勒索软件流行态势分析

2023 年 7 月

360数字安全

数 字 安 全 的 领 导 者

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。

2023 年 7 月，全球新增的活跃勒索软件家族有 RA GROUP、Cactus、Rancoz 等家族。其中 RA GROUP 是本月开始活跃的双重勒索软件，该勒索软件团伙最初出现于 2023 年 4 月。当时他们在暗网上推出了一个数据泄露网站，发布受害者的详细信息和被盗数据，采用了流行的“双重勒索”策略。勒索页面于 2023 年 4 月 22 日上线，4 月 27 日发布了第一批受害组织，包括样本文件、被盗内容类型的描述以及被盗数据的链接。

以下是本月值的关注的部分热点：

1. 雅诗兰黛集团遭到两个勒索软件团伙的攻击

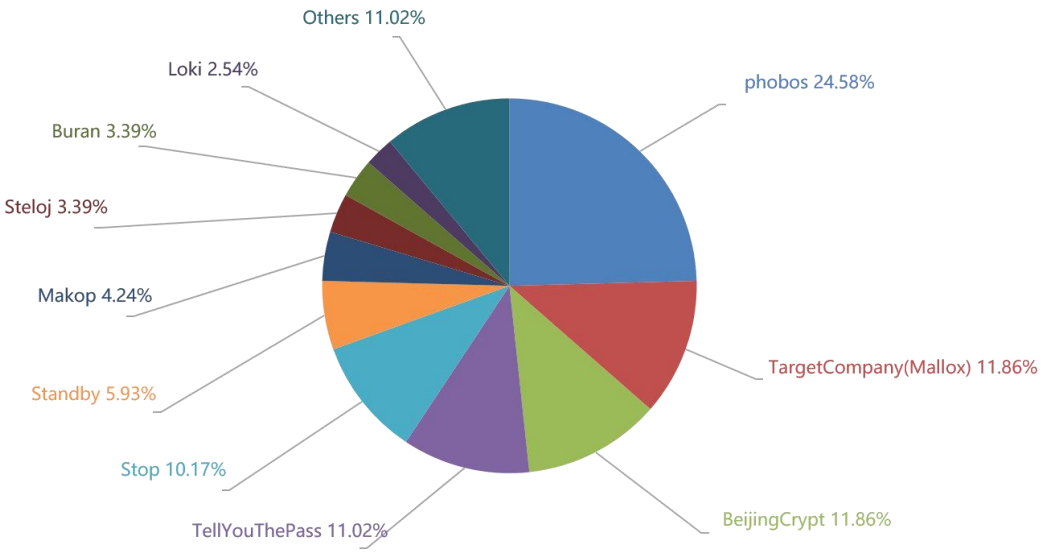
2. Clop 团伙利用 MOVEit 漏洞发动的勒索攻击已赚取超过 7500 万美元

3. ALPHV 勒索软件在其数据泄露网站中加入了获取泄露数据的 API

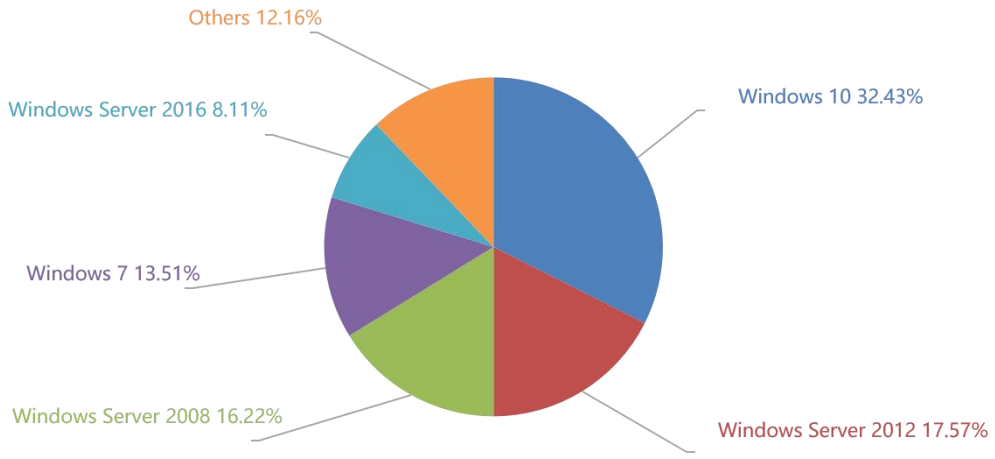
基于对 360 反勒索服务数据的分析研判，360 数字安全集团高级威胁研究分析中心(CCTGA 勒索软件防范应对工作组成员）发布本报告。

感染数据分析

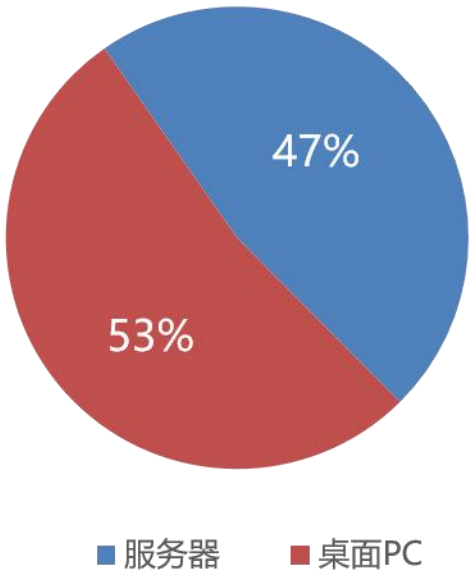
针对本月勒索软件受害者设备所中病毒家族进行统计：Phobos 家族占比 24.58%居首位，并列第二的是占比同为 11.86%的 TargetCompany(Mallox)与 BeijingCrypt 勒索病毒家族。



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。



2023 年 7 月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型占比基本相当。



勒索软件热点事件

雅诗兰黛集团遭到两个勒索软件团伙的攻击

两款勒索软件 ALPHV/BlackCat 和 Clop 均在其数据泄露网站上将美妆巨头雅诗兰黛列为攻击目标。而在发给公司的勒索信息中，BlackCat 团伙嘲笑了雅诗兰黛的安全措施并称它们的勒索工具仍存在于公司内部的网络上。

雅诗兰黛公司在 7 月 18 日提交给美国证券交易委员会(SEC)的文件中证实了其中一次攻击，称攻击者获得了其部分系统的访问权限并可能窃取了数据。但雅诗兰黛并没有提供有关该事件的太多细节，称公司已采取了积极行动并关闭了一些系统以防止攻击者在网络上的进一步扩张。

而 Clop 勒索软件团伙则似乎是利用了 MOVEit Transfer 平台的漏洞，获取了对该公司的访问权限。在 Clop 的数据泄露网站上，勒索团伙列出了雅诗兰黛并附上了简单的信息：“该公司不关心其客户，它忽视了他们的安全！！！”同时注明团伙目前已拥有超过 131GB 的该公司数据。BlackCat 方面暗示，目前获取到的信息可能会影响客户、公司员工和供应商。

雅诗兰黛对 BlackCat 的威胁没有做出回应，这可能表示该公司不愿与攻击者进行任何谈判。而在其向 SEC 提交的文件中也表示，重点是“补救措施，包括恢复受影响的系统和服务的努力”，并且“该事件已经导致并且预计将继续对公司的部分业务运营造成干扰”。

Clop 团伙利用 MOVEit 漏洞发动的勒索攻击已赚取超过 7500 万美元

Clop 勒索软件团伙正在效仿 ALPHV 勒索软件团伙的勒索策略——创建专门针对特定受害者的信息披露网站，从而更方便地泄露数据并进一步迫使受害者支付赎金。当此类勒索软件团伙攻击企业目标时，他们首先会从受害者的网络中窃取数据，之后再加密文件。这些被盗的数据会被用作双重勒索攻击的筹码——威胁受害者如果不支付赎金便会泄露其重要的机密数据。

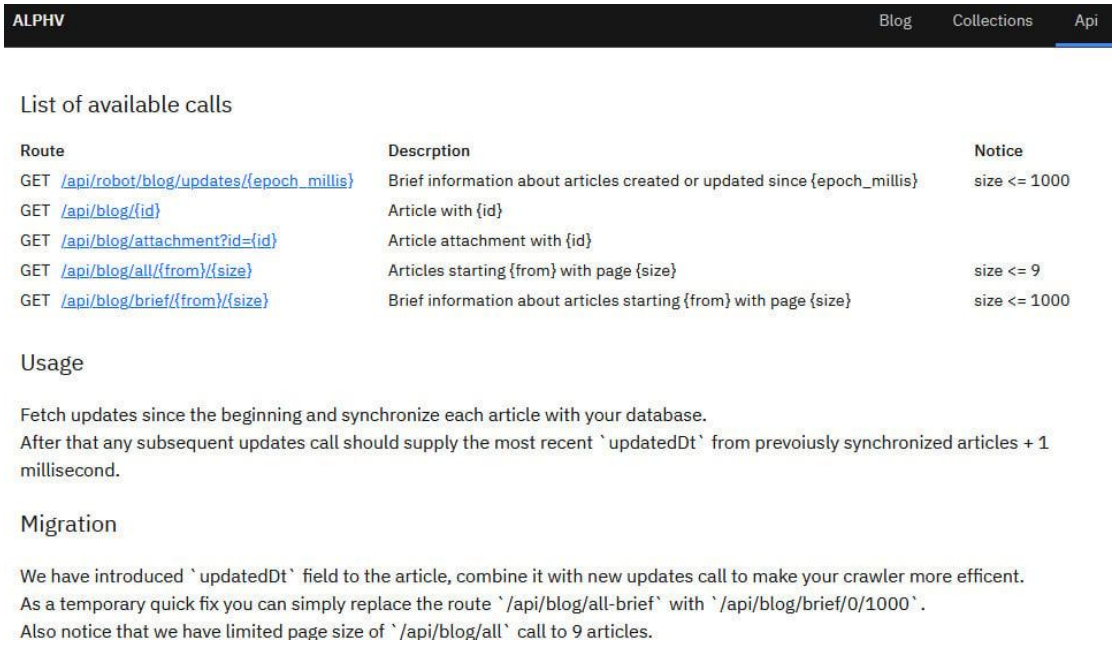
勒索软件用于发布数据的站点通常位于 Tor 网络上，因为这可以让网站更难被关闭或被执法部门查获。然而，这种托管网站的方法对于勒索软件团伙来说也有其自身的问题。因为需要专门的 Tor 浏览器才能访问此类网站，搜索引擎也不会收录此类数据，而且下载速度通常非常慢。为了克服这些问题，ALPHV 勒索软件团伙在去年引入了一种新的勒索策略，即创建 ClearWeb（透明网站）来泄露窃取到的数据。Clearweb 网站直接托管在公开的普通互联网上，而非 Tor 等匿名网络中。

而在本月中旬，安全人员发现 Clop 勒索软件团伙也开始创建自己的 ClearWeb 用来公布他们本轮通过 MOVEit Transfer 漏洞攻击所盗窃到的数据。攻击者创建的第一个网站是为商业咨询公司普华永道（PWC）创建的，并将该公司的被盗数据打包成了 4 个 Zip 压缩包发布在了该网站上。而这之后不久，攻击者还为 Aon、EY（安永）、Kirkland 和 TD Ameritrade 等公司创建了网站。

ALPHV 勒索软件在其数据泄露网站中加入了获取泄露数据的 API

ALPHV 勒索软件团伙（又名 BlackCat）正尝试通过为其数据泄漏网站提供 API 来提高公众对其公布数据的访问便利性，从而向受害者施加更大压力来迫使其支付赎金。在此之前，该团伙对雅诗兰黛发起了攻击，但就目前的公开信息来看，这家美容公司完全无视了攻击者的赎金要求。

7 月下旬，多名安全研究人员发现 ALPHV/BlackCat 的数据泄露网站添加了一个新页面——其中包含其最新公布的 API 及使用说明。API（应用程序编程接口）通常用于根据商定的定义和协议实现两个软件组件之间的通信。而本次勒索软件团伙发布的 API 将有助于公众通过程序自动其网站发布的关于最新受害者的各种信息。此外，该团伙还提供了一份用 Python 编写的爬虫代码以帮助检索数据泄露网站的最新信息。尽管该团伙没有解释为何要发布这些 API，但据推测原因之一可能是由于愿意支付勒索赎金的受害者越来越少。



黑客信息披露

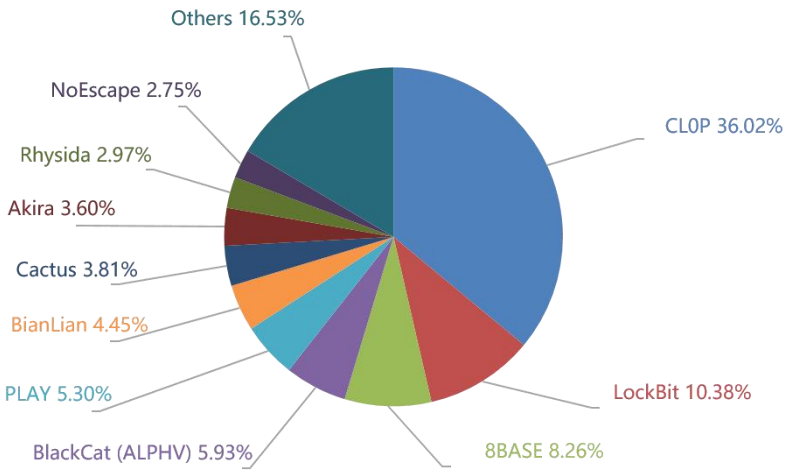
以下是本月收集到的黑客邮箱信息：

walterwhite@onionmail.org	kallit3rmux@gmail.com	lixcalisto@onionmail.org
casual2@test.com	dr.resetfile@gmail.com	calixcalisto@tutanota.com
777backup@tutanota.com	unknownsupport@mailfence.com	zitenmax@rambler.ua
ithelp10@securitymy.name	Unknownsup@tutanota.com	crypter1help@cyberfear.com
ithelp10@yousheltered.com	xxback@keemail.me	Ardimontechnologies@gmail.com
ithelp01@yousheltered.com	darkusmbackup@protonmail.com	rdphelp@tutanota.com
consert1777@tuta.io	deritim@proton.me	rdphelp@cock.li
myers@airmail.cc	nury_espitia@tuta.io	brenda_matthews_1976@protonmail.com
andrez.vegaz@zohomail.com	black_pirates@zohomail.com	josh.carinoso83@protonmail.com
rsamanager@tuta.io	x8154207@gmail.com	sudorocky@tutanota.com
bkpsvr@email.tg	decdata@tutanota.com	sudorocky@protonmail.com
vulcanteam@cock.li	decdata@msgsafe.io	sirattacker@mailfence.com
vulcanteam@airmail.cc	bob1997marley@onionmail.org	sirattacker@proton.me
stelој@mailfence.com	helper@cyberfear.com	ergsdhu@tutanota.com
stelој@rbx.run	franklin1328@gmx.com	dodocryptomail@proton.me
quvn5llxkk@mailfence.com	protec5@tutanota.com	tadora982928@mail.com
JnSeYvZw34@onionmail.org	camry2020@aol.com	informant3345@protonmail.com
Q6uBdWWuu4@proton.me	b_@mail2tor.com	security_ss123@tutanota.com
Hw2k0SZdxa@msgsafe.io	b_@mail2tor.com	securityss@cock.li
2020host2021@tutanota.com	geerban@email.tg	cheese47@cock.li
master1restore@cock.li	doctor.encrypted@onionmail.org	cheese47@tutanota.com
candice.wood@post.cz	tools.encrypted@onionmail.org	Black.Berserk@onionmail.org

candice.wood@swisscows.email	qweasd@toke.com	Black.Berserk@skiff.com
jerd@420blaze.it	qweasdzxc@toke.com	unidbenmykn@gmx.com
jred@keemail.me	stopproblema@proton.me	tianihokeem66@gmx.com
ronrivest@airmail.cc	stopproblema@tutamail.com	backmydata@bk.ru
rajah@airmail.cc	ryuksupport@yahooweb.co	backmydata@outlookpro.net
DevicData@tutanota.com	dectokyo@onionmail.org	patchworkapt@msgden.net
dopingen@rambler.ru	PatchWorkApt@tutanota.com	dopingen@rambler.ua

表格 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）。



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 471 个组织/企业遭遇勒索攻击，其中包含中国 2 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，因此不再以下表格中。

Great Opportunity to monetize your corporate access	nbcc.org	obrelli.it
paretophone.com	Announcement: Batesville Tool & Die, Inc will be leaked in 3 Days	www.garac.com
fushimitsu.com	hydrex.co.uk	txmplant.co.uk
westoaksschool.co.uk	llombart.de	TELNET Redes Inteligentes S.A.
Retail Information Systems	Ace Micromatic Group	St Landry Parish School Board
All States Ag Parts	twv-staderland.de	Alinabal

One Health Solutions	Village Church of Barrington	Modern Eyez
AT&S	Muncy Homes	Ashley HomeStore
Axity	ESMOD	Frost & Sullivan
Chu De Rennes	CMC Marine	Dekko Window Systems
Regional Family Medicine	Rouzbeh Educational Complex	McAlester Regional Health Center
INSULCANA CONTRACTING LTD	Handi Quilter	Morehead State University (MSU)
Offutt Nord	MACOM.COM	KALEPW.COM
DATAENGINE.EU	SAUL.ORG.UK	CCED.COM.OM
VIRGINPULSE.COM	ACLARA.COM	QUARK.COM
INFINIGATE.CH (INFINIGATE.CO.UK)	INFORMATICA.COM	ALOHACARE.ORG
SOFTTECH.NL	ALOGENT.COM	CONVERGEONE.COM
AMERISAVE.COM	KELLYSERVICES.COM	HUBBELL.COM
ALEKTUM.COM	HOERMANN-GRUPPE.COM	SALELYTICS.COM
FLUTTER.COM	ENTERPRISEBANKING.COM	MECHANICSBANK.COM
TRICOPRODUCTS.COM	JONESLANGLASALLE.COM	ARISTOCRAT.COM
ADARESEC.COM	TTIGROUP.COM	CHUCKECHEESE.COM
DELOITTE.COM	SIU.EDU	WSP.COM
SAFILOGROUP.COM	SLEEPCOUNTRY.CA	PLANETHOMELENDING.COM
TOYOTA-BOSHOKU.BE	DDCOS.COM	THEVITALITYGROUP.COM
METROBANK.COM.PH	GENESISENERGY.COM	GNC.COM
INFORMA.COM	EMSBILLING.COM	AWAZE.COM
PAYBACK.GROUP	scmh.org.tw	CF Assicurazioni
www.beijer.es	www.ville-chevilly-larue.fr	www.addison-electronique.com
Globacom Limited	Lumberton Independent School District	Kovair Software
GARRETTMOTION.COM	SMURFITKAPPA.COM	MCW.EDU
GOALSOLUTIONS.COM	GENSLER.COM	HINDUJAGROUP.COM
FANUCAMERICA.COM	CHEVRONFCU.ORG	FERRING.COM
SBMOFFSHORE.COM	CAP.ORG	QBITS.CH
MESVISION.COM	PBINFO.COM	HALLMARKCHANNEL.COM
MAXIMUS.COM	ARROW.COM	AJOOMAL.COM
DRYDOCKS.GOV.AE	HILLROM.COM	PRO2COL.COM
ENCOREANYWHERE.COM	AMF.SE	ORAU.ORG
AGILYSYSAP.COM	Decimal Point Analytics Pvt	Spectra Industrial
Miranda Brokerage	Institut Mensalus S.L.	Kersey & Co
FANSIPAN CONSTRUCTION CONSULTANTS CO.,LTD	DV8 Technology Group	CROWD
BoomData	EDVMS	rampi.com
Becht Engineering	The Sinbad Club	ridgeviewindustries.com
NEBRASKALAND	Republic Steel	IT Luggage
John Mulder Heating & Air Conditioning	Scharco Elektronik	Primoteq
Grupo MH	FERRE BARNIEDO	BionPharma

El Milagro	SBM	DYNAMITE
Charles & Colvard Ltd.	IRIS Informatique	ebpsupply.com
ICT-College	EJM Engineered Systems	Bluelinea
The Big Life group	Stephen F. Austin State University	Exbon Development, Inc
THE COLLINS LAW FIRM	Jackson Township Administration	Jackson Township Police Department
championgse.com	Pechexport	Cvlan
Sun Pain Management	Cafe Britt	Samson Electric
Chan and Associates	Siden & Associates	Hungarian Investment Promotion Agency
Bartlett	Caterham High School	Azimut.it
CORDELL	Hirsch Bedner Associates	Yamaha Canada Music Ltd
Alberto Couto Alves	Agoravita	American Meteorological Society
Biocair International	Confartigianato Federimpresa FC	ScanSource
CWS	Hawa Sliding Solutions	Imagination
Italkraft	Michigan Production Machining	Novobit
Artemide	Reyes Automotive Group	Rotomail Italia SpA
Phoenix Taxis	Wasserstrom	Americold
Bright Future Electric, LLC	www.coriniumcarpets.co.uk	Campbell Killin Brittan & Ray LLC
Entegra	cityserve-mech.co.uk	Hightway Care
Magnolia Steel	New Braunfels Cardiology	Kensington Publishing
Fernmoor Homes	ECS Technology Group	Anesco Ltd
Woodbine Hospitality	Sea Force IX	Centennial Management
Braintree Public Schools	Blount Fine Foods	Collins Aerospace (An RTX Business)
obeidpartners.com	DMA.US	VENTIVTECH.COM
BLUEFIN.COM	ESTEELAUDER.COM	OFCOM.ORG.UK
ALLEGIANTAIR.COM	ITT.COM	SMC3.COM
COMREG.IE	JONASFITNESS.COM	AA.COM
EA SMITH	VOG	The Estée Lauder Companies
DTD Express	KUITS	Tampa general hospital
www.acomen.fr	www.girardini.it	Health Springs Medical Center
Nini Collection Ltd (Nini's Jewels)	cotrelec.com	berg-life.com
lfcaire.org	suninsurance.com.fj	ope.com.na
dixiesfed.com	flexity.com	academia21.com
CashCall, Inc.	Lenders Choice Escrow	SettleIt, Inc.
The Loan Exchange	Ocean Breeze Ranch	Servicing Solutions
RCI.COM	SIERRAWIRELESS.COM	COMPUCOM.COM
CFINS.COM	DESMI.COM	FMGL.COM.AU
VALMET.COM	VITESCO-TECHNOLOGIES.COM	TJX.COM
Seasia Infotech	Ningbo Joyson Electronic Corp.	Wasserstrom
Senior Sistemas	Cavanaugh, Biggs & Lemon P.A., Attorneys at Law	hopetech.com
johnreilly.co.uk	Citta Nuova	Venture Drilling Supply
THENOTABLEFRONTIER.COM	GRACE.COM	PRGX.COM
HESS.COM	MYCWT.COM	SCHNABEL-ENG.COM

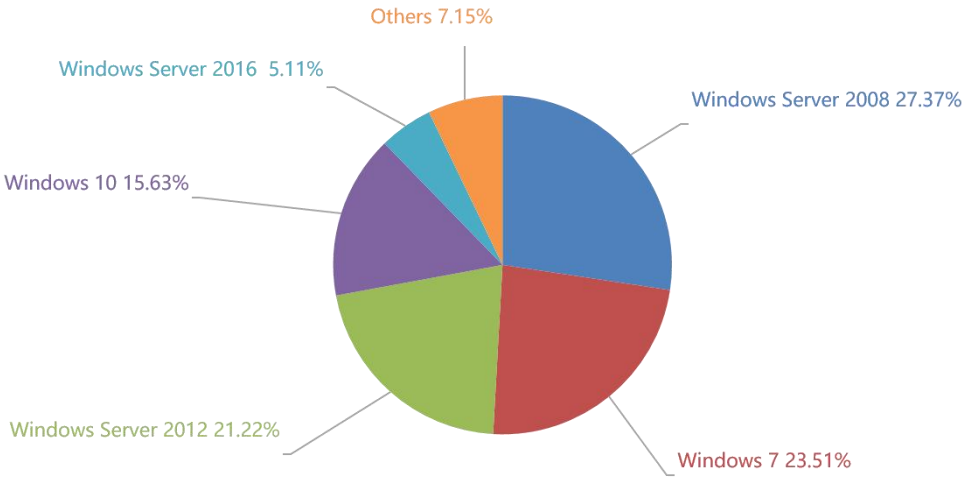
ARIETISHEALTH.COM	PINNACLETPA.COM	REPSOLSINOPECUK.COM
JTI.COM	selmi.com.br	Baumschlager Hutter Partners
confido.ae	confido.eu	equmedia.es
magnumphotos.com	Jasper Picture Company	co.langlade.wi.us
hgc.com.hk	province.namur.be	energym.co.il
konrad-mr.de	greatlakesmbpm.com	Highland Health Systems
Superloop ISP	Chin Hin Group	Meteksan Defence Industry
www.jordanairmotive.com	www.bsdc.ac.uk	CPA Advisors Group
Info Salons	Kenya Bureau Of Standards	VOSS.NET
UFCU.ORG	YAKULT.COM.PH	ROCHESTER.EDU
SHUTTERFLY.COM	DISCOVERY.COM	ASPENTECH.COM
MOTHERSON.COM	PAYCOM.COM	Gerber Childrenswear LLC
Blackjewel L.L.C.	Telepizza	The Traffic Tech
Quikcard Solutions Inc.	Jadranka Group	Dental One Craigieburn
ANL Packaging	BTU	GRIPA.ORG
SLB.COM	AMCTHEATRES.COM	AINT.COM
JACKENTERTAINMENT.COM	NASCO.COM	TGIDIRECT.COM
HONEYWELL.COM	CLEARESULT.COM	RADIUSGS.COM
Ministry of Energy and Mines of Cuba	Ministerio de Cultura de la República de Cuba	Ministry of Foreign Trade and Foreign Investment of Cuba
affinityhealthservices.net	Henock Construction	innodisgroup.com
Divgi-TTS	Eastin Hotel Makkasan Bangkok	SMS-SME
Algeiba.com	Amber Court	Maruchan Inc
Schmidt Salzman & Moran, Ltd	Wright Moore DeHart Dupuis & Hutchinson	Better System Co.,Ltd
www.protactics.com.co	BM GROUP POLYTEC S.p.A.	Hollywood Forever
Ayuntamiento de Arganda City Council	Polanglo	KIRWIN FRYDAY MEDCALF Lawyers LLP
ROBERT L BAYLESS PRODUCER LLC	Cabra Consulting Ltd	Pesquera Diamante S.A.
Weitkamp · Hirsch and Kollegen Steuerberatungsgesellschaft mbH	Kansas medical center LLC	Danbury Public Schools
Advanced Fiberglass Industries	Citelis Mobility	Motor Components, LLC
CONSOLENERGY.COM	KALEAERO.COM	AGILYSYS.COM
SCCU.COM	ARVATO.COM	RITEAID.COM
PIONEERELECTRONICS.COM	BAM.COM.GT	TOMTOM.COM
EMERSON.COM	Propper International	Nipun Consultancy
mamboafricaadventure	A123 Systems	LivaNova
MicroPort Scientific	panoramaeyecare.com	gis4.addison-il
RICOHACUMEN.COM	SMA.DE	VRM.DE
UMASSMED.EDU	VISIONWARE.CA	JHU.EDU
FMFCU.ORG	JPRMP.COM	WESTAT.COM
RADISSONHOTELSAMERICAS.COM	Customer Elation	Hamre Schumann Mueller & Larson HSML
Green Diamond	Belize Electricity Limited	CROWE.COM

AUTOZONE.COM	BCDTRAVEL.COM	AMERICANNATIONAL.COM
USG.EDU	CYTOMX.COM	MARYKAY.COM
FISCDP.COM	KERNAGENCY.COM	UOFLHEALTH.ORG
L8SOLUTIONS.CO.UK	TDAMERITRADE.COM	leeindustries.com
roys.co.uk	Evergreen Seamless Pipes & Tubes	Mission Parks
Tracker de Colombia SAS	Lane Valente Industries	Industrial Heat Transfer
DELARUE.COM	ENERGYTRANSFER.COM	PAYCOR.COM
NETSCOUT.COM	WOLTERSKLUWER.COM	CADENCEBANK.COM
BANKWITHUNITED.COM	NEWERATECH.COM	Lazer Tow
Star Island Resort	Indiana Dimension	Lawer SpA
NST Attorneys at Law	Uniquify	Geneva Software
MUJI Europe Holdings Limited	Betty Lou's	Capacity LLC
Wesco Equipment	Safety Network	Centex Personnel
Encore Pro Staffing	Carvin Software	Ella Insurance Brokerage
ATS Infrastructure	chasc.org	cls-group.com
gacegypt.net	siegfried.com.mx	betalandservices.com
Pinnergy	eyedoc.com.na	Bangladesh Krishi Bank
ASIC Soluciones	TRANSPERFECT.COM	QUORUMFCU.ORG
MERATIVE.COM	NORGREN.COM	CIENA.COM
KYBURZDRUCK.CH	UNITEDREGIONAL.ORG	TDECU.ORG
BRADYID.COM	BARRICK.COM	Avalign Technologies
Portugal Scotturb	guestgroup.com.au	Murphy
recamlaser.com	eurosupport.com	mitr.com
DURR.COM	Hoosier Equipment company	Yunus Emre Institute Turkey
Peroni Pompe	DVA - DVision Architecture	Jefferson County Health Center
Townsquare Media Inc	oneexchangecorp.com	snjb.net
Duncan Disability Law	Mutuelle LMP	Luna Hotels & Resorts
Brett Martin	blowtherm.it	Guatemala Military Intelligence Directorate
ALTARGRUP	Atherfield Medical Service	Ucamco Belgium

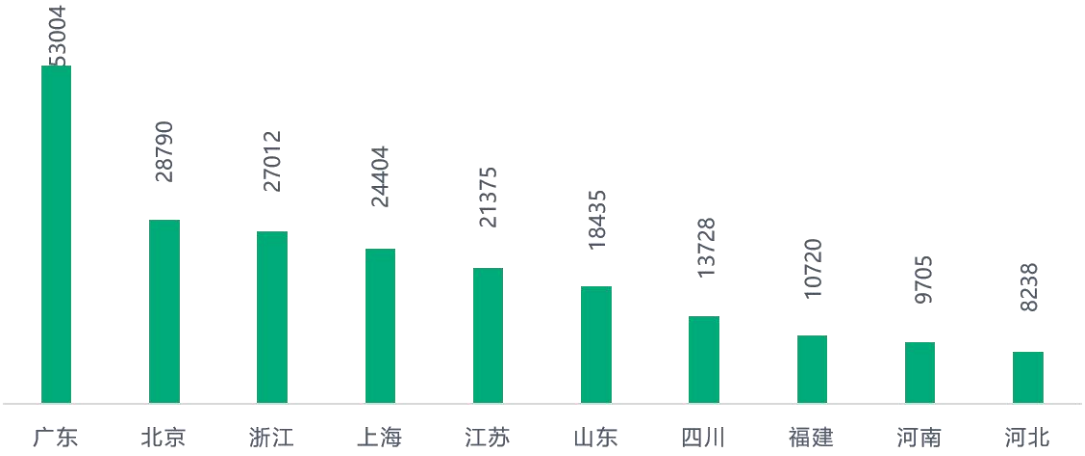
表格 2. 受害组织/企业

系统安全防护数据分析

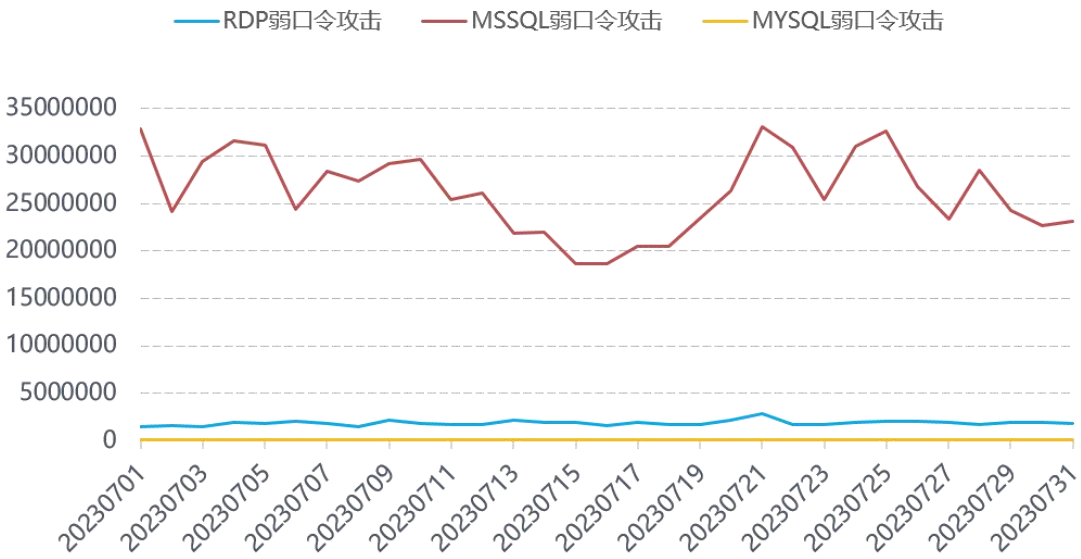
360 系统安全产品，目前已加入黑客入侵防护功能。在本月被攻击的系统版本中，排行前三的依次为 Windows Server 2008、Windows 7 以及 Windows Server 2012。



对 2023 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。



通过观察 2023 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。



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。

- devos：该后缀有三种情况，均因被加密文件后缀会被修改为 devos 而成为关键词。但本月活跃的是 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。

- locked：属于 TellYouThePass 勒索软件家族，由于被加密文件后缀会被修改为 locked 而成为关键词。该家族主要通过各种软件漏洞、系统漏洞进行传播。

- 360：属于 BeijngCrypt 勒索软件家族，由于被加密文件后缀会被修改为 360 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，本月新增通过数据库弱口令攻击进行传播。

- malox：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。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。

- faust：同 devos。

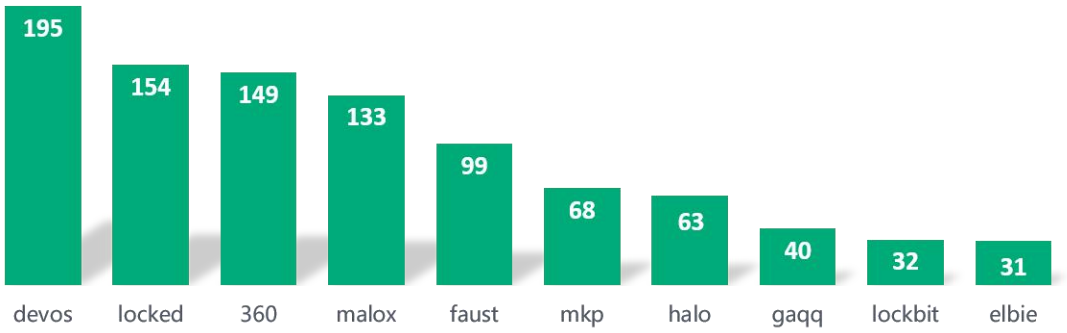
- mkp：属于 Makop 勒索软件家族，由于被加密文件后缀会被修改为 mkp 而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。

- halo：同 360。

- gaqq：属于 Stop 勒索软件家族，由于该家族频繁变更加密文件后缀导致很少出现在 top 查询量中。从开始传播至今其传播渠道一直是通过在破解软件网站上传激活工具、破解软件来诱导用户下载运行，且大部分网站均为国外网站。

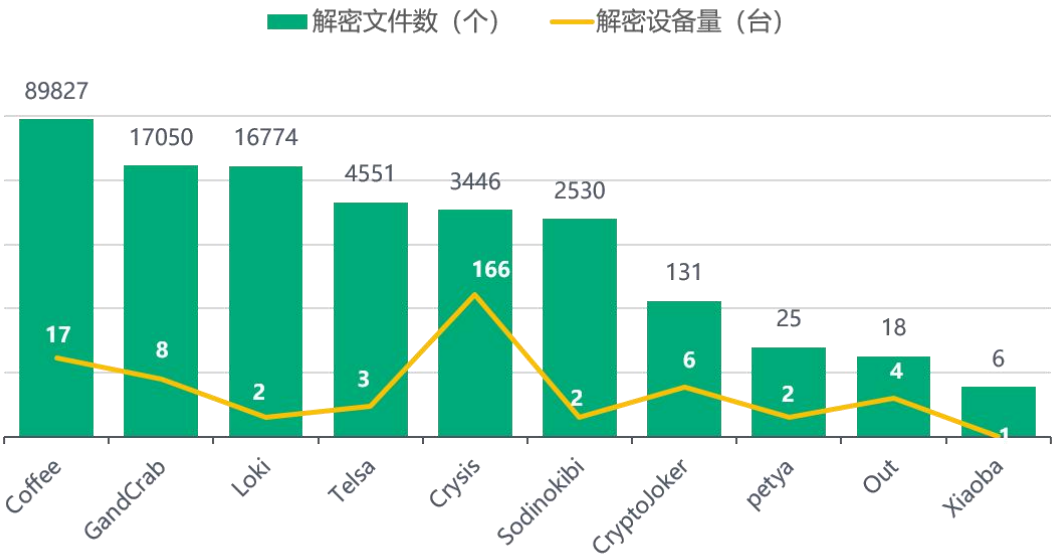
- lockbit：属于 LockBit 勒索软件家族，因被加密文件后缀会被修改为 lockbit 而成为关键词。该家族的运营模式可以分为两种不同的方式。第一种是无差别攻击，该方式会对全网发起数据库弱口令攻击或远程桌面弱口令攻击，一旦攻击成功，勒索软件将被投毒到受害者计算机中。在这种情况下，攻击者并不会窃取受害者的数据。第二种是针对性攻击，该方式主要针对大型企业，攻击者不仅会部署勒索软件，还会窃取企业重要的数据。如果受害组织或企业无法在规定时间内缴纳赎金，该团伙将会把数据发布到其数据泄露站点上，任何可以访问该网站的人都可以下载受害者的数据。

- elbie：同 devos。



解密大师

从解密大师本月解密数据看，解密量最大 的仍是 Coffee，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。


解密文件数（个）
解密设备量（台）
89827
17050
16774
4551
3446
2530
131
25
18
6
17
8
2
3
166
2
6
2
4
1
Coffee
GandCrab
Loki
Telsa
Crysis
Sodinokibi
CryptoJoker
petya
Out
Xiaoba


360数字安全
数 字 安 全 的 领 导 者