勒索软件流行态势分析

2024 年 7 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 7 月，全球新增的双重勒索软件家族有 Lynx、Cicada3301、Fog、MAD LIBERATOR、Pryx、Vanir Group。Fog 最早出现在 2024 年 5 月，并在 7 月开始通过其数据泄露网站对外发布受害者名单。新增的传统勒索软件家族有 ShadowRoot、Black4Over。

以下是本月值得注的部分热点：

1. 新的 Eldorado 勒索软件攻击 Windows 及 Vmware ESXi 虚拟机

2. 来德爱承认 6 月份遭遇勒索攻击后发生数据泄露事件

3. 洛杉矶高等法院因遭遇勒索软件攻击而关闭

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 36.02%居首位，第二的是 Makop 占比 22.46%，Anony 家族以 12.29%位居第三。

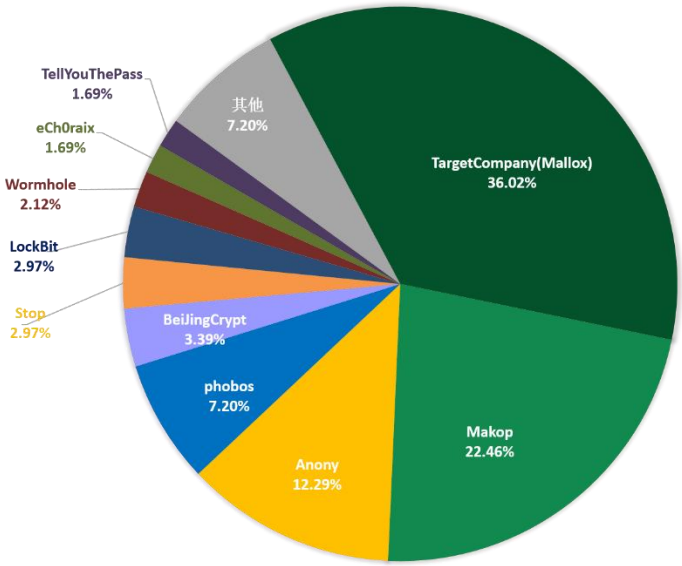

图 1. 2024 年 7 月勒索软件家族占比

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。

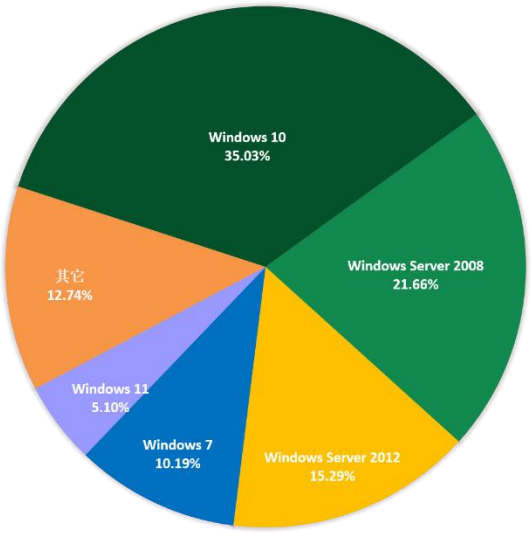

图 2. 2024 年 7 月勒索软件入侵操作系统占比

2024 年 7 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。

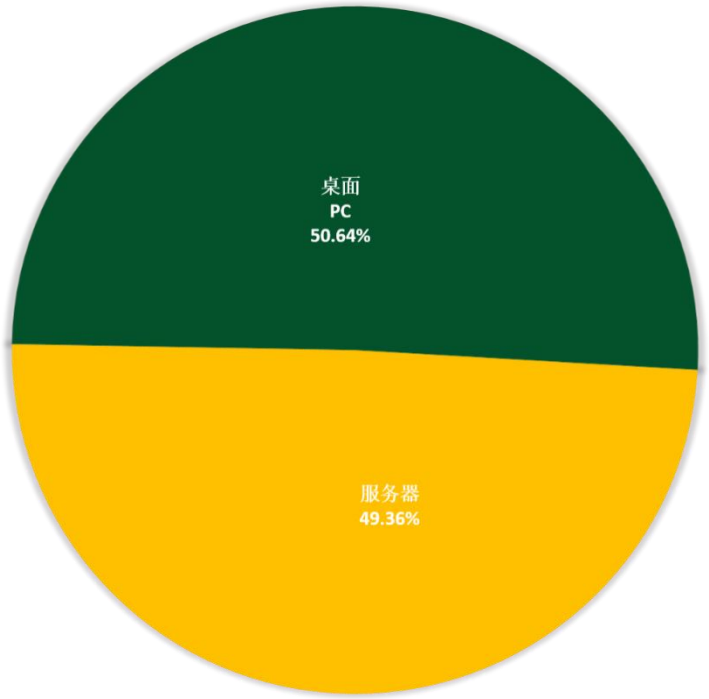

图 3. 2024 年 7 月勒索软件入侵操作系统类型占比

勒索软件热点事件

新的 Eldorado 勒索软件攻击 Windows 及 Vmware ESXi 虚拟机

一种名为“Eldorado”的新型 RaaS（勒索软件即服务）勒索软件于今年 3 月被首次发现，并带有针对性的攻击 VMware ESXi 和 Windows 平台。该勒索软件团伙据称已攻击了 16 个组织，其中大部分受害者在美国，涉及房地产、教育、医疗保健和制造业等领域。

网络安全研究人员监控到了“Eldorado”的活动，发现其幕后控制者在 RAMP 论坛上推广该勒索服务，并寻找有相关技术能力的合作伙伴加入项目。此外，Eldorado 还运营着一个数据泄露网站用于列出了受害者名单，但目前该网站尚无法访问。

Eldorado 是一款基于 Go 语言开发的勒索软件，可以通过两种具有相似功能的变种在 Windows 和 Linux 平台上进行文件加密操作。研究人员从提供 RaaS 的供应商手中取得了一个加密器以及其附带的用户手册，说明该加密器有适用于 VMware ESXi 虚拟机管理程序和 Windows 操作系统的 32 位及 64 位版本。根据分析发现，该勒索软件使用 ChaCha20 算法进行加密，并针对每台受害设备生成一个独有的 32 字节密钥和 12 字节初始向量。然后，使用 RSA 加密算法对密钥和初始向量进行加密，采用的是最优的非对称加密填充（OAEP）方案。加密完成后，文件会被添加“.00000001”的扩展名，并在系统的“文档”和“桌面”文件夹中放置名为“HOW_RETURN_YOUR_DATA.TXT”的勒索说明文件。另外，Eldorado 还利用 SMB 通信协议对网络中的共享设备进行加密，以最大程度地发挥其作用，并在被入侵的 Windows 机器上删除卷影副本，以防止受害者通过副本对文件进行恢复。同时，该勒索软件会跳过 DLL、LNK、SYS 和 EXE 文件，以及与系统启动和基本功能相关的文件和目录，以防止使系统无法启动或无法使用。最终，勒索软件会删除自身文件以避免被安全响应人员发现和分析。

安全研究人员表示：“虽然目前来看，Eldorado 是一个新出现的勒索软件组织而非此前的勒索软件组织的重生团队，但其在短时间内已展现出了对受害者数据、声誉和业务可用性的重大破坏能力。”

来德爱承认 6 月份遭遇勒索攻击后发生数据泄露事件

大型连锁药店来德爱在 6 月份遭受了一次网络攻击，随后确认发生了数据泄露事件，该事件被 RansomHub 勒索软件组织所宣称。

大型连锁药店来德爱在 7 月 12 日表示其正在调查今年 6 月份发现的一起网络攻击，并正在努力向受数据泄露影响的客户发送数据泄露通知。该公司还表示，在聘请外部专家解决此次攻击影响的过程中，已恢复了所有受影响的系统。尽管来德爱没有透露在数据泄露事件中被访问的客户数据内容以及受影响的个人数量，但该公司表示，此次数据泄露事件并未涉及健康或财务信息。

尽管来德爱尚未透露 6 月份袭击事件的幕后黑手是谁，但这份声明是在 RansomHub 勒索软件团伙已声明表示入侵了这家药品巨头的系统并窃取了客户数据之后发布的。

在 RansomHub 的声明中，明确表示在获取了 Riteaid 网络的访问权限后，已获取了超过 10GB 的客户信息，相当于约 4500 万人的个人信息。这些信息包括姓名、地址、dl_id 号码、出生日期和 Riteaid 推广号码。在将来德爱添加到其泄露网站后，据传由于该公司已停止了赎金谈判，勒索软件组织分享了一些据称是被盗数据的截图作为证据，并表示两周内将公布所有数据。

根据来德爱方面的最新统计，此次数据泄露事件已经影响到其约 220 万名客户的隐私信息。

洛杉矶高等法院因遭遇勒索软件攻击而关闭

美国最大的地方法院——洛杉矶县高等法院于 22 日关闭了其 36 个法院的所有地点，以恢复在 19 日遭受勒索软件攻击的系统。这起尚未被勒索软件组织公布的攻击影响了洛杉矶高等法院的整个网络。此次攻击也波及了包括“MyJuryDuty Portal”门户网站在内的外部系统，以及一些如案件管理系统在内的内部系统。

此次攻击在当地时间 20 日时被首次披露，当时该法院透露袭击开始于 7 月 19 日星期五清晨。洛杉矶高等法院还(LASC)表示，此次事件与全球范围内影响 Windows 系统的 CrowdStrike 更新故障无关。在发现遭到攻击后，LASC 被迫立即关闭了所有网络系统以遏制漏洞，这些设备很可能至少要到下周二才能恢复并重新上线。法院补充说，他们没有发现任何证据表明被入侵系统的数据被泄露，目前正与加州紧急服务办公室（CALOES）以及地方、州和联邦执法机构合作，调查此次事件并评估其影响。

虽然法院仍在迅速推进恢复和恢复阶段，但截至 21 日晚间，许多关键系统仍处于离线状态。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

Barbara.li@gmx.com	admin@stex777.xyz	bitsupportx@protonmail.com
emily.florez@zohomail.com	ramachandra7@india.com	bitsupportx@cock.li
getdataback@rambler.ru	5j3Kyz7F2@gmail.com	decrypt@europe.com
amaya_payne2@aol.com	decrypthelp@cock.li	reservereserv@airmail.com
nikki.lond2@aol.com	skynet45@cock.li	emmanuel.earsome@aol.com
admin@sectex.net	skynet45@tutanota.com	mclainmelvin@aol.com
admin@sectex.world	delta@onionmail.org	GetDecoding@zimbabwe.su
boost	delta@bingzone.net	getdecoding@msgsafe.io
boston.crypt@tuta.io	decryptinfo@protonmail.com	Client9522@tutanota.com
koreadec@tutanota.com	decryptinfo@cock.li	decfile1@protonmail.com
yourrealdecrypt@airmail.cc	future911@tuta.io	rapax123@protonmail.com
Enigmawave@zohomail.com	dragon2024@onionmail.org	michael_ethan@zohomail.eu
helpservice@cyberfear.com	dragon2024@tutanota.com	michael.ethan@onionmail.org
youhau@tutamail.com	paybit@aol.com	valorantskins108@gmail.com
China.Helper@aol.com	paybit765@aol.com	jinwooksransome@gmail.com
China.Helper@india.com	pexdatax@gmail.com	geometrical@geometrical.ransome.kr

sergev_petrov1983@mail.ru	admin@spacedatas.com	duca17512@gmail.com
clovergroup@skiff.com	teamdecrypt@disroot.org	lord_bomani@keemail.me
Helpyoudc1966@Gamil.com	teamVV@cock.li	jbomani@protonmail.com
zkungfu@skiff.com	xcsset@criptext.com	Bomani@Email.Com
anony@mailum.com	xcsset@aol.com	salesrestoresoftware@firemail.cc
ithelp08@decorous.cyou	squadhack@email.tg	salesrestoresoftware@gmail.com
ithelp08@wholeness.business	back_data@foxmail.com	getbtc@aol.com
mail4restore@swismail.com	getdecoding@protonmail.com	steloj@bk.ru
welcome24dat@outlook.com	prancesonce@tuta.io	steloj@lycos.com
returnal_data@proton.me	prancesonce@cock.li	stelo@onet.eu
returnaldata@airmail.cc	ebc83e48b03b390223e3f0b9eb2983d6	admin@fentex.net
returnal_data@tuta.io	operator@cypherx.info	admin@fentex.world
AdminLoki@onionmail.org	Operatorb@cock.li	admin@datastex.club
LokiAdmin@mail2tor.com	fidelio.bartyn@aol.com	dkqcnr@cock.li
8filesback@onionmail.org	glynnaddey@aol.com	d.hanry@tutamail.com
foo8tbFpc@gmail.com	888@cock.email	LBfdgpo.info.ru@onionmail.com
my0day@aol.com	getscoin3@protonmail.com	Rdpdik6@gmail.com
daysupp@aol.com	getscoin@tuta.io	Rdpp771@gmail.com
biashabtc@redchan.it	decrypt@files.mn	purchase@lnt-corp.com
Bit_decrypt@protonmail.com	techwin@post.cz	xwolf69@onionmail.org
1Buba@protonmail.com	timesungroup@skiff.com	admin@lntdeal.com
filesgetback@protonmail.ch	marshall@airmail.cc	purchase@lntdeal.com
getthefiles@airmail.cc	orderof@tuta.com	devos-2686@libertymail.net
fastrecovery@onionmail.org	Rileyb0707@aol.com	support@bloomscollect.com
fastrecovery2@msgsafe.io	Rileyb0707@cock.li	93048decoder@tutanota.com
restoreassistance@decorous.cyou	tiprltd@skiff.com	pasomnicadecryption@gmail.com
restoreassistance@wholeness.business	bluecrap8@gmail.com	NJUnju@skiff.com
BAD.JERRY@AOL.COM	bluecrap@my.com	frankmoffit@aol.com
BADJERRY@COCK.LI	diane.freen2@aol.com	emcrypts@tutanota.de
admin@stex777.com	opalburgh@aol.com	russoschwartz@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）。

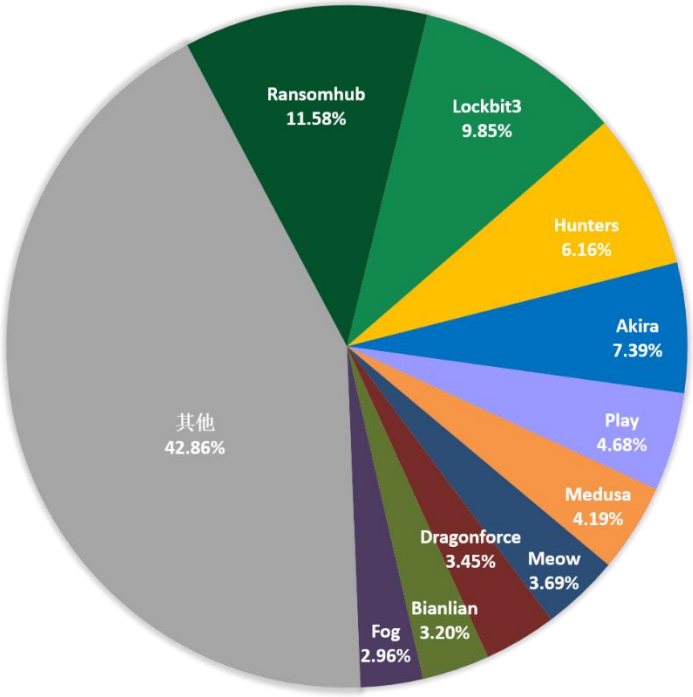

图 4. 2024 年 7 月通过数据泄露获利的勒索软件家族占比

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 406 个组织/企业遭遇勒索攻击，其中包含中国 6 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 9 个组织/企业未被标明，因此不在下表格中。

EBL PARTNERS (construction|interiors), Florida	CALDAN Conveyor	Odfjell Drilling
EFRON LAW FIRM	forestparkga.gov	Golan Christie Taglia
wgma.org	Regas (regasenergy.com)	First Commonwealth Federal Credit Union
biggreenegg.com	Dimbleby Funeral Homes	Apex Global | Big leak outlooks - 2tb.
nydj.com	John Gallin & Son	Sherbrooke Metals
www.pharm-int.com	Industrial Bolsera	luzan5.com
fingersstore.com	RhinoCorps	BrownWinick
Florence Cement Company, Inc.	Congoleum	Texas Alcohol and Drug Testing Service
Find Great People	Waupaca Middle School	Kenya Urban Roads Authority
Carlex Glass Luxembourg S.A.	sigmacontrol.eu	Carigali Hess Operating Company
Durham Manufacturing	siParadigm	gbhs.org 07/12 Publication 51gb
Kleven Construction	eurovilla.hr	The Coffee Bean & Tea Leaf

BRASPRESS	Notarkammer Pfalz	State of Alabama - Alabama Department Of Education
Sable International.	Win Systems	erne
www.srmedicalcenter.org	www.byzan.com	Preferred IT Group
sandytownshippolice.org	maingroup	ARISTA
atcdi.com.cn	thesourcinggroup.com	The Seattle Public Library
frilot.com	LawDepot	Wagner-Meinert
pbw-india.com	Association Management Strategies(AAMC.local)	painproclinics.com
agapefrance.org	CIMP.COM	www.zepter.de
ciberviaxesespecial.net	globes	www.riteaid.com
eastern-sales.com	aa munro insurance	www.donaanita.com
City of Columbus, Ohio	Wichita State University Campus of Applied Sciences and Technology	perfeitaplastica.com.br
St. Thomas Aquinas High School	Sibanye-Stillwater	www.respirarlondrina.com.br
Lake Washington Institute of Technology	Acadian Ambulance (US)	American Golf
Network Communications Group	SH Pension	Hyperice
verwarmingheyndrickx.be	memc.com	diligentusa.com
stb.ro	Guaranteed Supply Company	Uae gov breach
chubb-bulleid.co.uk	RiverSoft	Image Microsystems
leonardssyrups.com	Cole Technologies Group	www.lynchaluminum.com
westernwyomingbeverages.com	Family Wealth Advisors Ltd.	www.eurostrand.de
demos.fr	Mars 2 LLC	Financoop
denkaiamerica.com	www.garudafood.com	Sigma
Macadam Europe	Queens County Public Administrator	www.netavent.dk
Gemicar	Reward Hospitality from EFC Group	Sonol (Gas Stations)
welevelup.com	Doodle Tech	www.bfcsolutions.com
Olschewski Davie	www.kumagaigumi.co.jp	concorddirect.com
www.chsd117.org	H&H Group	Texas Electric Cooperatives
udch.in.th	Jariet Technologies	The 21st Century Energy Group
SAGE Publishing	Arcmed Group	City of Cedar Falls
labor-koblenz.de	Leech Lake Gaming	P448
BASF - Nunhems	KuiperCompagnons	Usina Alta Mogiana S/A
The Gill Corporation	www.glowfm.nl	Beowulfchain
Crownlea Group	Law Offices of the Public Defender - New Mexico	Qinao
Priefert	Infomedika	Athlon
Al-Karam Textile Mills Pvt	Northeast Rehabilitation Hospital Network	Ronglian Group
Gentlemen Group GmbH	Seamon Whiteside	Unitedpropertiescorp.com
The Greenhouse People	Santa Rosa	Inland Audio Visual

True Blue Environmental	customssupport.be	Indika Energy
Ascent Group	fbrlaw.com	Heidmar
zoppo.com	troyareasd.org	Cedar Technologies
intrama-bg	barkingwell.gr	REPLIGEN
hanoverhill.com	wattlerange.sa.gov.au	HITC.VN
New Jersey City University	claycountyin.gov	Excelsior Orthopaedics
ayurcan	iteam.gr	Allied Industrial Group
Computer Networking Solutions	albonanova.at	Esedra
Kalaswire.com	lothar-rapp.de	Raffmetal Spa
Community Care Alliance	joliet86.org	Federated Co-operatives
www.neurologicalinstitute.com	goldstarmetal.com	Guhring USA
www.whittakersystem.com	glsco.com	noab.nl
www.castelligroup.com	paysdelaloire.fr	Viasat
City of Cold Lake	all-mode.com	Olympus Group
pioneerworldwide.com	www.erma-rtmo.it	MYC Media
summervillepolice.com	metalfrio.com.br	a-g.com 7/10/24 - data publication 38gb (150K)
blankstyle.com	www.newcastlewa.gov	baiminstitute.org
Augusta Orthopedic	pgd.pl	The Wacks Law Group
Karvo Companies, Inc.	texas tech university	pomalca.com.pe
Planet Group International	encore	Center for Human Capital Innovation (centerforhci.org)
LITEON	Modernauto	waupacacounty-wi.gov
Lago Group Spa	Gandara Center	ws-stahl.eu
Villarreal and Begum Law Firm	Hayden Power Group	homelandvinyl.com
ach.co.th	assih.com	eicher.in
bpjaguar.com	norton.k12.ma.us	National Health Laboratory Services
oficina.oficinadasfinancas.com.br	energateinc.com	Un Museau
Global Industry Analysts	plantmachineworks.com	Lexibar
Daikin	piedmonthoist.com	Haylem
Miami Gardens Florida	gptchb.org	Legend Properties, Inc.
Nuclep	MIPS Technologies	Elyria Foundry
Andersen Tax	labline.it	Texas Recycling
The Physical Medicine Rehabilitation Center	ZSZAALEJI.cz	INDA's
glnf.fr	www.hlbpr.com	Innerspec Technologies
Speed Advisory	isometrix.com	Prairie Athletic Club
mrhme.org	A.L.P. Lighting Components	Fareri Associates
The Computer Merchant	VITALDENT	Island Transportation Corp.
Williams Construction	MINISTERO DELLA CULTURA	Transit Mutual Insurance Corporation
Gateway Extrusions	MONTERO & SEGURA	hcri.edu
panitchlaw.com	CROSSWEAR TRADING LTD	Abileneisd.org
cminsulation.com	Cities Network	Coquitlam Concrete

baytoti.com	ZB Financial Holdings	Multisuns Communication
Golden Business Machines	The Law Office of Omar O. Vargas, P.C.	Creative Realities
Odyssey Fitness Center	STUDIO NOTARILE BUCCI – OLMI	gerard-perrier.com
OfficeOps	GroupePRO-B	sequelglobal.com
BK Aerospace	Geelong Lutheran College	Alimac
D&K Group, Inc.	Asbury Theological Seminary	Explomin
Voss Belting & Specialty	Djg Projects	badel1862.hr
Tri-Star Display	Verweij Elektrotechniek	ramservices.com
NARSTCO	Alvin Independent School District	aedifica.com
Gendron & Gendron	West Allis-West Milwaukee School District	foremedia.net
Odessa College	German University of Technology in Oman	www.swcs-inc.com
Environmental DesignInternational	ceopag.com.br / ceofood.com.br	RCBC.edu Data Breach: over 30,000 University Applications Exposed
KMLG	www.benchinternational.com	valleylandtitleco.com
Empereon Constar	www.cameronhodges.com	merrymanhouse.org
Norther n Bedford County School District (nbcsc.org)	Braum's Inc	fairfieldmemorial.org
Physical & Occupational Therapy Examiners ofTexas	Lantronix Inc.	www.daesangamerica.com
CertiCon	HOYA Corporation	www.finecopneumatica.com
EHS Partnerships	Mainland Machinery	www.hauptmann.at
Insula Group	SBRPCA	Salton
e21c.co.uk	verco.co.uk	P1 Technologies
crimsonwinegroup.com	Nuevatel	Conexus Medstaff
Stienemann	atos.com	www.sfmedical.de
Pojoaque	posiplus.com	Strauss Brands
Kusum Group of Companies	hpecds.com	Harry Perkins Institute of medical research
TheLutheranFoundation	Amino Transport	WheelerShip
Melchers Singapore	Innovalve Bio Medical	Grand Rapids Gravel
Valisana	integraservices	Franciscan Friars of the Atonement
simple-solution-systems	XENAPP-GLOBER	Elite Fitness
Bunkhouse Group	Gramercy Surgery Center	Gray & Adams
Playa Vista Job Opportunities and Business Services	Goede, DeBoest & Cross, PLLC.	Vermont Panurgy
Accelon Technologies Private	Sheba Medical Center	floridahealth.gov
SOLOMONUS.COM	usdermpartners.com	www.nttdata.ro
Owens Valley Career Development Center	Gibbs Hurley Chartered Accountants	Super Gardens
Coffrage LD	ComNet Communications	Hampden Veterinary Hospital

Vivara	MS Ultrasonic Technology Group	SYNERGY PEANUT
tccfleet.com	RZO	Indonesia Terkoneksi
petroassist.co.uk	thompsoncreek.com_wa	Ethypharm
ORBINOX	northernsafety.com_wa	latinusa.co.id
SKC West	greenlightbiosciences.com	kbc-zagreb.hr
Uw logistieke partner	royal brighton yacht club	TUV Rheinland AG
Betances Health Center	valecard	maxcess-logistics.com
BLEnergy	townandforest.co.uk	Independent Education System
Jack "Designer" Sparrow.	Hewlett Packard Enterprise	Bartlett & Weigle Co. LPA.
American Acryl	BCS Systems	Guhring
Electroalfa		

表格 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。

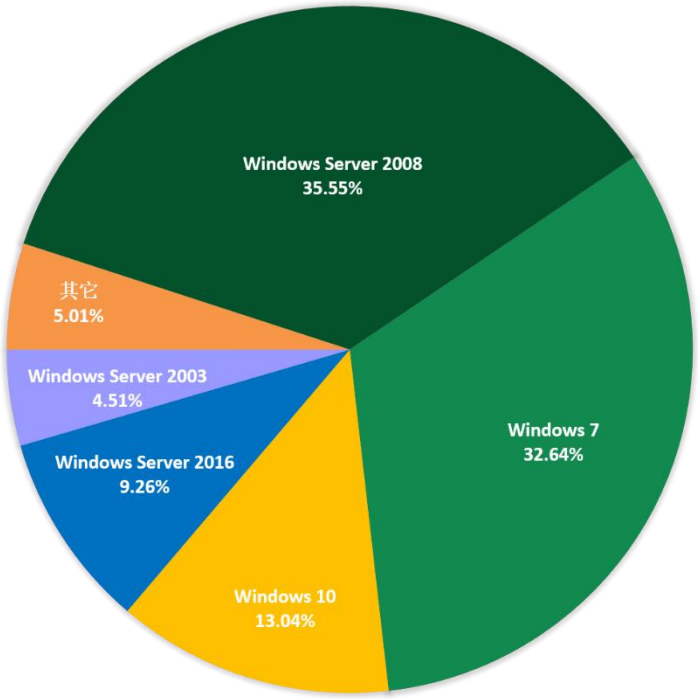

图 5. 2024 年 7 月受攻击系统占比

对 2024 年 7 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。

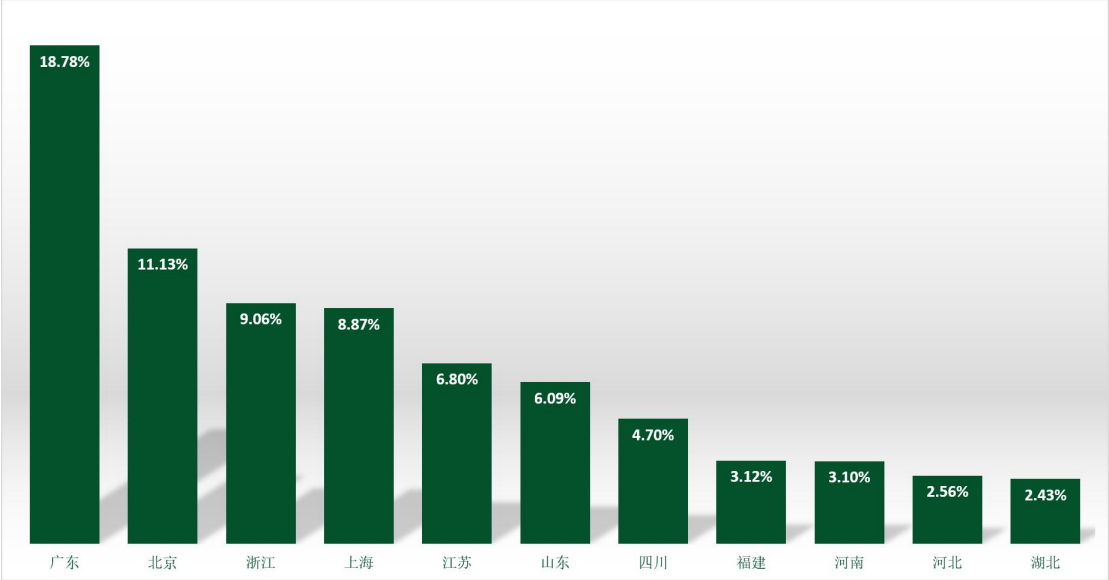

图 6. 2024 年 7 月国内受攻击地区占比排名

通过观察 2024 年 7 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。

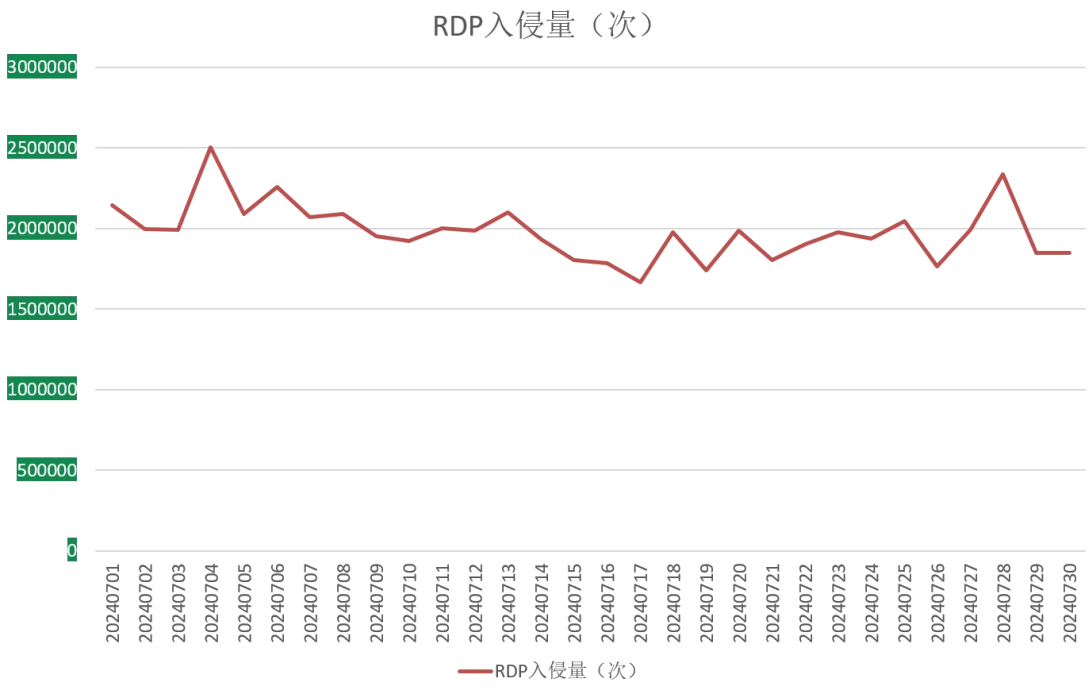

图 7. 2024 年 7 月监控到的 RDP 入侵量

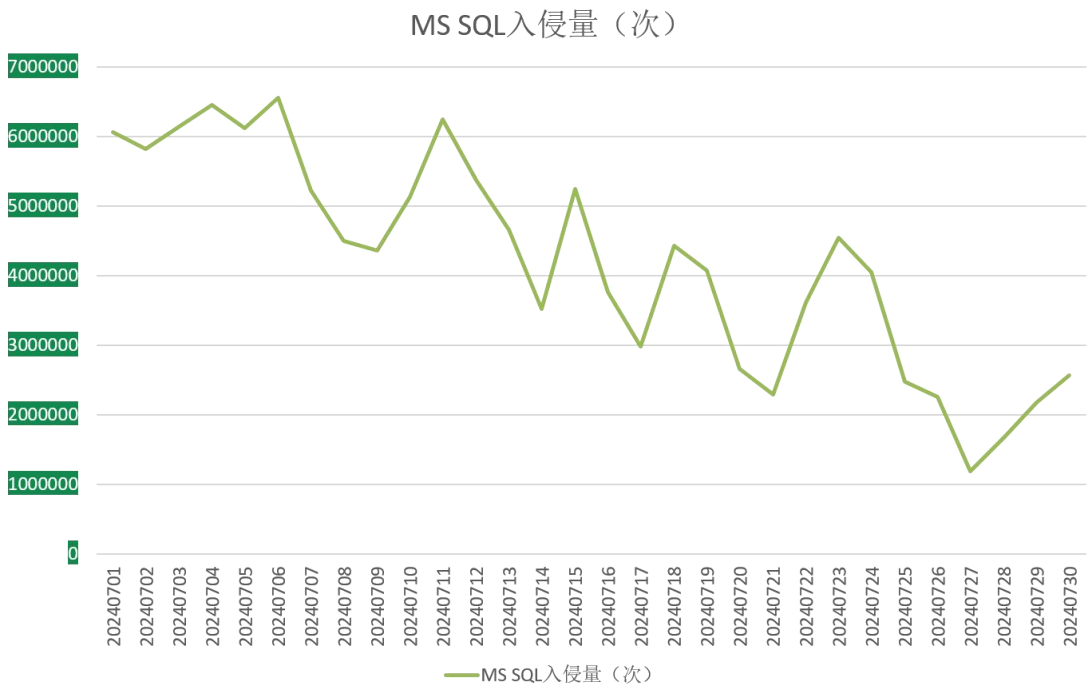

图 8. 2024 年 7 月监控到的 MS SQL 入侵量

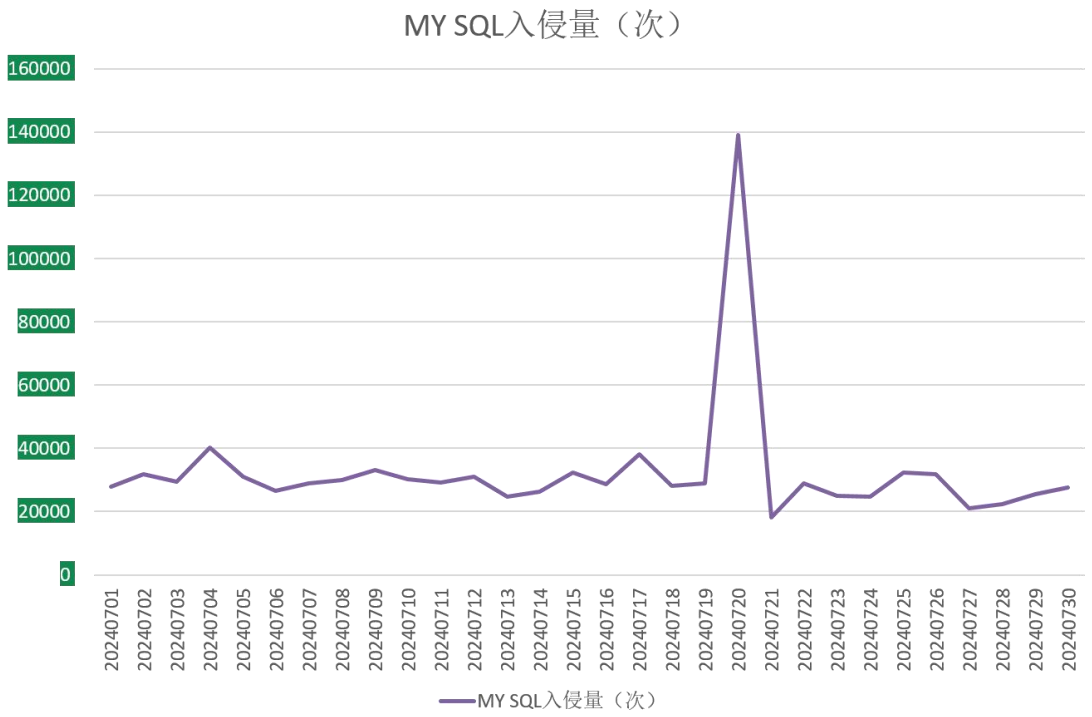

图 9. 2024 年 7 月监控到的 MYSQL 入侵量

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。

- 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。

- svh：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。

- src：同 svh。

- rmallox：同 hmallox。

- 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。

- jaff：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。

- mallox：同 hmallox。

- mkp：同 svh。

- faust： phobos 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。

- bixi：同 baxia。

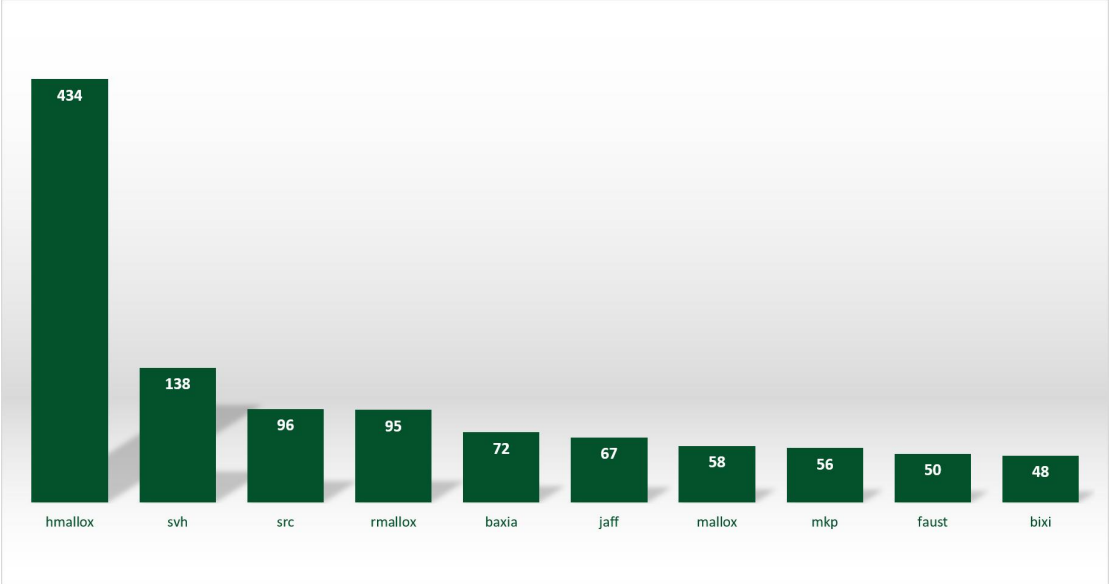

图 10. 2024 年 7 月反病毒搜索引擎关键词搜索排名

解密大师

从解密大师本月解密数据看，解密量最大的是 Loki 其次是 Telsa。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。

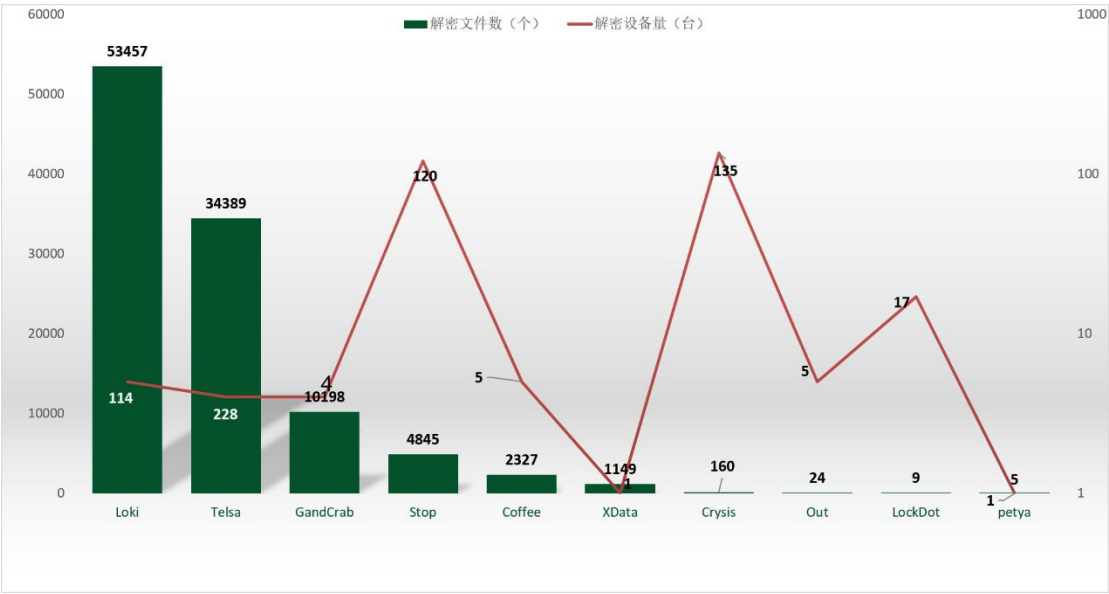

图 11. 2024 年 6 月解密大师解密文件数及设备数排名


360数字安全
数 字 安 全 的 领 导 者
360安全大脑