勒索软件流行态势分析

2024 年 8 月

360数字安全
数 字 安 全 的 领 导 者
360安全大脑

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 8 月，全球新增的传统勒索软件家族有 RNTC、BaiduLock 等。相关家族在国内主要通过远程桌面与数据库弱口令登录方式投毒。

以下是本月值得关注的部分热点：

1. 法国凡尔赛宫在奥运会期间遭遇网络攻击
2. Patelco 向 72.6 万名客户通报了勒索软件数据泄露事件
3. 江河集团短期内被两个勒索软件家族泄露数据

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：Makop 家族占比 18.05%居首位，第二的是 TargetCompany(Mallox)占比 16.59%的，phobos 家族以 15.61%位居第三。

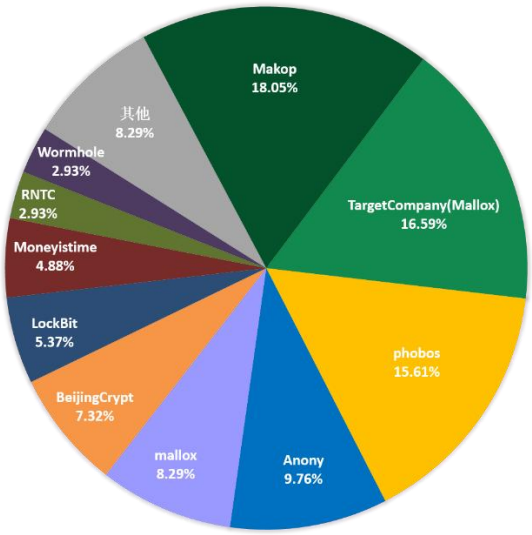

图 1. 2024 年 8 月勒索软件家族占比

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 2008。

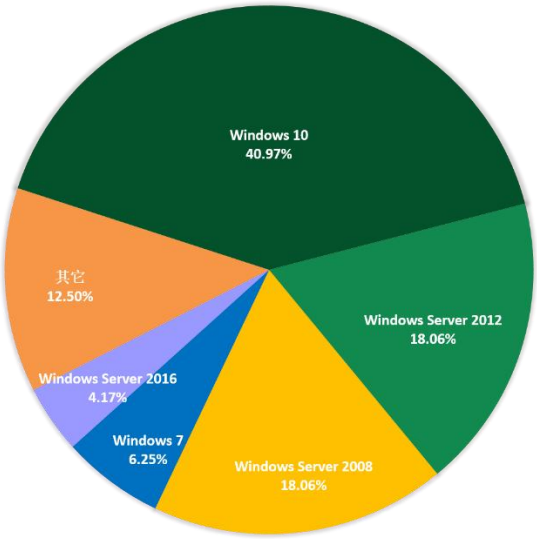

图 2. 2024 年 8 月勒索软件入侵操作系统占比

2024 年 8 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。

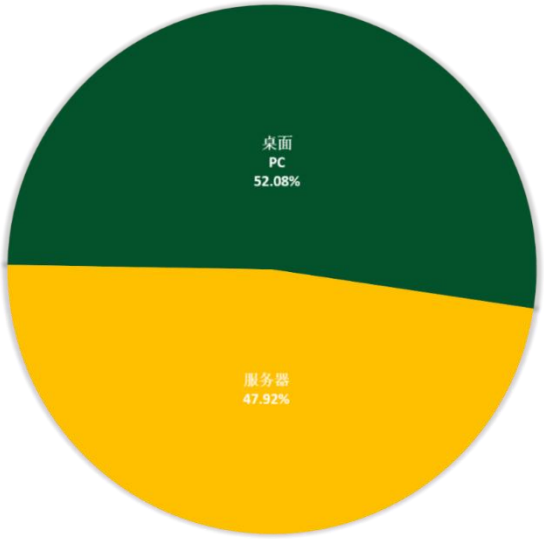

图 3. 2024 年 7 月勒索软件入侵操作系统类型占比

勒索软件热点事件

法国凡尔赛宫在奥运会期间遭遇网络攻击

法国的大皇宫国家博物馆联盟（RMN）于 2024 年 8 月 3 日晚间遭遇网络攻击。据《巴黎人报》内部消息来源透露，由于遭遇勒索软件攻击，大皇宫博物馆的运营受到了干扰。

然而，大皇宫博物馆馆长 Matthias Grolier 在社交媒体上否认了这一说法，称此次攻击并未影响到其他博物馆。而法国媒体《西南报》则报道称，此次袭击导致大皇宫博物馆关闭了其系统以防止攻击蔓延，这扰乱了法国众多博物馆的书店和精品店，只不过该情况目前已得到了暂时性的解决。

大皇宫博物馆联盟表示，此次网络攻击并未对其管理下的其他博物馆造成影响，这些博物馆仍继续正常运营。由大皇宫管理的 36 家博物馆商店目前同样也在正常运营。

据该博物馆表示，其已向法国网络安全特别行动组（ANSSI）、法国国家信息与自由委员会（CNIL）以及文化部通报了此次网络攻击事件。ANSSI 目前正在协助进行修复和网络恢复工作，初步调查尚未发现任何从被入侵系统中窃取数据的迹象。

然而，据称此次事件的攻击者留下了一封勒索信来索要赎金，并威胁称如果不支付赎金他们将公布在攻击中窃取的数据。不过，目前还没有任何勒索软件组织宣称对此次攻击负责，因此攻击者的身份尚不明确。

Patelco 向 72.6 万名客户通报了勒索软件数据泄露事件

Patelco 信用合作社警告客户称今年早些时候该信用合作社在遭受 RansomHub 勒索软件攻击时，客户的个人数据或已被盗，信用合作社因此遭受了数据泄露事件。虽然 Patelco 并没有透露袭击者的身份，但勒索团伙“RansomHub”于 2024 年 8 月 15 日宣称对此事负责，当时他们将所有被盗数据发布在他们的勒索门户网站上。

此前，该公司曾透露其于 2024 年 6 月 29 日遭遇勒索软件攻击，被迫关闭面向客户的银行系统以控制损失并保护客户的数据。该系统中断事件持续了大约两周时间。在此期间，该组织恢复了其 IT 系统大部分功能。

在事件曝光时，Patelco 公司尚未确定攻击中是否存在数据泄露情况。但在 2024 年 8 月 14 日，该组织经调查后最终确认了攻击者已窃取了客户数据。

被攻击者获取的个人信息因人而异，可能包括：

- 客户全名
- 社会安全号码（SSN）
- 驾驶执照号码
- 出生日期
- 电子邮件地址

以上信息也与暗网勒索平台“RansomHub”泄露的信息相符。该平台上的黑客声称在为期两周谈判之后，他们未能与 Patelco 达成协议。

根据缅因州检察长办公室网站上的一份名单显示，该事件影响了 72.6 万名 Patelco 客户。Patelco 公司也在其网站首页放置了一个警告横幅，提醒会员该公司团队绝不会直接联系他们要求提供卡号信息，包括 PIN 码、有效期或 CVV 码。而对于那些身份信息被泄露的人来说，遭受钓鱼攻击、社会工程攻击和诈骗的风险大大增加。因此他们现在被建议要对未经请求的通信和恶意企图保持警惕。

国内某建筑集团短期内被两个勒索软件家族泄露数据

国内一家集建筑幕墙系统、建筑装饰、医疗健康和投资等多元化业务于一体的全球化大型建筑企业集团在今年 8 月时，分别被两个勒索软件组织 Hunters International 与 RansomHouse 公开了入侵后窃取的数据。

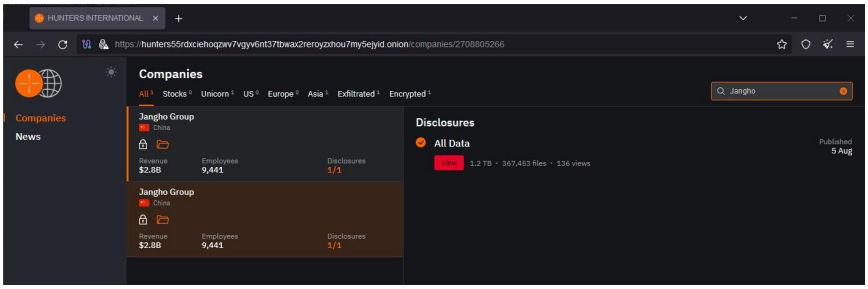

图 4. Hunters International 勒索组织宣称攻陷国内某建筑集团

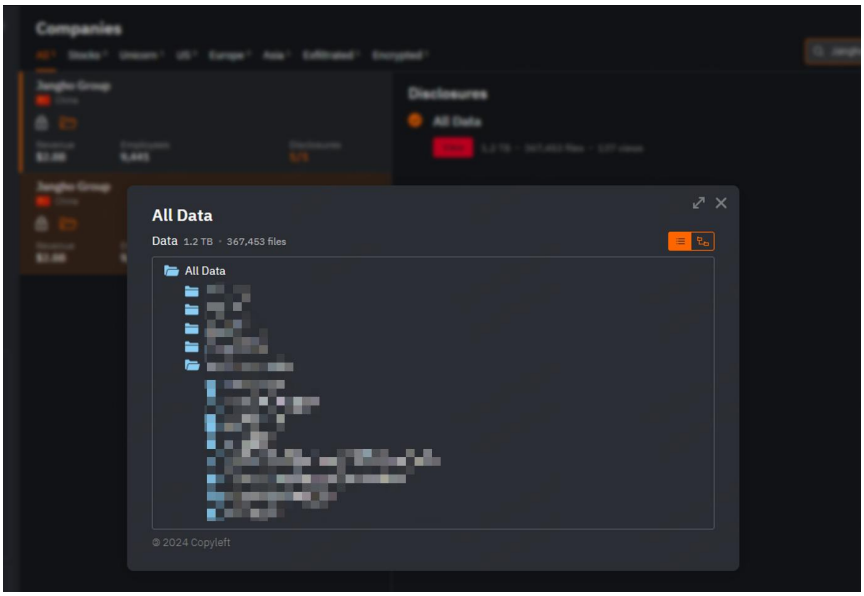

图 5. 据勒索团伙称窃取自该集团内部的数据列表

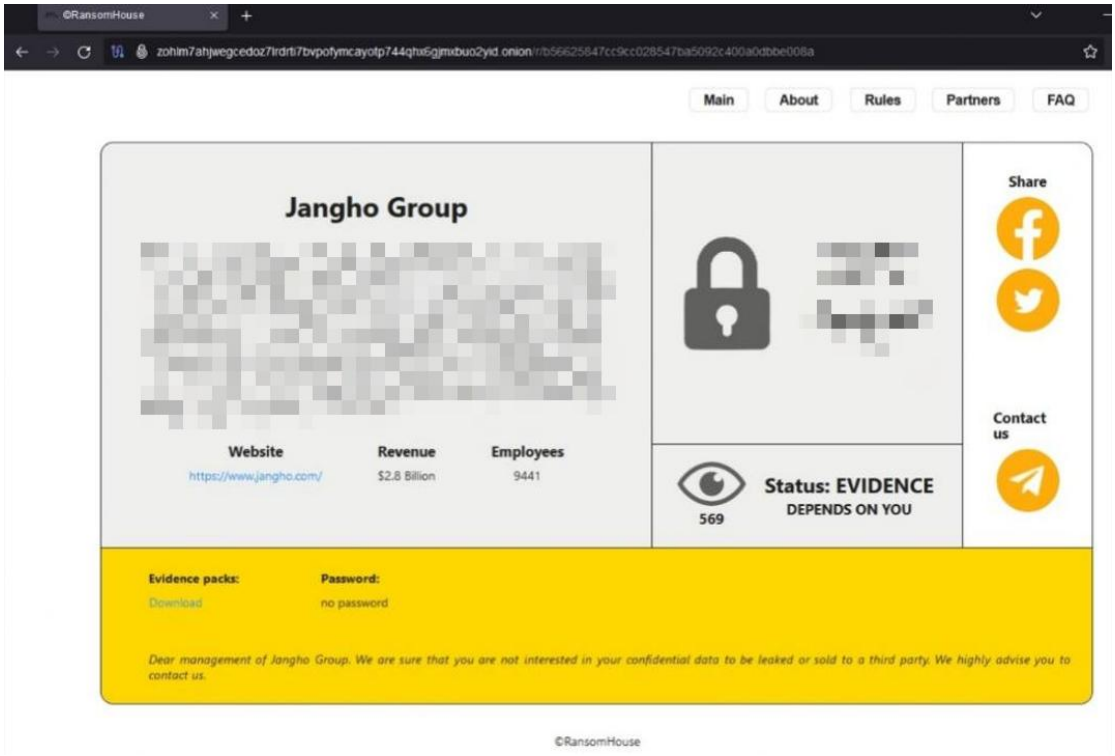

图 6. RansomHouse 勒索团伙信息泄露页面挂出国内某建筑集团

早在 7 月 20 日，360 安全大脑就监测到相关攻击团伙通过域控制器下发计划任务的方式，实施了在企业内部大规模部署勒索攻击的行为。

图 7. 360 安全大脑监控到攻击者利用域控部署勒索软件

我们也已第一时间通报了相关单位，对方目前尚未进对该事件进行回应。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

dolores@bpe.cash	wewillhelp@airmail.cc	somran@onionmail.com

faust.recovery@gmail.com	yourhope@airmail.cc	decryptcyberfear@onionmail.org
faust.restore@gmail.com	helpersmasters@airmail.cc	ChantellGrant@onionmail.org
default1@tutamail.com	crab7765@gmx.de	LorriBuckridge@onionmail.org
Default@firemail.de	bruuuuz@yahoo.com	pomocit03@kanzensei.top
re2c@tuta.com	anonimus.mr@yahoo.com	pomocit03@surakshaguardian.com
pomocit07@kanzensei.top	firmabilgileri@bk.ru	saidabujavi@firemail.cc
pomocit07@surakshaguardian.com	Filesreturn247@gmx.de	nomoredata@cock.li
givebackdata@mail.ru	mrbin775@gmx.de	baidulock@cyberfear.com
getmydata@inbox.ru	dan@cock.email	baidulock@tuta.io
example@airmail.cc	fastsupport@xmpp.jp	Hoeosi@airmail.cc
8base@tuta.io	fastrecovery@xmpp.jp	dataserver@airmail.cc
8base@mailfence.com	infovip@airmail.cc	BaseData@airmail.cc
8base@proton.me	Help-Mails@Ya.Ru	SuppBlackbit@gmail.com
amgdecode@proton.me	xmail@cock.li	SuppBlackBit@protonmail.com
amgdecode@onionmail.com	macc.edont@protonmail.com	ccfarmy@tutanota.com
decryptdata@qq.com	suupport@protonmail.com	ccfarmy@protonmail.com
Crypsys@mailfence.com	worcservice@protonmail.ch	kasperskyrans@gmail.com
griffin@cock.lu	cashdashsentme@protonmail.com	kasperskyrans@outlook.com
griffi777n@gmail.com	hupstore@keemail.me	vinsulan@tutamail.com
dark.encrypt@onionmail.org	revezar@zohomail.eu	decsupp24@mail2tor.com
emmo.encrypt@onionmail.org	plingplong@mail.com	decsupp24@cock.li
octanix@onionmail.org	backupdecoder@aol.com	iskaluz@protonmail.com
octanix@tutamail.com	decoderhelp@aol.com	lacklivesmatter@qq.com
Help557@cock.li	ownerde@cock.li	reservedecryption@protonmail.com
zoro4747@gmx.de	ownerde@cyberfear.com	decryption@qbmail.biz
mrpeterson@cock.li	Datablack0068@gmail.com	Dan@cock.email
crab2727@gmx.de	Datablack0068@cyberfear.com	criptote@hmamail.com
decrypt2019@gmx.de	besttrcovery@firemail.cc	referas@hmamail.com
Traher@Dr.Com	randbnothing@tutanota.com	terder@hmamail.com
crab1917@gmx.de	lambdasupp@airmail.cc	utera@hmamail.com
.aztecdecrypt@protonmail.com	filesupp911@gmail.com	marshaldec@aol.com
online24files@airmail.cc	prodecrypter@aol.com	derick_btc@tuta.io
stevenseagal@airmail.cc	prosupport@cyberfear.com	d3cryptme@firemail.cc
supportfiless24@protonmail.ch	vortexecho@zohomail.eu	

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）。

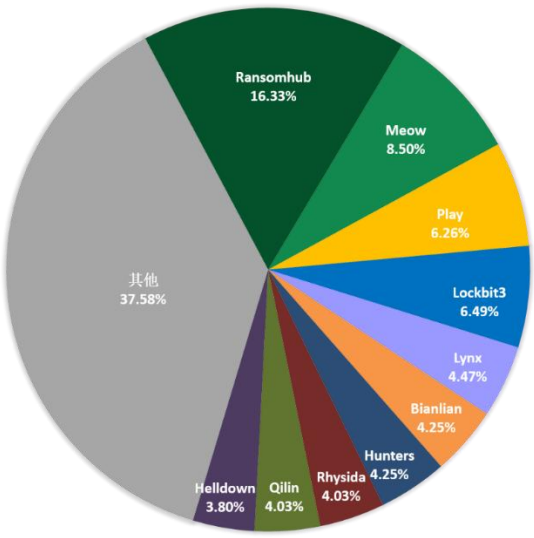

图 8. 2024 年 8 月通过数据泄露获利的勒索软件家族占比

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 446 个组织/企业遭遇勒索攻击，其中包含中国 3 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 7 个组织/企业未被标明，因此不在以下表格中。

White Mountain Backpacks	Bay Sales (cog.local)	Element Food Solutions
Southwest Traders	PBS group	Aerotech Solutions
Nevada Heart Vascular Center	Studio Legale Associato Isolabella	E-Z UP
Donco and Sons Inc.	HL Lawson & Sons	deganis.fr
Grupo Modesto Cerqueira	terralogs.com.br	The White Center Community Development Association
NOBI AS	Chama Gaucha	gpf.org.za
Instituto Cardiovascular del Cesar	idahopacific.com	lenmed.co.za
Special Oilfield Services Company LLC	Crimson Interactive	Banner and Associates
Caseificio Alta Valsesia	www.seaeng.com	Southwest Family Medicine Associates
MorningStar Senior Living	Saeilo	glazkov.co.il
Goodless Dermatology	schoolrush.com	XPERT Business Solutions GmbH
Effortless Office	Life University	MyFreightWorld
ciot.com	Sherwood Stainless & Aluminium	cbmm.org

www.nissan-dubai.com	Igloo Cellulose	AZIENDA TRASPORTI PUBBLICI S.P.A.
Bogdan & Frasco, LLP	Raifalsa-Alelor	briju.pl
BLVD Residential INC	Deane Roofing and Cladding	vindix.pl
John W. Brooker & Co., CPAs	instadriver.co	Albatros S.r.l.
Khoo and Company, Inc	www.cincinnatipainphysicians.com	NetOne
New River Electrical Corporation	Kronick Moskovitz Tiedemann & Girard	fabamaq.com
The Recycler Core Company	Don't Waste Group	cyceron.fr
Tranter (tcn.local)	UFCW Local 135	bedford.k12.oh.us
Sports & Spine Orthopaedics	EBA Ernest Bland Associates	Warwick Hotels and Resorts
Mitsubishi Chemical Group	level.game	nicholsfleet.com
grant-associates.uk.com	antaeustravel.com	VVS-Eksperten
Phyton Biotech	rylandpeters.com	Brookshire Dental
Burgess Kilpartik	saudi arabia(general secretariat of the military service council)	Alvan Blanch Development
Richmond Auto Mall	Engedi	naturalcuriosities.com
Seng Tsoi Architect	Larc	TelPro
Raeyco Lab Equipment Systems Management	Stjamesplace.org	Jeffersoncountyclerk.org
Welding and Fabrication (humblemfg)	policiaauxiliarcusaem.com.mx	brockington.leisc.sch.uk
City Projects	Policy Administration Solutions	Amco Metal Industrial Corporation
Prism Construction	beinlaw.co.il - Prof. Bein & Co.	alliuminteriors.co.nz
Cotala Cross-Media	MacEwen Petroleum	Moser Wealth Advisors
pfsbrands.com	Grid Subject Matter Experts	robertshvac.com
Eric Rossi CPA LLC	The SMS Group	dmmerch.com
www.timortelecom.tl	Quilvest Capital Partners	luisoliveras.com
www.mineduc.gob.gt	RCG	legacycpas.com
www.primariatm.ro	Armour Coatings	allweatheraa.com
www.suvacity.org	Dunlop Aircraft Tyres	soprema.com
www.iph-bet.fr	Vibo.dk	exol-lubricants.com
www.johnkellys.com	Hvb-ingenieure.de	fremontschools.net
www.fenceauthority.com	Westermans.com	acdcexpress.com
www.gruyeria.ch	Jinny Corporation	clinicatezza.com.pe
www.lfewines.com	BARRYAVEPLATING	divaris.com
Lane Supply Inc.	RSK-IMMOBILIEN	sullivansteelservice.com
Riverside Resort Hotel and Casino	capitalfund1.com	johnllowery.com
www.citebd.org	www.pindrophearing.co.uk	qespavements.com
www.ramoncorripio.com	spvmhc.org	emanic.net
www.iiitd.ac.in	www.banhampoultry.co.uk	Hanon Systems
www.swinburne.edu	kidkraft.com	lmgroup.com
Wayne Wright, LLP.	Luigi Convertini	kronospublic.com
ICWI	Findel	Brontoo Technology Solutions

Stein Fibers	HOERBIGER Holding	Cydcor
akanea.com	Burns Industrial Equipment	Credible Group
fanningfanning.com	Olympus Financial	Nilorngruppen AB
Navitas Semiconductor	globacap.com	arkworkplacerisk.co.uk
alconca.com.ve	Codival	Majestic Metals
tdsb.on.ca	jpoint.in	Anniversary Holding Company
sampoernaagro.com	inlighten.net	GCA Global Cargo Alliance
albanybank.com	blowerdempsay.com	Concut (ddm.local)
hphood.com	Rushlift (lks.net)	New TSI Holdings, NYSC
inces.com	North Georgia Brick	dhcgrp.com
Hollywood Burbank Airport	Akkanat Holding	Boombah Inc.
Risser Oil	Percento Technologies Internationa	www.dunnsolutions.com
glasstile.com	imobesidade.com.br	Sumter County Sheriff
Clatronic International GmbH	osg.com	pierrediamonds.com.au
Corbally Gartland and Rappleyea	Waynesboro Nurseries	golfoy.com
Stiller Aesthetics	The Transit Authority of Northern Kentucky (TANK)	tibaitservices.com
malonetoyota.com	Khonaysser	mihlfeld.com
Gortemoller Engineering (gorteng.local)	Certified Transmission	NIDEC CORPORATION
Appletec Ltd	Jangho Group	inv-dar.com
christen-sanitaer.ch	Bandier	icarasia.com
Bayou DeSiard Country Club - Monroe, LA	ccsdschools.com	rationalenterprise.com
rainierarms.com	Ferraro Group	modernceramics.com
Epi Breads	Mohawk Valley Cardiology PC	comoferta.com
Software Engineering Associates	kbo	mercadomineiro.com.br
GDB International	PBC Companies	Horizon View Medical Center
ABC Parts International	Yang Enterprises	www.jgsummit.com.ph
Universal Pure	Carver Companies	hudsoncivil.com.au
Omicron Granite & Tile	J&J Network Engineering	Bayhealth Hospital
Clabots	PER4MANCE	amplicon.com
rmn.fr	SMK Ingenieurbüro	infotexim.pe
tjs.com	Cosmetic Dental Group	suandco.com
ghanare.com	TELECO	Miller Boskus Lack Architects (ad.mbl-arch.com)
medisetter.com	peoplewell.com	kempe.com.au
agra-services.be	aerworldwide.com	Anderson Oil & Gas
Atwood & Cherny, P.C.	awsag.com	bonatra.com
Fish Nelson & Holden	www.netconfig.co.za	HUD User
M.Royo & KlockMetal	www.albynhousing.org.uk	KLA
JM Thompson	www.lennartsfors.com	FatBoy Cellular
Scott Pharma Solutions	www.allanmcneill.co.nz	Johnson Laschober & Associates

freshairefranchise.com	www.martinswood.herts.sch.uk	Cambria Automobiles (summitgroup.local)
Diamcad	www.gmchc.org	Pyle Group
comtruck.ca	www.regentcaravans.com.au	Reef-PCG (pcg.local)
mykukun.com	tiendasmacuto.com	Granit Design
www.polycohealthline.com	www.manotherm.ie	www.sobha.com
Y. Shilat Management Services Ltd	nrcollecties.nl	Alternate Energy
Success Microfinance Bank	Zyxel.eu	True Blue Environmental
dpfza.gov.dj	www.wmwmeyer.com	KinetX
Rinehart Butler Hodge Moss & Bryant	www.vinakom.com	biw-burger.de
www.chwa.com.tw	Keios Development Consulting	Omni Family Health
KidKraft	Lennartsfors AB	Casco Antiguo
codacinc.org	Rostance Edwards	IOI Corporation Berhad
Woden	SuperDrob S.A.	Ziba Design
WT Gruber Steuerberatung GmbH	www.patelco.org	Fractalia Group
Finlogic S.p.A	Hiesmayr Haustechnik	Banx Systems
Academy of Model Aeronautics	promises2kids.org	exco-solutions.com
Barkal Food Industries	Prefeitura do Jaboatão dos Guararapes	Silipos
Modulkit	on365.co.uk	kierlcpa.com
Artesanía Chopo	ccj.edu.lb	Square One Coating Systems
Mason City Recycling Center	BTS Biogas	Hi-P International
Crowe	ljglaw.com	HP Distribution
securityinstrument.com	www.aaconsultinc.com	Maryville Academy
Precom	Sterling Rope	notariusze.waw.pl
Microchip Technology	www.isnart.it	Ranney School
Vans Lumber and Custom Builders	www.atwoodcherny.com	nursing.com
Optimize EGS	Mill Creek Lumber	Bettis Asphalt
Complete Payroll Solutions	FD S.R.L	fcl.crs
South American Tours	Seaway Manufacturing Corp.	LRN
All Parks Insurance	Zydus Pharmaceuticals	aikenhousing.org
www.alabamaplate.com	The Pyle Group	David E Shambach Architect
www.smarterp.com	EPS Tech Ltd	Hayes Beer Distributing
htsusa.com	Patterson Health Center	Khandelwal Laboratories Pvt
www.spie-tec.de	Liberty Resources	CPA Tax Solutions
Brookshire Dental - Hospitals & Clinics	MBS Radio	www.bahia-principe.com
pocketrisk.com	Innoquest	www.normandydiesel.fr
widex.com	megatravel.com.mx	retaildatallc.com
Blue Maven Group	startaxi.com	Keystone Engineering
US Marshals Service	Boni	Kemlon Products & Development Co Inc
NewsBank	The Washington Times	q-cells.de
onedayonly.co.za	Texas Centers for Infectious Disease	Veren Inc and Crescent Point

	Associates	Energy
Affordable Tools	Benson Kearley IFG - Insurance Brokers & Financial Advisors	coinbv.nl
autonomous.ai	Thompson Davis & Co	Valley Bulk
prasarana.com.my	police.praca.gov.pl	ENEA Italy
dt-technologies	mmtransport.com	dahlvalve.com
Penn Veterinary Supply INC	Riley Pope & Laney	mcdowallaffleck.com.au
Meli (BCYF & Bethany)	hugwi.ch	effinghamschools.com
The University and College Union	Air International Thermal Systems	warrendale-wagyu.co.uk
nwcsb.com	Forrec	Adorna & Guzman Dentistry
Myelec Electrical	Adina Design	Camp Susque
www.curvc.com	Parker Development Company	Ali Gohar
Eagle Safety Eyewear	CinemaTech	acsi.org
Health Quality Council	Erie Meats	premier equities
Hofmann Malerei AG	Safefood	remitano
ingotbrokers.com	Gaston Fence	Peñoles
HBGJEWISHCOMMUN	SCHLATTNER.de	American Contract Systems
Wallace Construction Specialties (wcs.local))		

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。

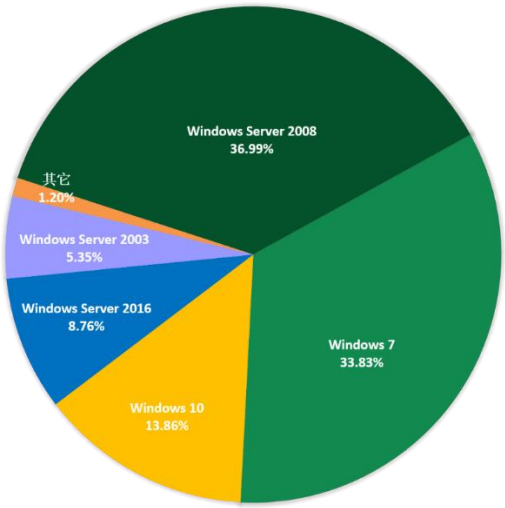

图 9. 2024 年 8 月受攻击系统占比

对 2024 年 8 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。

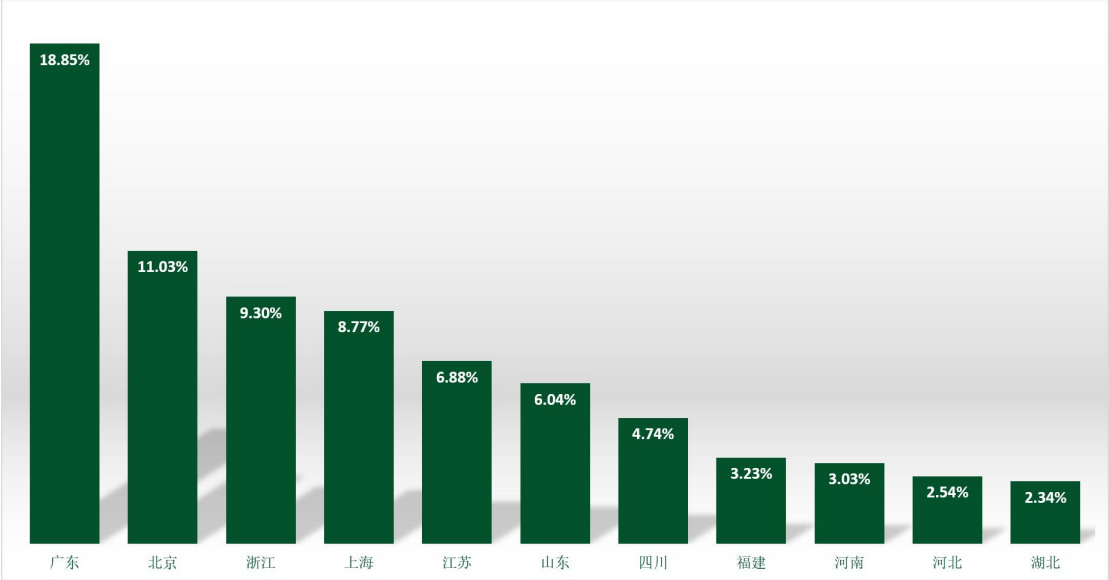

图 10. 2024 年 8 月国内受攻击地区占比排名

通过观察 2024 年 8 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。

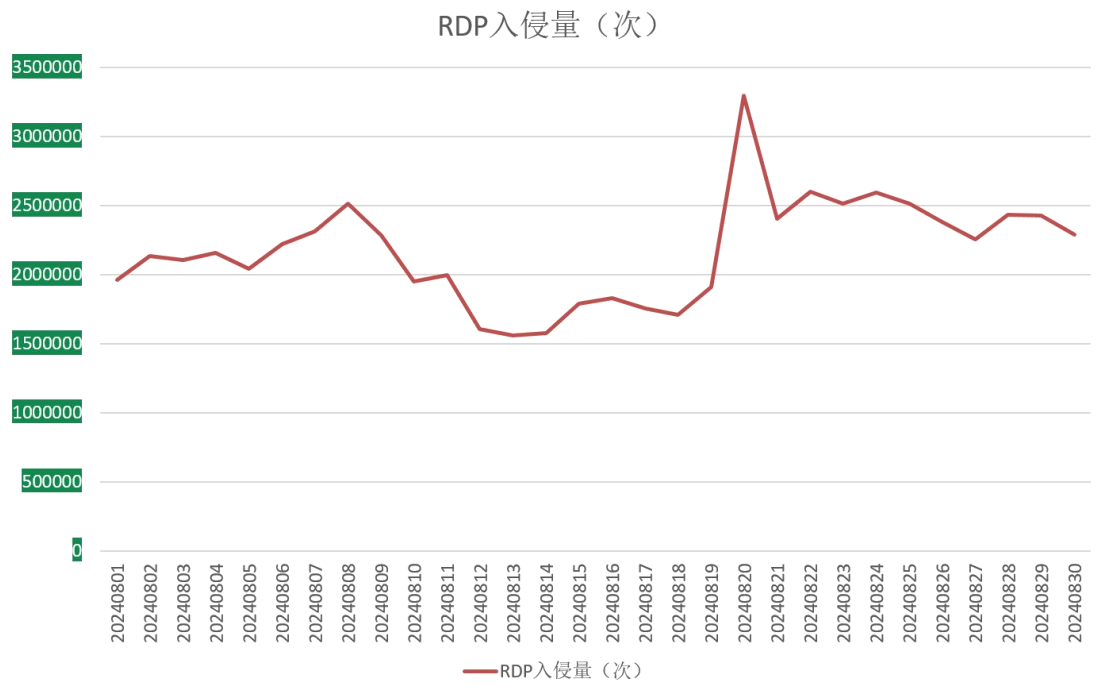

图 11. 2024 年 8 月监控到的 RDP 入侵量

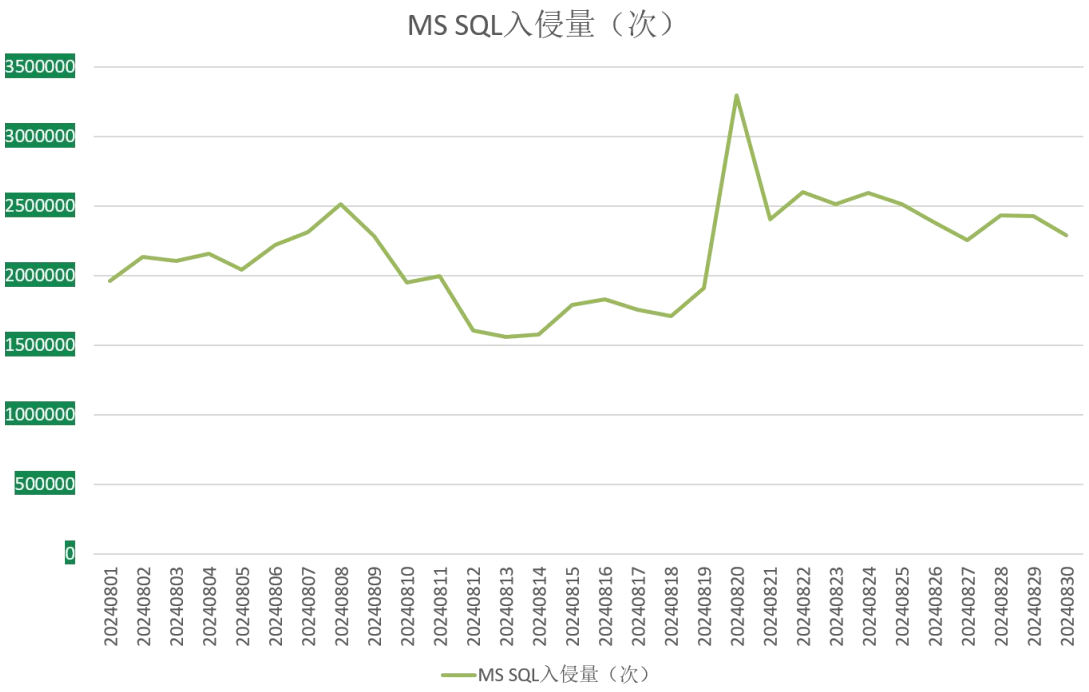

图 12. 2024 年 8 月监控到的 MS SQL 入侵量

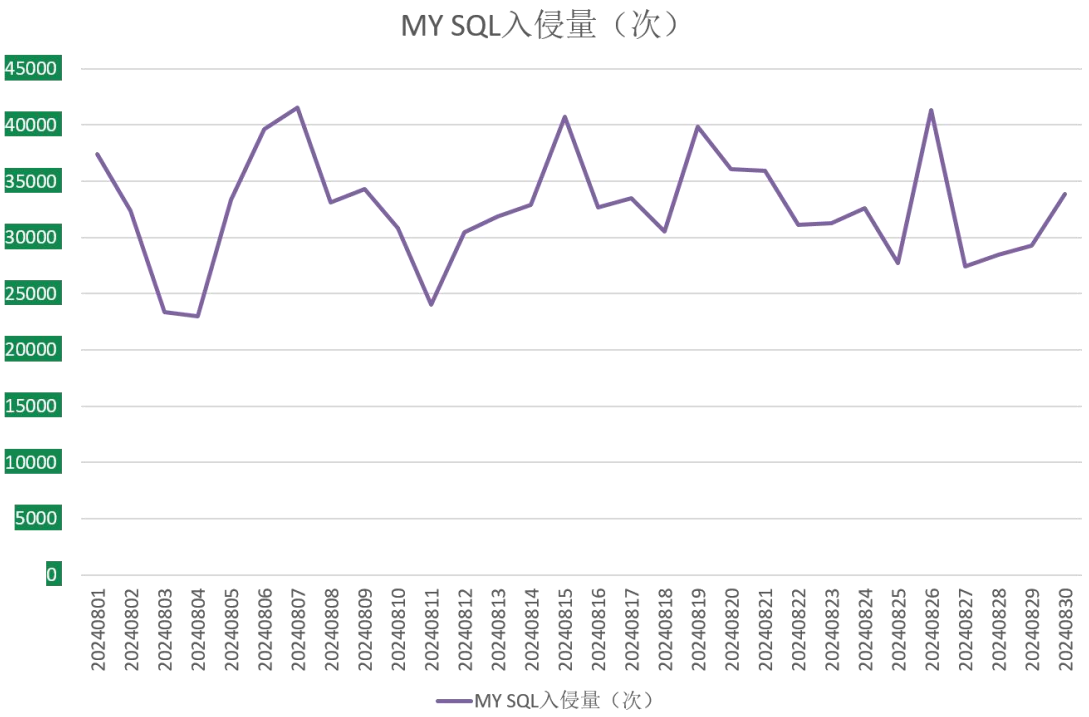

图 13. 2024 年 8 月监控到的 MYSQL 入侵量

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。
- hmallox：同 rmallox。
- 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。
- 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。
- svh：同 src。
- bixi：同 baxia。
- mallox：同 rmallox。
- 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。
- 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。
- Moneyistime： 属于 Moneyistime 勒索软件家族，由于被加密文件后缀会被修改为 Moneyistime 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。

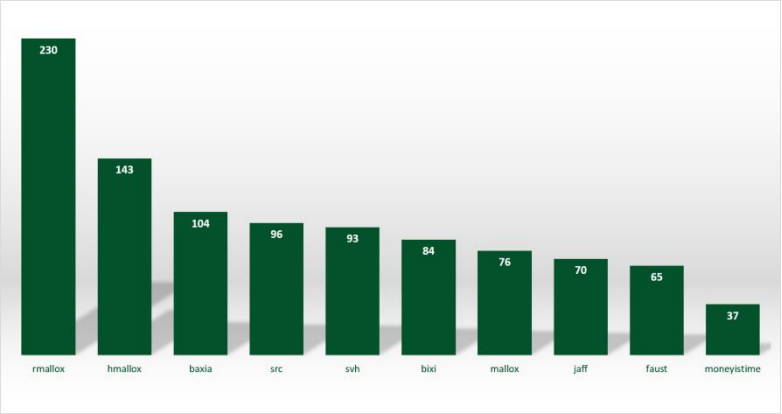

图 14. 2024 年 8 月反病毒搜索引擎关键词搜索排名

解密大师

从解密大师本月解密数据看，解密量最大的是 Lime 其次是 Loki。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。

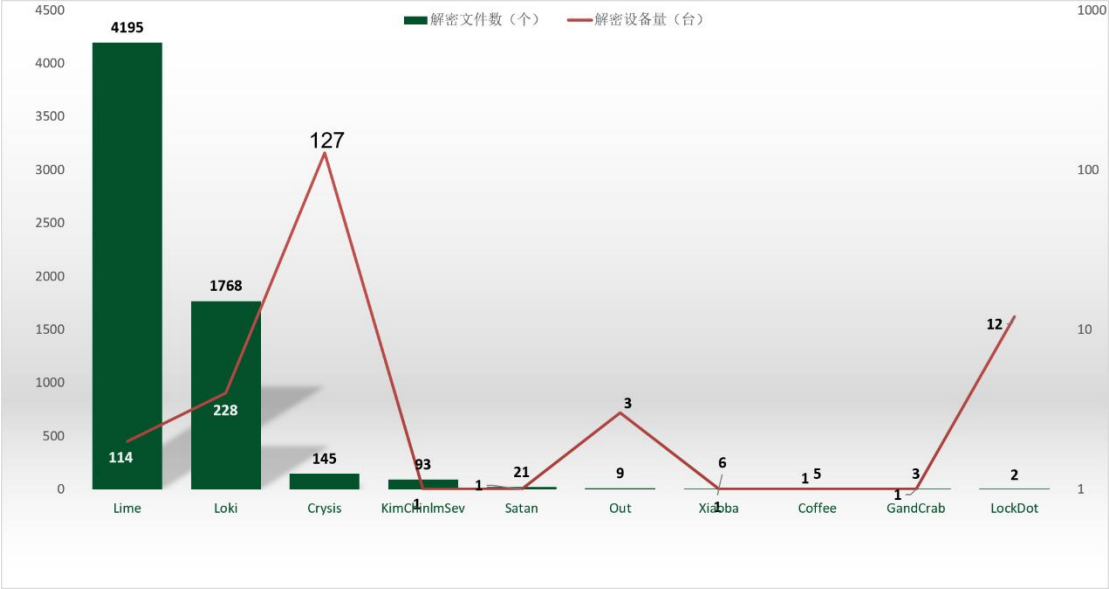

图 15. 2024 年 8 月解密大师解密文件数及设备数排名


360数字安全
数 字 安 全 的 领 导 者
360安全大脑