capetech.us)
Pioneer Urban Land & Infrastructure	Bells Tax Service	GSR Andrade Architects (gsr-andrade.com)
Pinnacle Plastic Products	Tiendas Carrion & Fernandez	Smitty's Supply
GMG	LA LUCKY Brand	Interoute agency
Marketing Incentives	SUSTA S.r.l.	klinkamkurpark
Metroline	Maxeon	hausdesstiftens.org
reliv.la	eastgateauto.com	nightnurse.ch
SCM GROUP	kciaviation.com	fuelco
walkingtree.org	totaldevelopmentsolutions.com	VALLEYFIRM
TWRU CPAs & Financial Advisors	jergenspiping.com	children
OfficeZilla.com	sealevelinc.com	knoxlawcenter
cal-tool.com	Jornstax.com	AMERICANVENTURE
waltersgardens.com	allconstructiongroupwv.com	CSIKBS
CNHW Landscape Design, Ltd	Waters Truck and Tractor	SANJACINTOCOUNY
tacomaengineers.com	Dorner Law & Title Services	compassfs
mdmcusa.com	Monster Electrical	lacliniqueducoureur
goformz.com	Maxus Group	TIVOLI-33
empowersettlementservices.com	Guard1	qualiform.cz
mydelux.com.my	Bulbrite Industries	SMARTS-ENGINEER
karberinsulation.com	H2OBX Waterpark	metroelectric.com
Browne McGregor Architects	Travis Pruitt & Associates	Alliance Technical Group
glts.net	HUTTER ACUSTIX	sector5.ro
Kela Health	Hager Group	S & W Kitchens
Fancy Foods	www.protectasecurity.pe	Paragon Plastics
minneapolisparks.org	Mantinga	Delfin Design & Manufacturing
Perfection Plus Services Inc	Followup CRM	pacificglazing.com
www.netromsoftware.ro	Conseil scolaire Viamonde	Dome Construction
coppelltx.gov	Lebenshilfe Heinsberg	ebrso
isd109.org	Oman Oil	nwhealthporter.com
maynard.k12.ma.us	Culligan	wexfordcounty.org
parkleigh.com	Nifast	Model Die & Mold
dienesusa.com	uatf.edu.bo	Falco Sult
yunker.com	Buddy Loan	apoyoconsultoria.com
Everything Breaks	hetrhedens.nl	Fylde Coast Academy Trust
Keable & Brown	texanscan.org	Webb Institute
TOC	edwardsburgschoolsfoundation.org	sundt.com

www.itlindia.com	Tri-TechElectronics.com	www.colonialbh.org
INFiLED	bartow.k12.ga.us	Memorial Hospital & Manor
GuangDong South Land pharmaceutical	paaf.gov.kw	Scolari
JN attorney	hartwick.edu	McMillan Electric Company
Orshan, Spann & Fernandez-Mesa	The Egyptian Tax Authority (ETA)	AXIOM
borohradek	Dragon Capital	www.schweiker.de
atfservices.com.au	Nunziaplast Srl	www.drbutlerandassociates.com
aclaser.com.au	Apple Electric Ltd	maxdata.com.br
Nicholsons Solicitors	LEGO Construction Co	goodline.com.au
Hadwins Volkswagen	Logistical Software Ltd	kenanasugarcompany.com
Ithbar	brandywinecoachworks.com	www.mssupply.com
Dardoc	kapurinc.com	College of Business - Tanzania
inv[...]nator	Manens-Tifs SpA	Ministry of Education - Jordan
RiverRestHome	American Addiction Centers	Schneider Electric - France
Ace Laboratories Limited	Grupo_Trisan	International University of Sarajevo
BeClever	klarenbeek-transport.nl	Whitaker Construction Group
Extra	surgicalassociates.com	fullfordelectric.com
titlenine.com	billyheromans.com	San Francisco Ballet
STIIIZY	kenmore.com	European External Action Service (EEAS)
Hypertype	Total Patient Care LLC	csucontracting.com
Concord Orthopaedics	jhs.co.uk	redphoenixconstruction.com
Pastor Real Estate	potteau.com	Air Specialists Heating & Air Conditioning
Sa.SS Datentechnik	Vector Transport (vectortransport.com)	caseconstruction.com
co.cullman.al.us	marysville.k12.oh.us	krigerconstruction.com
Silicom	Bio-Clima Service Srl	lambertstonecommercial.com
Nationwide Legal	PHARMATIS-SAS	Hemubo
Eassy Life	A Sensitive Touch Home Health	Elad municipality
Efi Sales	www.gob.mx	The Law Offices of Jed Silverman
Vogue Homes	Pinger - USA	Russell Law Firm, LLC
Service Avicole JGL	A&O IT Group	L & B Transport, L.L.C.
Darlington EMS	fortinainvestments.com	bravodigitaltrader.co.uk
Schuck-Gruppe	BluMed Health	Imprimerie Peau
Jones & Mayer	Live Aquaria	SVP Worldwide
Aeris Energy	Wright Engineers	Sumitomo
Gulf Energy Maritime	El Dorado Stores and Supermarkets	DieTech North America
IPE Engwicht	Ocean BeautySeafoods	www.sym-global.com
lgpunjab.gov.in	AACANet	www.fatboysfleetandauto.com
Alna-Bioscience	Ocean Park Mechanical	www.tetco-group.com

gureco.pl	Datron WorldCommunications	www.tigre.gob.ar
Trinity Petroleum Management, LLC	Duplo USA	www.usm.cl
blr.com	MONVIA Holding, a.s.	www.ua4rent.com
madison-home.com	Falvey LinenSupply	www.rosito-bisani.com
sheboyganwi.gov	Xtrim TVCable	obe.com
Zimmerman & Frachtman PA Law Firm	Action COACH	lighthouseelectric.com
LBCO Contracting LTD	Yazoo ValleyElectric Power Assosiation	JS McCarthy Printers
Calvert Home Mortgage Investment	Allegheny Millwork & Lumber	CGR Technologies
Hronopoulos	Irr Supply Centers	lumiplan.com
ABC Group	EnviromentalDesign International	United Sleep Diagnostics
LenelS2	SKS Bottle &Packaging	eap.gr
suit-kote.com	Compass Group	Cerp Bretagne Nord
curenta.com	REV Engineering	vikurverk.is
Goldsmith & Hull	Bergeron LLC	mirandaproduce.com.ve
Brueck Golosow Kim & Associates	Morehead State University	Hope Valley Recovery
Suneva Medical(sunevamedical.com)	mk Technology Group	lsst.ac
United Bakery Equipment	Saint Andrews Bureau	Sabesp
MGEMAL	VOSS ENTERPRISES	MENZIES CNAC (Jardine Aviation Services)
Symantric IT	Ascend Packaging Systems	www.mltmua.com
ViralPitch	Tedkomp AB	Heritage Golf
Zimmerei Buder	Pemberton Fabricators, Inc	Groupe Althays
www.sfr.fr	Burmeister &Wain Scandinavian Contractor	AIMS, Inc.
www.cobeldarou.com	Optical Cable Corporation	Acco
www.damcapital.in	Ultimus	Freyberg Petroleum
DMF Lighting	Tennis Canada	aziz oil
Stalcop Metal Forming LLC	Don's MobileGlass	PetroSouth
Hogan Mfg (hoganmfg.com)	Mark Thomas	patria.hu
Fifteenfortyseven Critical Systems Realty	OMara Ag Equipment	Arctrade

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。

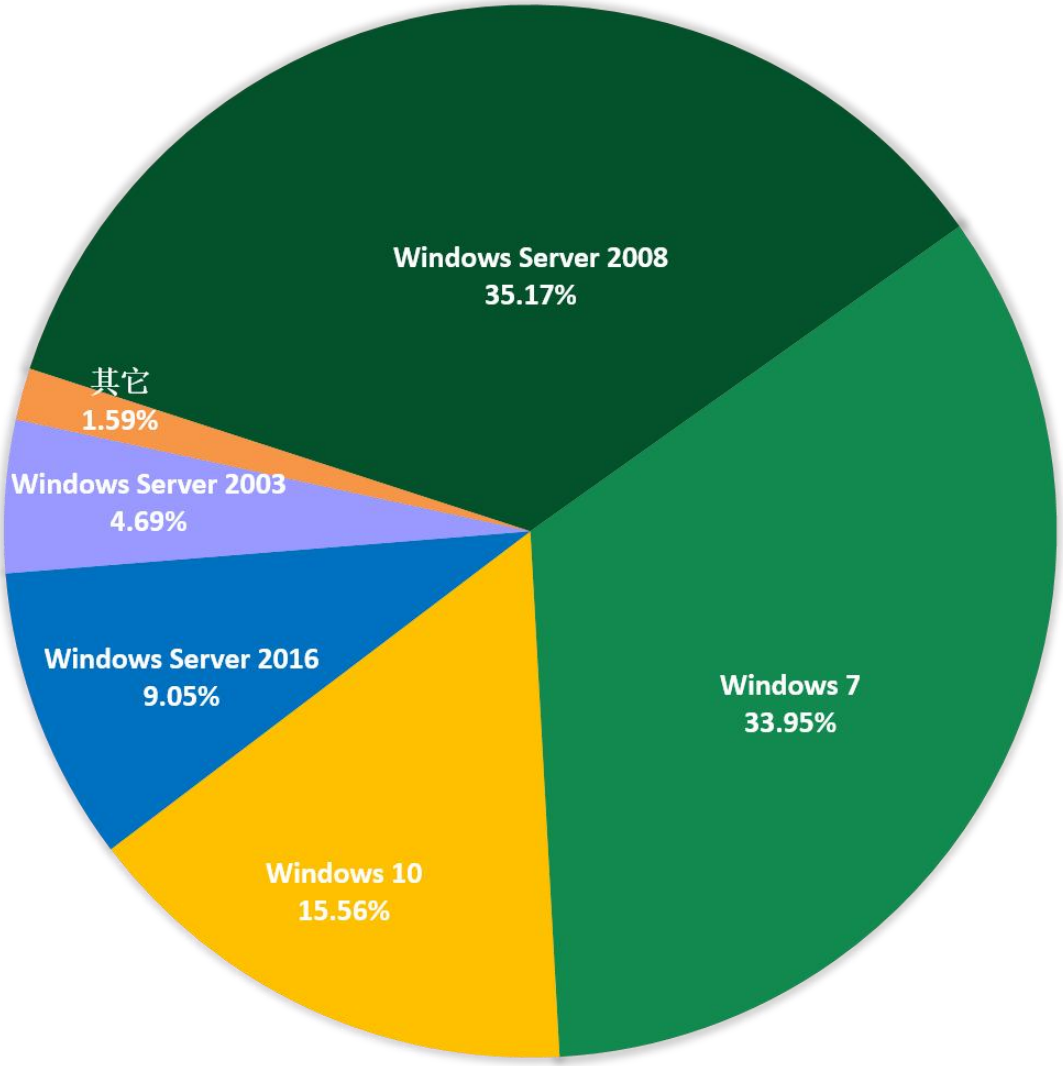

图 8 2024 年 11 月受攻击系统占比

对 2024 年 11 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。

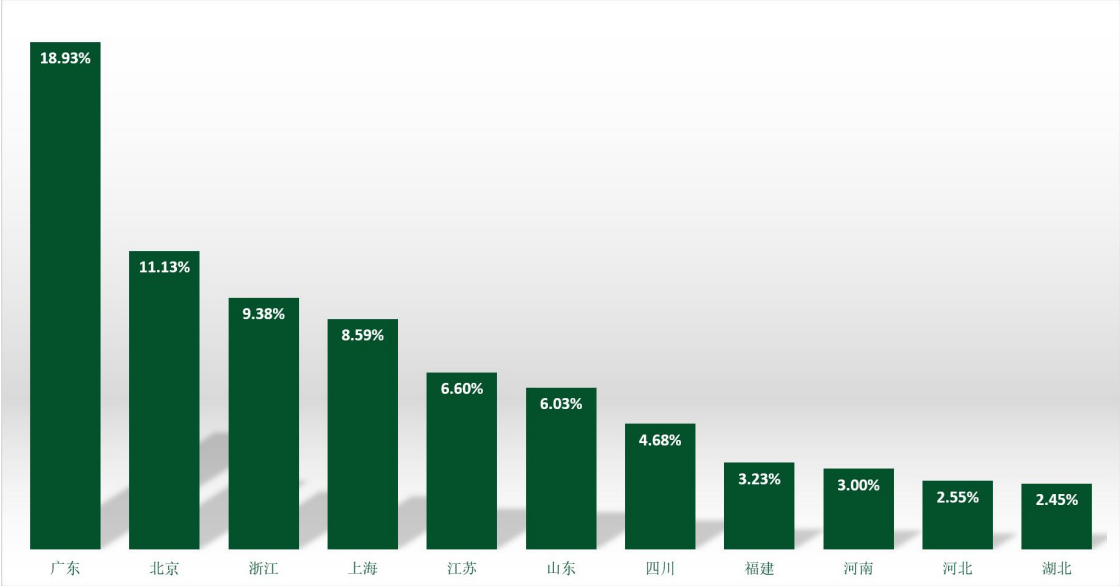

图 9. 2024 年 11 月国内受攻击地区占比排名

通过观察 2024 年 11 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。

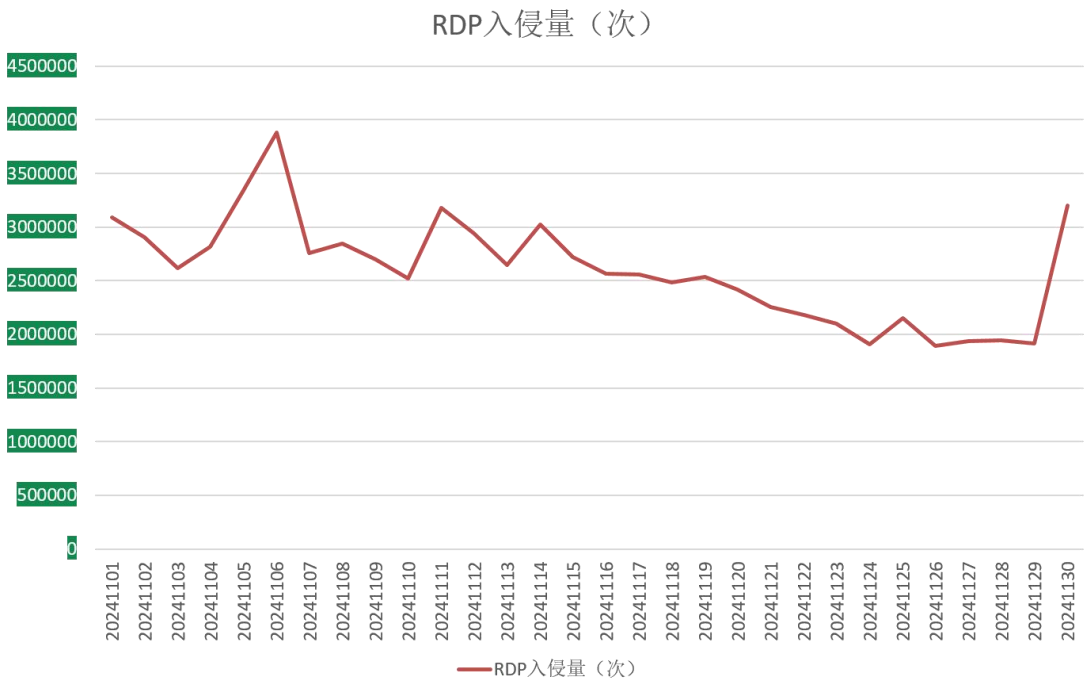

图 10. 2024 年 11 月监控到的 RDP 入侵量

图 11. 2024 年 11 月监控到的 MS SQL 入侵量

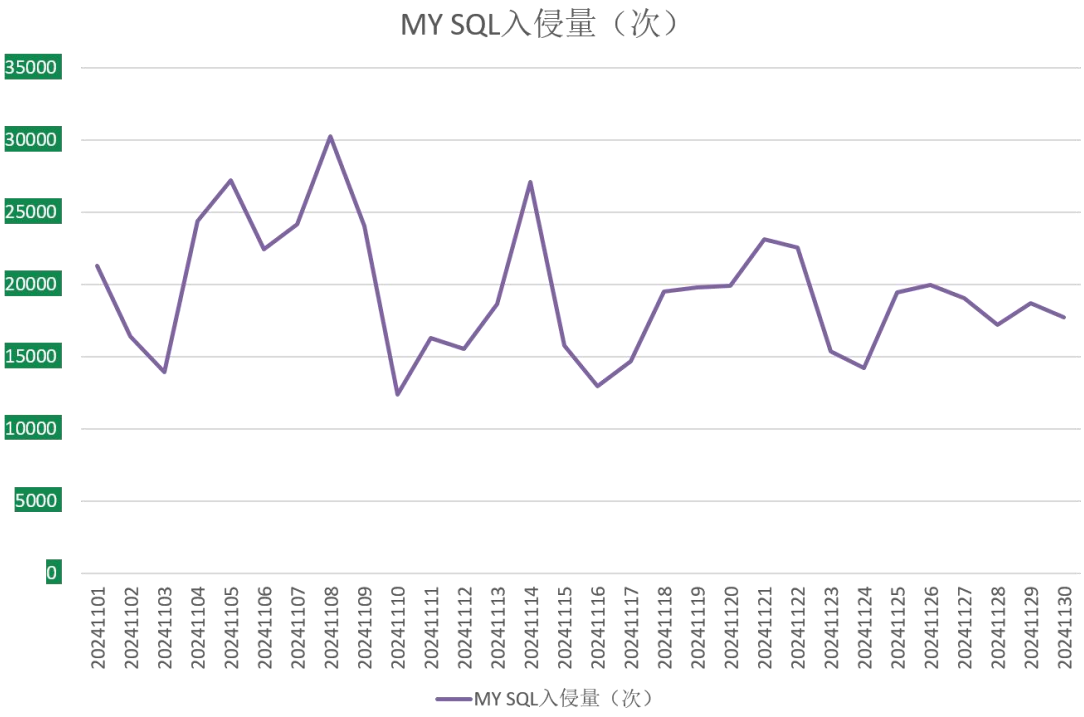

图 12. 2024 年 11 月监控到的 MYSQL 入侵量

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。
- 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。
- hmallox：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，今年起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本曾通过匿影僵尸网络进行传播。
- 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。
- rmallox：同 hmallox。
- src：同 mkp。
- baxia：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。
- bixi：同 baxia。
- mallox：同 hmallox。
- 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成功后手动投毒。

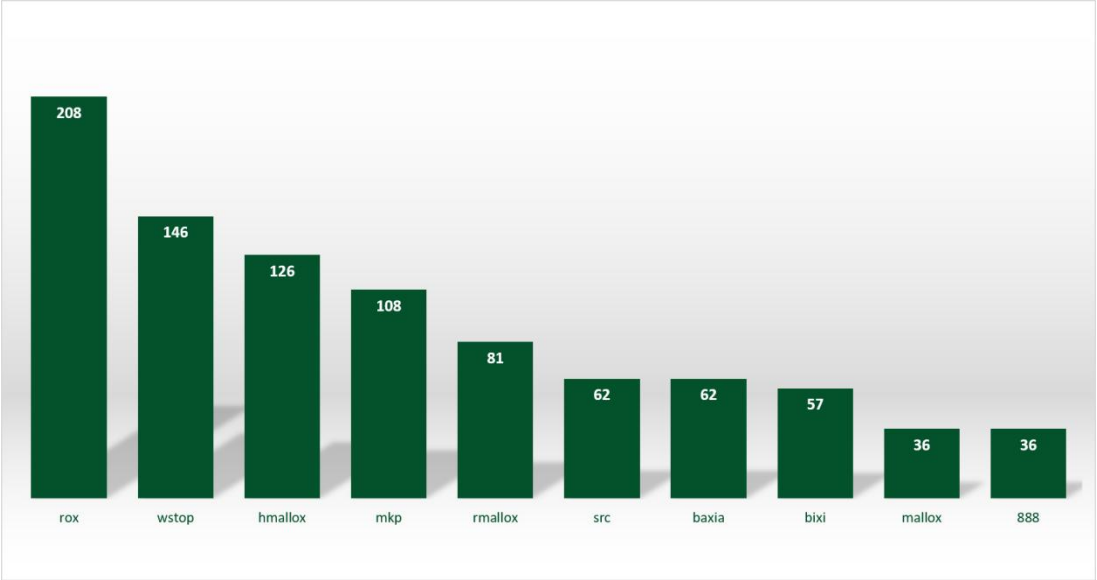

图 13 2024 年 11 月反病毒搜索引擎关键词搜索排名

解密大师

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

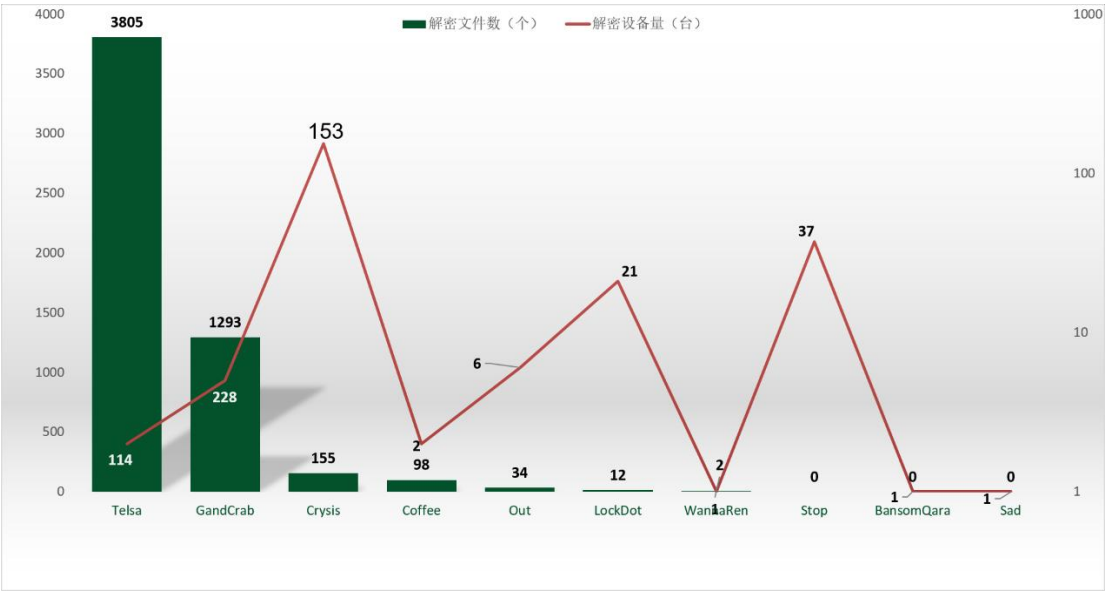

图 14. 2024 年 11 月解密大师解密文件数及设备数排名


360数字安全
数 字 安 全 的 领 导 者
360安全大脑