勒索软件流行态势分析

2024 年 9 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 9 月，全球新增的双重勒索软件家族有 Nitrogen、Orca、ValenciaLeaks。8 月新增的传统勒索软件家族 RNTC 在国内的传播较为显著，主要通过远程桌面登录手动投毒，同时通过 smb 共享扩大加密文件范围。

以下是本月值得关注的部分热点：

1. 法飞塔确认黑客窃取的 440G 文件已遭泄露
2. 堪萨斯州水厂遭网络攻击后被迫改为人工操作
3. NoName 勒索软件组织在最近的攻击中部署 RansomHub

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 31.21%居首位，第二的是 RNTC 占比 22.93%的，Makop 家族以 15.92%位居第三。

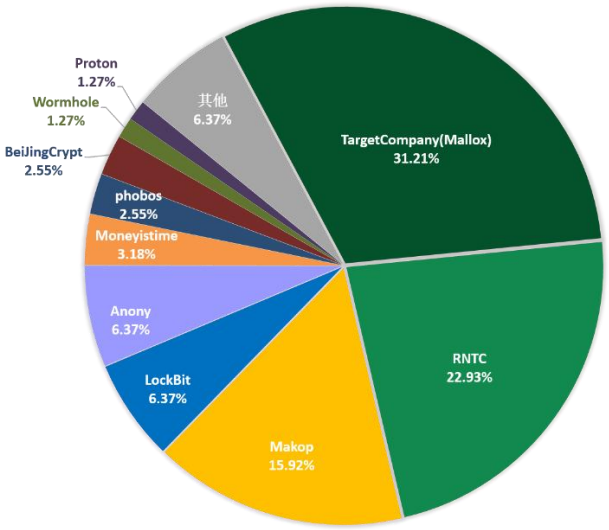

图 1. 2024 年 9 月勒索软件家族占比

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 2008 以及 Windows Server 2012。

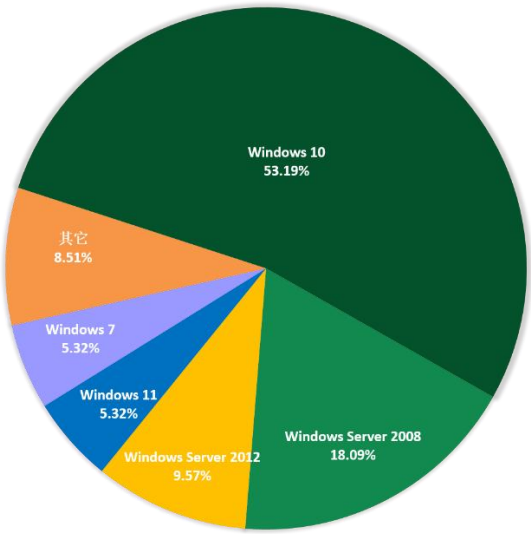

图 2. 2024 年 9 月勒索软件入侵操作系统占比

2024 年 9 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 与服务器平台的攻击比例基本相当。

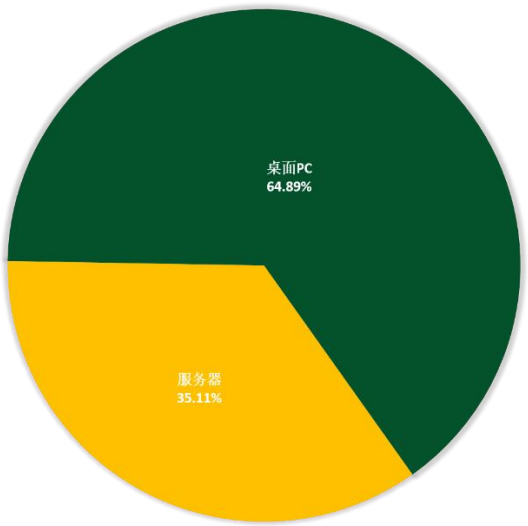

图 3. 2024 年 9 月勒索软件入侵操作系统类型占比

勒索软件热点事件

速汇金确认在长达数日的系统中断背后是网络攻击

汇款巨头速汇金证实自 9 月 20 日以来，其所处理的系统故障和客户投诉后均因该公司遭受了网络攻击所导致。虽然许多人此前就怀疑该公司受到了网络攻击，但直到当地时间 23 日早上，速汇金才证实了本次系统中断是由网络安全事件所致。

在速汇金客户无法转账或访问他们的资金后，该公司曾于 21 日表示他们遇到了“网络中断”影响了与系统的连接。

该公司最终于 23 日证实，网络安全事件是系统中断的原因，并向客户保证，该公司正在与外部专家和执法部门努力解决这一问题。

虽然速汇金没有透露他们遭受了哪种类型的攻击，但长时间的中断和与系统的连接中断表明存在勒索软件攻击。 考虑到速汇金庞大的客户群，该公司潜在的数据泄露可能会对许多人产生深远的影响。

堪萨斯州水厂遭网络攻击后被迫改为人工操作

负责监管西雅图港口和机场的美国政府机构——西雅图港务局于 9 月 13 日证实，Rhysida 勒索软件组织是过去三周内对该机构系统发动网络攻击的幕后黑手。此前，该机构于 8 月 24 日透露遭到网络攻击，并被迫隔离了一些关键系统以控制影响。由此导致的 IT 中断影响了西雅图塔科马国际机场的预订和登机系统，并导致航班延误。

在最初披露攻击事件的三周后，港口正式确认 8 月份的攻击事件是 Rhysida 勒索软件组织的成员策划的勒索软件攻击。该声明称：“此次事件是由名为 Rhysida 的犯罪组织实施的一起勒索软件攻击。从那天起，港口系统再也没有发生未经授权的活动。从西雅图-塔科马国际机场出发并使用西雅图港的海运设施仍然是安全的。”

据港口方面称，调查发现未经授权的黑客能够访问其部分计算机系统，并能够加密某些数据的访问权限。该港口决定关闭系统以及勒索软件团伙在未能及时隔离的系统上加密的行为导致了多重服务和系统的中断，其中包括行李处理、值机亭、售票、Wi-Fi、乘客信息显示屏、西雅图港口网站、flySEA 应用以及预留停车位。尽管港口已经在一周内将大多数受影响的系统恢复上线，但它仍在努力恢复其他关键服务，如西雅图港口网站、SEA Visitor Pass、TSA 等待时间和 flySEA 应用访问。此外，该港口也决定不向勒索软件犯罪团伙支付解密器费用，尽管攻击者很可能会在 8 月中旬至月底之间在其暗网泄露网站上发布窃取的数据。

“西雅图港没有向攻击者支付赎金的意图，”西雅图港执行主任 Steve Metruck 说。“向犯罪组织支付赎金不符合港口的价值观，也不符合我们作为纳税人资金守护者的承诺。”

NoName 勒索软件组织在最近的攻击中部署 RansomHub

一个名为“NoName”的勒索软件组织已经连续三年针对全球各地的小型和中型企业进行勒索攻击，并试图打出自己的名声。近日，该组织可能正在与 RansomHub 勒索软件交易平台开展合作。

该勒索组织使用了一款名为 Spacecolon 的恶意软件家族的自定义工具，并在利用 EternalBlue 或 ZeroLogon 等经典漏洞侵入网络后部署它们。而在最近的攻击中，NoName 则使用了名为 ScRansom 的勒索软件，该软件取代了之前的 Scarab 加密器。此外，该攻击者还试图通过尝试使用泄露的 LockBit 3.0 勒索软件声称器来创建类似的数据泄露网站以及使用类似的勒索赎金通知来为自己打响名号。

研究人员发现，尽管 ScRansom 在勒索软件领域并不像其他威胁那样复杂，但它仍在不断地进行着更新迭代。该恶意软件支持使用不同的速度模式进行部分加密，以使攻击者具有一定的灵活性。此外，其还具有一个名为“ERASE”的模式，可将文件内容替换为恒定值使其无法恢复。ScRansom 可以加密所有驱动器上的文件，包括固定驱动器、远程驱动器和可移动媒体，并且允许生成者通过可自定义的配置来确定要加密的文件扩展名。在启动加密程序之前，ScRansom 还会尝试杀死 Windows 主机上的一系列进程和服务，包括 Windows Defender、卷影副本、SVCHost、RDPclip、LSASS 以及与 VMware 工具相关的进程。与此同时，ScRansom 的加密方案也相当复杂：其采用了 AES-CTR-128 和 RSA-1024 的组合，并额外生成了一个 AES 密钥来保护公钥。

NoName 一直使用暴力手段来获取网络访问权限，但该攻击者还利用了几个更可能存在于 SMB 环境中的漏洞：

- CVE-2017-0144
- CVE-2023-27532
- CVE-2021-42278 与 CVE-2021-42287
- CVE-2022-42475
- CVE-2020-1472

在 6 月初的一起与 NoName 相关的勒索软件事件中，研究人员发现攻击者在不到一周后就在同一台机器上执行了 RansomHub 的 EDR 杀手工具。该工具允许攻击者通过在目标设备上部署一个合法但存在漏洞的驱动程序来提升权限并禁用安全代理。两天后，也就是 6 月 10 日，黑客在被入侵的机器上执行了 RansomHub 勒索软件。研究人员指出，提取 EDR 杀手的方法是典型的 CosmicBeetle 行为，而不是 RansomHub 的附属机构。

由于没有关于 RansomHub 代码或其构建者的公开信息，研究人员认为这一情况表明 NoName 加入了 RansomHub 的合作伙伴行列。尽管与 RanssomHub 的关联尚未确定，但研究发现 ScRansom 加密器目前正在积极开发中。结合 ScRansom 转向 LockBit 的事实，这表明 NoName 显然仍在进行着进一步更新。

国内勒索软件态势抬头，9 月多起勒索事件

2024 年 9 月 11 日，勒索软件团伙 Hunters International 声称对中国工商银行伦敦分部进行了网络攻击，并窃取了超过 520 万份文件，总计 6.6TB 的数据。该团伙在暗网上公布了这一信息，并设定了 9 月 13 日为支付赎金的最后期限，威胁若不满足其要求，将公开所有窃取的数据。

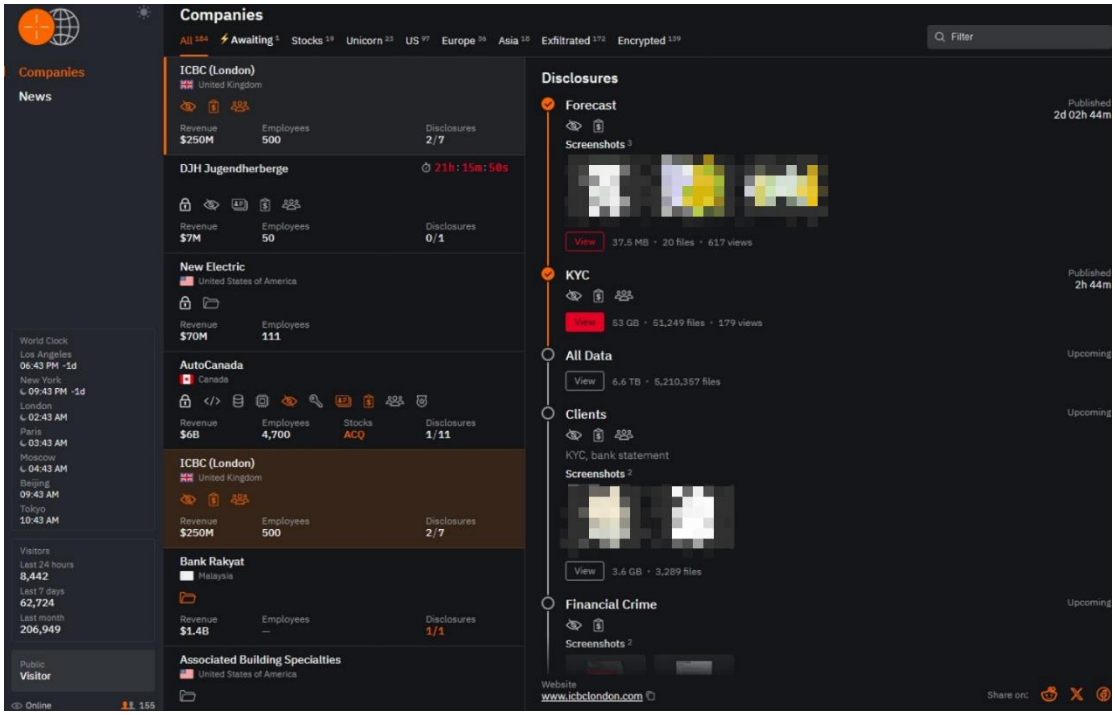

图 4. Hunters International 发布的工商银行泄露数据

此外 Killsec 勒索软件也在 9 月份于其官网上放出了据称是窃取自国内某政府单位的数据支付链接，这些数据包括但不限于：在中国机构与政府部门内的个人、行政、财务、审核流程等敏感信息。

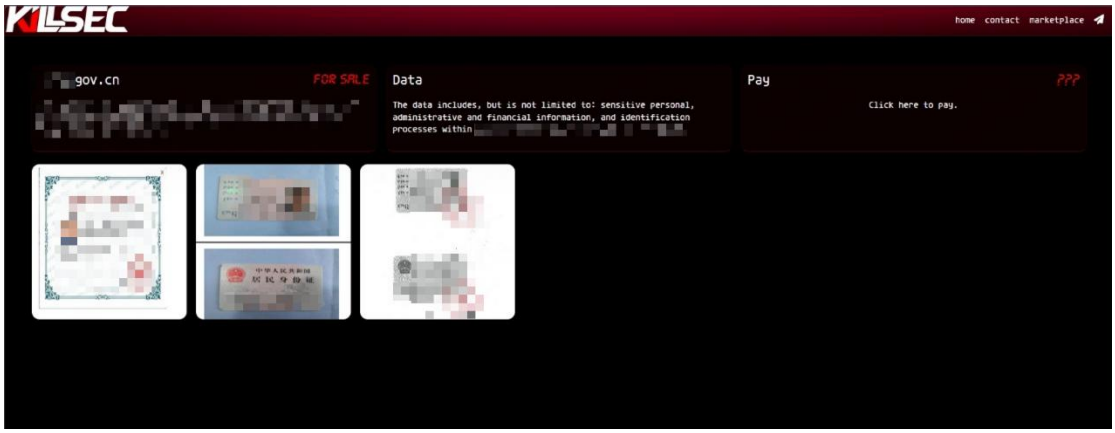

图 5. KillSec 发布的国内某政府单位泄露数据

黑客信息披露

以下是本月收集到的黑客邮箱信息:

itechsupport@onionmail.org	lcrypt@mailum.com	Fat32@airmail.cc
itschance@disroot.org	lcrypt@tuta.com	hashtreep@waifu.club
slamrestore1@gmail.com	mqpoa123@onionmail.org	Hoeosi@airmail.cc
moneyistime@mailum.com	mqpoa098@onionmail.org	MyFile@waifu.club
nemesis@888recover.4wrd.cc	helpdesk101@onionmail.com	Qyxugani@airmail.cc
nemesissupport@firemail.cc	imd3admi@gmail.com	Rast@airmail.cc
brahma2023@onionmail.org	maind3ad@gmail.com	user1@email.com
yourmaster1010@proton.me	foheg17549@marchub.com	BaseData@airmail.cc
razrhelp@firemail.cc	mantis1991@tuta.io	cwsp@tuta.com
jasalivan@420blaze.it	datarestore@cyberfear.com	pomocit01@surakshaguardian.com
ja.salivan@keemail.me	test@yadas.com	pomocit01@kanzensei.top
yan.laowang@mailfence.com	backup@waifu.club	decryptprof@qq.com
back777@tuta.io	BaseData@airmail.cc	therealencrypt@outlook.com
back777@cock.li	BitCloud@cock.li	ecrypter.files@gmx.com
blackpro.team24@onionmail.org	dataserver@airmail.cc	lerchsilas125@gmail.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）。

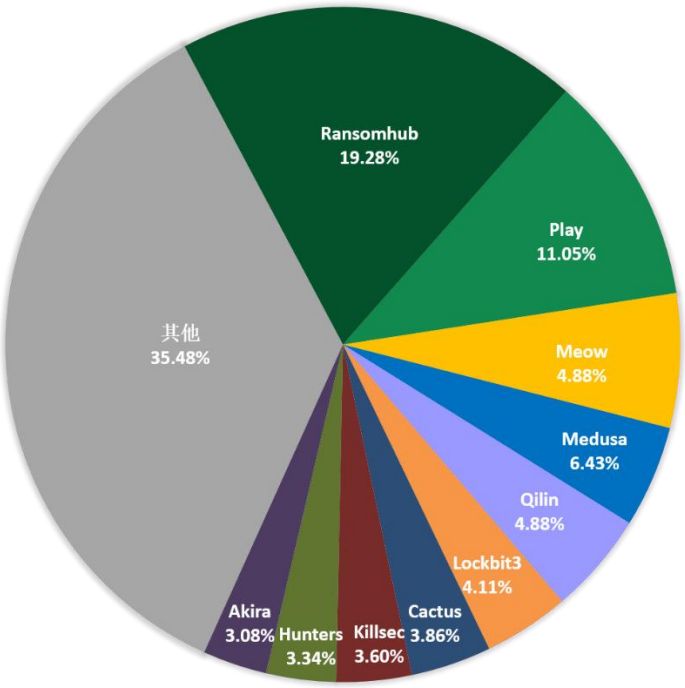

图 6. 2024 年 9 月通过数据泄露获利的勒索软件家族占比

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 388 个组织/企业遭遇勒索攻击，其中包含中国 5 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 3 个组织/企业未被标明，因此不在以下表格中。

verco.co.uk	Omega Industries	mechdyne.com
Community Hospital of Anaconda	Pacific Coast Building Products	Starr-Iva Water & Sewer District
BELL DATA, Inc	Thompson Construction Supply	Karakaya Group
Travel Alberta	Jackson Paper Manufacturing	CNPS Cameroun
IDEALEASE INC	Visionary Homes	www.jatelindo.co.id
Control Panels USA	KW Realty Group	allamericanpoly.com
Spectrum Industries	Capital Printing	Charles Darwin School
Magenta Photo Studio	virainsight.com	Cathedral Prep (villalan.edu)
Brechbuhler Scales Inc	Juice Generation	S. Walter Packaging
MDSi INC	River Region Cardiology	Clatronic International GmbH

	Associates	
carlile-group.com	Greene Acres Nursing Home	Advanced Physician Management Services LLC
sacredheart.southwark.sch	aroma.com.tr	Arville
mctas.org.au	rarholding.com	ICBC London
mnpl.com.sg	Fritzøe Engros	Ladov Law Firm
itap.nacc.go.th	Wilson & Lafleur	Regent Care Center
TOTVS	Wertachkliniken.de	www.vinatiorganics.com
Lee Hoffoss Injury Lawyers	a1mobilelock.com	Elgin Separation Solutions
McAbee Construction, Inc	patricksanderscompany.com	Bel-Air Bay Club
decalesp.com	thinksimple.com	Evans Distribution Systems
Isola	pesprograms.com	Weldco-Beales Manufacturing
Sub-Zero, Wolf, and Cove	palmfs.com	PIGGLY WIGGLY ALABAMA DISTRIBUTING
Plastics Plus	kennedyfunding.com	Joe Swartz Electric
MacGillivray Law	advbe.com	Virginia Dare Extract Co.
Freshstart Credit Repair	Sunrise Farms	Southeast Cooler
Andantex USA	libertyfirstcu.com	rupicard.com
weisermemorialhospital.org	Nusser Mineralöl GmbH	IDF and Mossad agents
porter.in	avl1.com	Vickers Engineering
Affirm Agency	tims.com	Controlled Power
poorvika.com	bspcr.com	Arc-Com
InteriorWorx Commercial Flooring	lakelandchamber.com	HDI
Performance Food Centers	yesmoke.eu	Myelec Electrical
Reutter	efile.com	Qeco/coeq
G/S Solutions	paybito.com	E-Z Pack Holdings LLC
Condere Ip, Infracom Group	Structural Concepts	Bank Rakyat
The Rubber Resources	Vidisco	americagraphics.com
Classic Business Products	IIB (Israeli Industrial Batteries)	City of Pleasanton, California
Garvey	Plaisted Companies	Pennsylvania State Education Association
Divine Interprises INC	Bertelkamp Automation	Battle Lumber Co.
DINAS Corp	DJH Jugendherberge	www.unige.it
4B Components	Prentke Romich Company	www.dpe.go.th
Alvan Blanch	agricola	www.bsg.com.au
OffRoadAction	Amerinational Community Services	www.avf-biomedical.com
Moeller Door and Window	Providence Public School Department	Appellation vins fins
cdc-biodiversite.fr	AZPIRED	schynsassurances.be
SaniRent	Compass Group	pv.be
markdom.com	Chernan Technology	kahle cpa

nfe.fazenda.gov.br	www.galloway-macleod.co.uk	Smart Source, Inc.
appweb.usinacoruripe.com.br	globe.com.bd	atlanticice.com
Soreq NRC	satiagroup.com	Phoenix Air Conditioning & Heating
rockymountaingastro.com	duopharmabiotech.com	Exitz Technologies
www.contegritygroup.com	tendam.es	kashima-coat.com
PipelBiz.com	ringpower.com	Stratford School Academy
Southern Fire Sprinkler	www.quenotedeporten.com	cardiovirginia.com
Røros Hotell	*.gov.cn	Prosolit
Direct Access Partners	www.plumbersstock.com	Grupo Cortefiel
infina.vn	www.nikpol.com.au	Nocciole Marchisio
Benny Gantz Hacked	capecodacademy.org	Elsoms Seeds
gccustommetal.com	natcoglobal.com	Millsboro Animal Hospital
actionfirepros.com	New Electric	briedis.lt
Xtera Communications	AutoCanada	America Voice
www.naniwa-pump.co.jp	gestiriego.com	CK Associates
www.law-taxes.pl	Sherr Puttmann Akins Lamb PC	Keya Accounting and Tax Services LLC
www.tokiwa-group.co.jp	peerlessumbrella.com	Arbitech (arb.local)
www.careco.se	thomas-lloyd.com	ctelift.com
www.vbrlogistica.com.br	Port of Seattle/Seattle-Tacoma International Airport (SEA)	SESAM Informatics
Mile Hi Foods	Rsp	riomarineinc.com
Shenango Area School District	Protective Industrial Products	champeau.com
KGK Group	Inktel	Custom Security Systems
Zimmerman & Walsh	Hariri Pontarini Architects	cda.be
kumhotire.com	Baskervill	belfius.be
chcm.us	Multidata	dvv.be
Schäfer, dein BäckerGmbH & Co. KG	www.8010urbanliving.com	cbt-gmbh.de
lolaliza.com - 250kk	www.faithfc.org	Inglenorth.co.uk
English Construction Company	www.adantia.es	cps-k12.org
tolsa.com	topdoctors.com	inorde.com
Concord Management Services	www.taperuvicha.com	tri-tech.us
Lawrie Insurance Group	Robson Planning Group Inc	PhD Services
Luso Cuanza	SuperCommerce.ai	kawasaki.eu
ATG Communications Group	EnviroNET Inc	phdservices.net
Hairstore	oipip.gda.pl	Baird Mandalas Brockstedt LLC
IP blue Software Solutions	kryptonresources.com	www.towellengineering.net
Pennvet.com	www.tta.cls	rhp.com.br
triverus.com	Cruz Marine (cruz.local)	Imetame
hindlegroup.com	Environmental Code Consultants Inc	SWISS CZ

kjtait.com	MCNA Dental 1 million patients records	Cellular Plus
www.amchar.com	ExcelPlast Tunisie	Arch Street Capital Advisors
gsdwi.org	accurateraillroad.com	Hospital Episcopal San Lucas
PetEdge	advantagecdc.org	www.parknfly.ca
libraries.delaware.gov	www.atlcc.net	Western Supplies, Inc
Hughes Gill Cochrane Tinetti	lafuturasrl.it	Crain Group
Menninger Clinic	dowley.com	Bakersfield
Israel defense minister private photos	apexbrasil.com.br	Farmers' Rice Cooperative
cottlesinc.com	fivestarproducts.com	Parrish
Crown Mortgage Company	ignitarium.com	Seirus Innovation
First Choice Sales & Marketing Group (First Choice)	nfcaa.org	www.pcipa.com
Frigocenter	Emtel	www.galgorm.com
Partners Air	EAGLE School	OSDA Contract Services
Solutii Sistemas	www.rockymountaingastro.com	www.bennettcurrie.co.nz
Nova Sinseg	salaam.af	ych.com
Model Engineering	Rextech	plannedparenthood.org
BroadGrain Commodities	Like Family's	idom.com
tellurianinc.org	UNI-PA A.Ş	Sunrise Erectors
Eurobulk	Gino Giglio Generation Spa	gardenhomesmanagement.com
www.datacampos.com	OnePoint Patient Care	simson-maxwell.com
cucinatagliani.com	Retemex	balboabayresort.com
cmclb.com	ORCHID-ORTHO.COM	flodraulic.com
Kravit, Hovel & Krawczyk SC	ecbawm.com	mcphillips.co.uk
f-t.com	jatelindo	rangeramerican.com
oleopalma.com.mx	mivideo.club	United Methodist Retirement Homes, Inc
Dlamond Contracting, LLC	Micron Internet	W. A. Richardson Builders, LLC
Avi Resort & Casino	TECHNOLOG S.r.l.	wilmingtoncc.org
medicheck.io	FD Lawrence Electric	VOP CZ
Benny Gantz	True Family Enterprises	Turman
Brown Bottling Group	Dimensional Merchandising	Kingsport Imaging Systems
bakpilic.com.tr	Creative Playthings	www.amberbev.com
Idre Fjäll	Law Offices of Michael J Gurfinkel, Inc	www.sanyo-bussan.co.jp
Pureform Radiology Center	Hostetler Buildings	www.pokerspa.it
Detroit Public TV	Associated Building Specialties	Removal.AI
ten8fire.com	VIcom Corporation	Project Hospitality
Fabrica Industrial Machinery & Equipment	HB Construction	www.schneider.ch
Graminex	Arch-Con	Shomof Group

Canstar Restorations	www.southeasternretina.com	www.sanyo-av.com
hanwa.co.th	Ascend Analytics (ascendanalytics.com)	San Francisco Sheriff's Department (sjcso.local)
Daughterly Care	Kingsmill Resort	www.electriforce.com
Woodard , Hernandez , Roth & Day	Carpenter McCadden and Lane LLP	ERoko Distributors + Colonial Countertops
savannahcandy.com	CSMR Agrupación de Colaboración Empresaria	Quálitas México
Acho.io	brunswickhospitalcenter.org	welland
Noble Environmental	thornton-inc.com	nhbg.com.co
Messe C		

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。

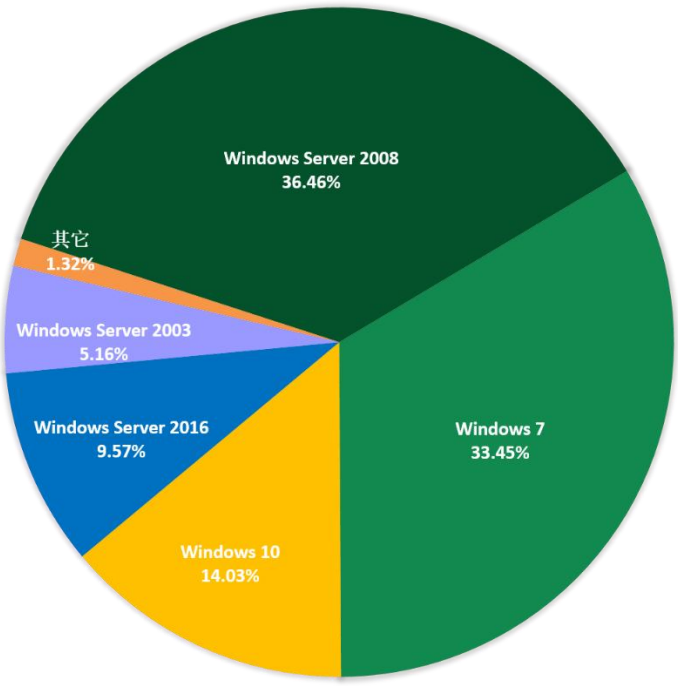

图 7. 2024 年 9 月受攻击系统占比

对 2024 年 9 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。

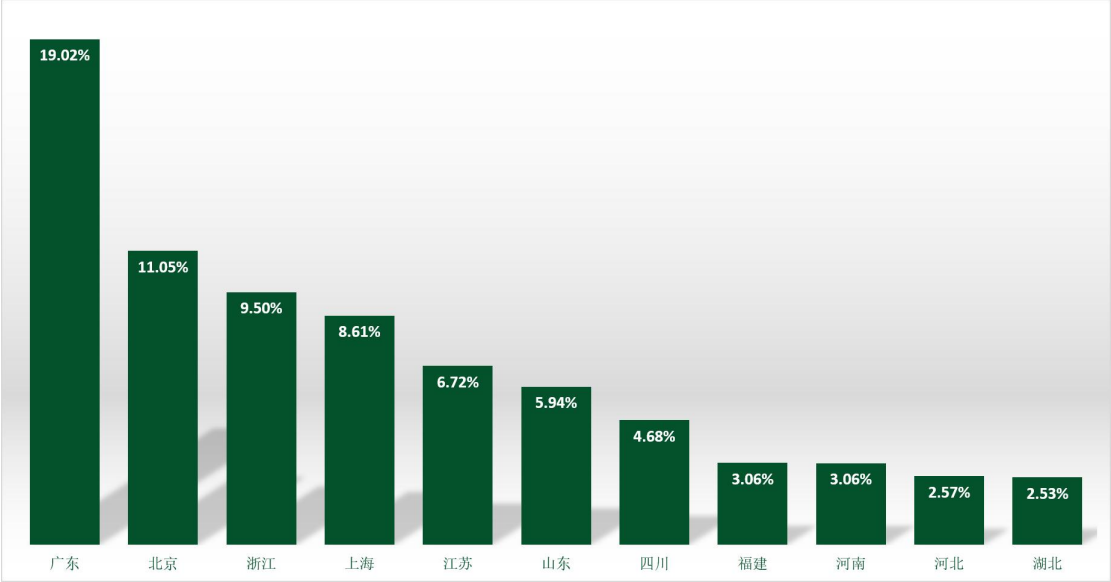

图 8. 2024 年 9 月国内受攻击地区占比排名

通过观察 2024 年 9 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。

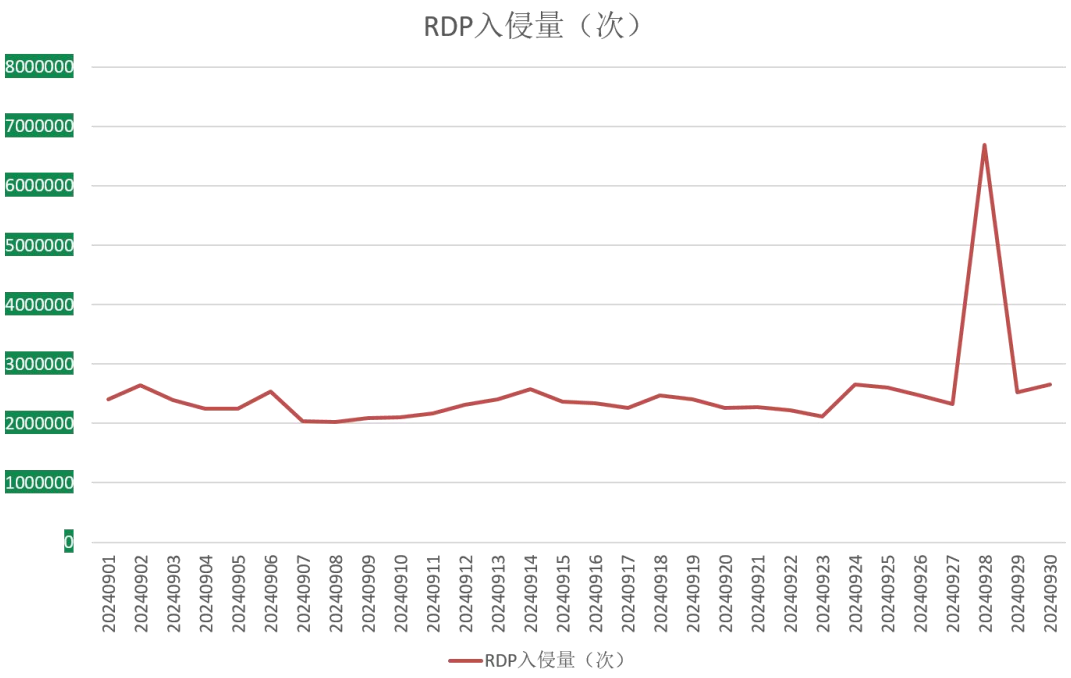

图 9. 2024 年 9 月监控到的 RDP 入侵量

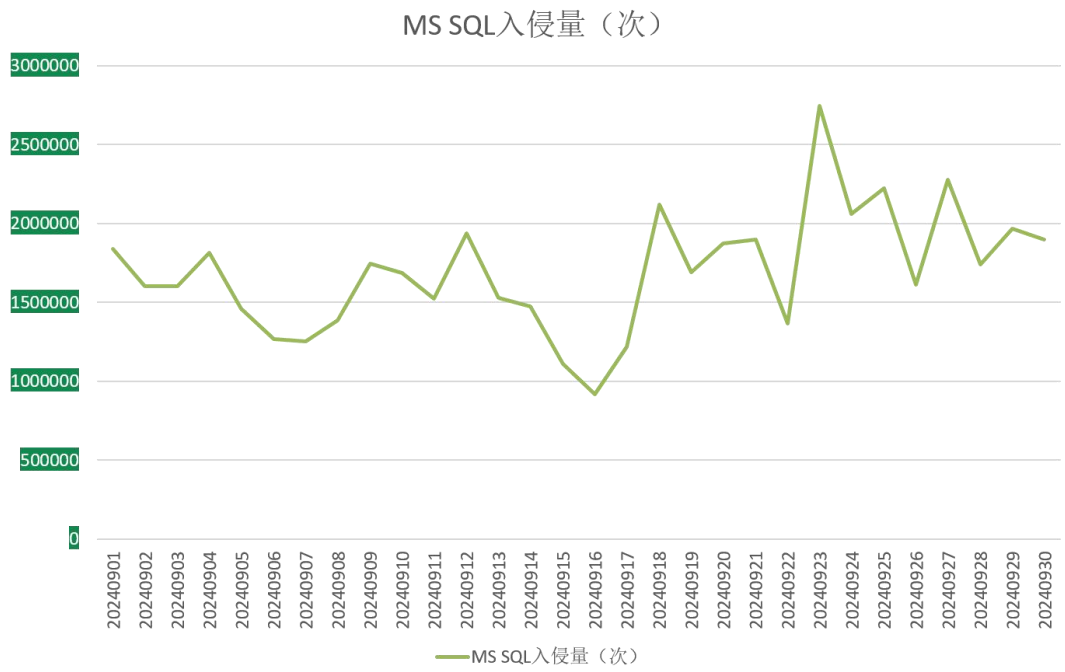

图 10. 2024 年 9 月监控到的 MS SQL 入侵量

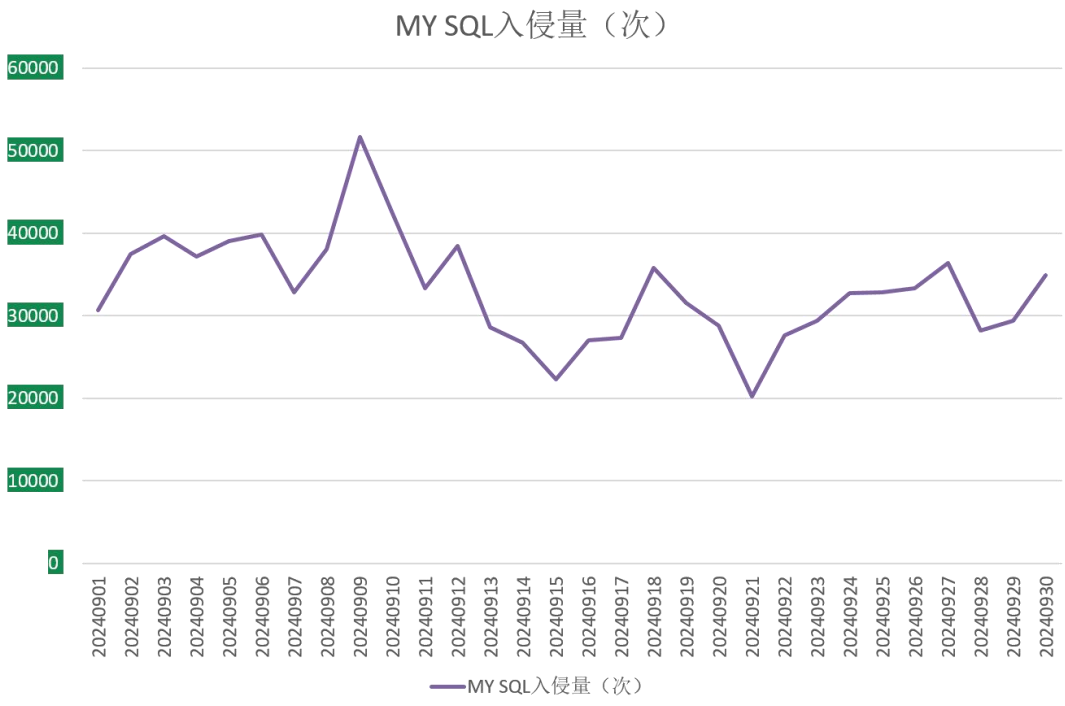

图 11. 2024 年 9 月监控到的 MYSQL 入侵量

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。

- rmallox：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。
- 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。
- src: 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。
- mallox：同 rmallox。
- mkp：同 src。
- devicdata：同 rmallox。
- bixi：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。
- wormhole：属于 Wormhole 勒索软件家族，由于被加密文件后缀会被修改为 Wormhole 而成为关键词。该家族主要的传播方式为：通过瑞友天翼软件漏洞发起攻击。
- baxia：同 bixi。
- lcrypt 属于 Anony 勒索软件家族，由于被加密文件后缀会被修改为 anony 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。

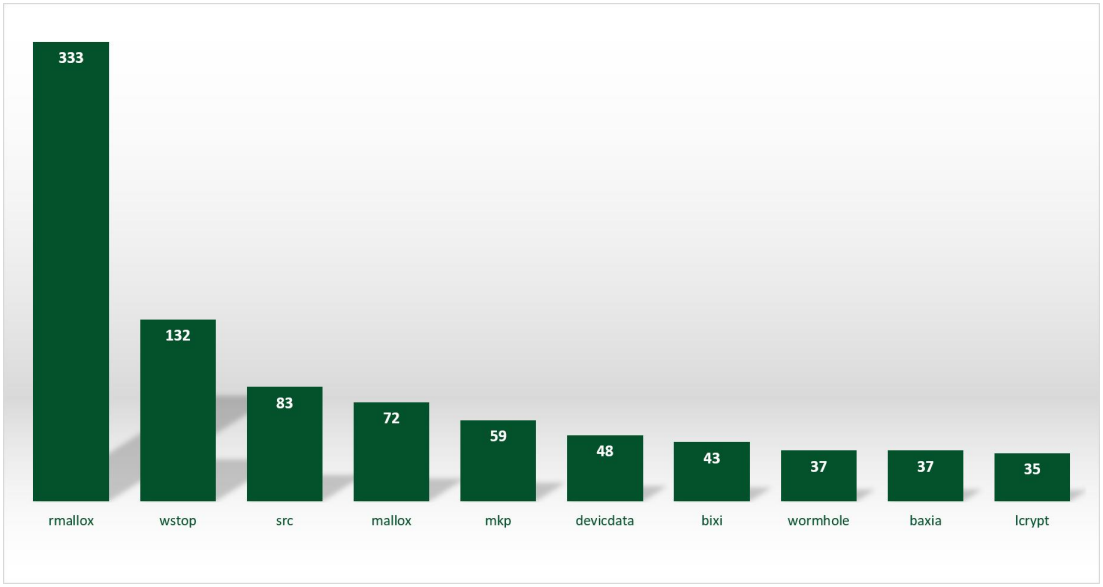

图 12. 2024 年 9 月反病毒搜索引擎关键词搜索排名

解密大师

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

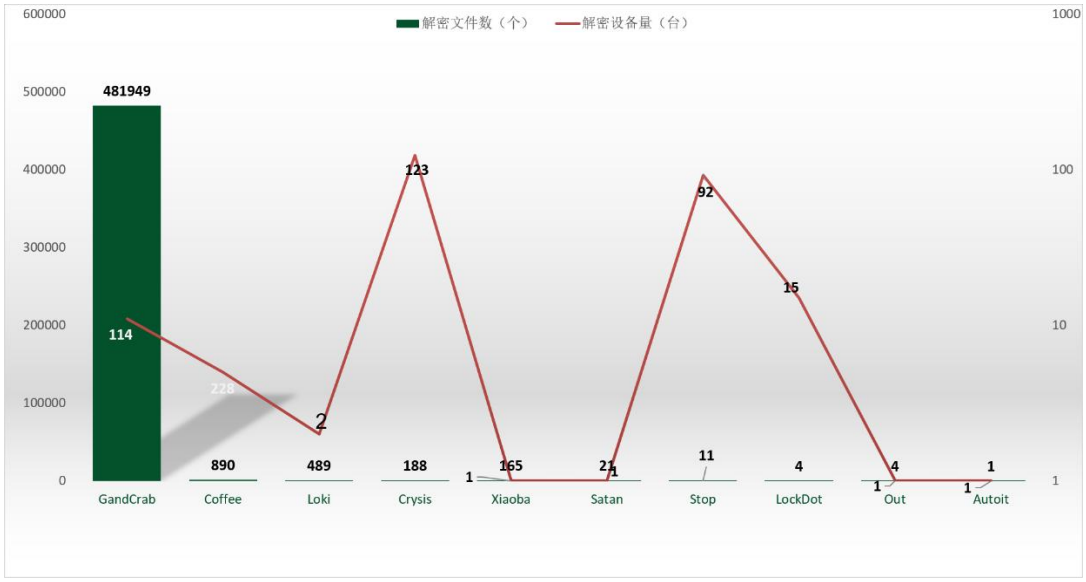

图 13. 2024 年 9 月解密大师解密文件数及设备数排名


360数字安全
数 字 安 全 的 领 导 者
360安全大脑