勒索软件流行态势分析

2023 年 3 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上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 3 月，全球新增的活跃勒索软件家族有:Merlin、726、DarkPower 等家族。其中 DarkPower 是本月新增的双重勒索软件，该家族最早出现于 2022 年，于本月开始采用双重勒索模式运营，其编程语言采用了在勒索软件中罕见的 Nim 语言。

以下是本月值的关注的部分热点：

1. CL0P 勒索软件再度活跃，超百家机构成受害者。

2. 水果巨头都乐遭受勒索软件攻击影响运营

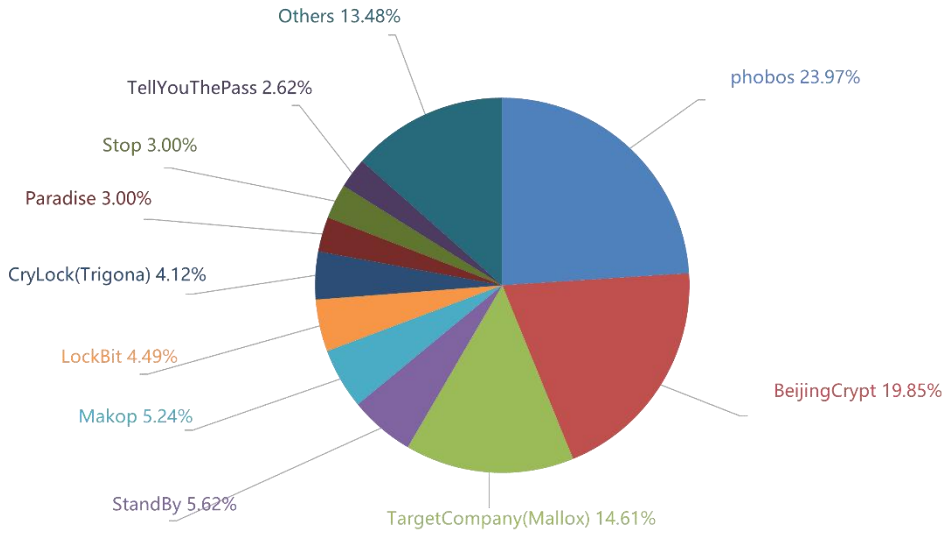
3. 法拉利在收到勒索赎金要求后遭数据泄露。

基于对 360 反勒索数据的分析研判，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。

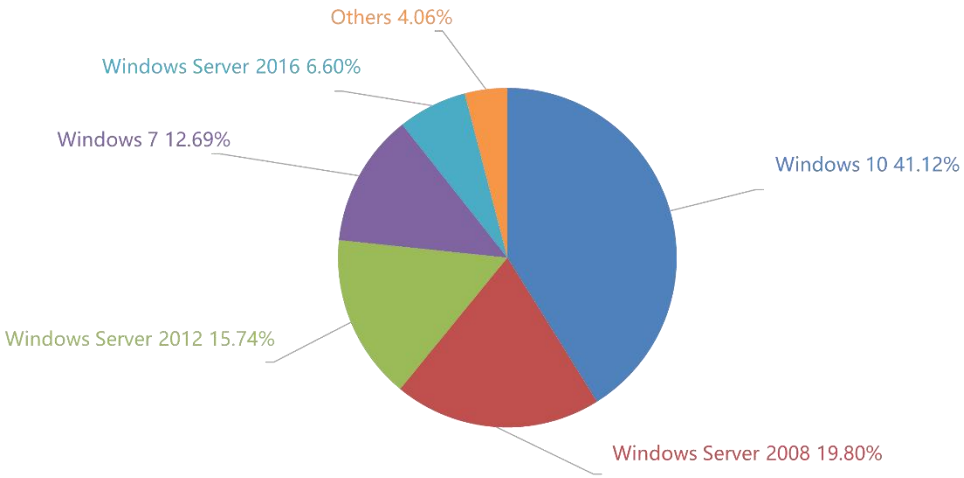
感染数据分析

针对本月勒索软件受害者所中病毒家族进行统计：phobos 家族占比 23.97%居首位，其次是占比 19.85%的 BeijingCrypt，TargetCompany(Mallox)家族以 14.61%位居第三。

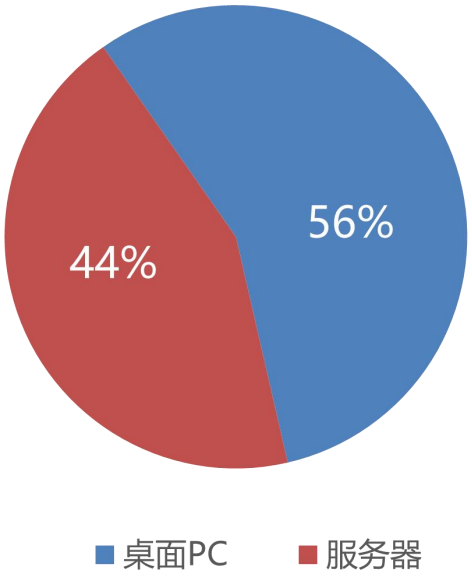
通过暴力破解远程桌面成功后手动投毒的 Standby 勒索软件家族感染量持续在上升。



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 2012。



2023 年 3 月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型仍以桌面系统为主。



勒索软件流行态势分析

CL0P 勒索软件再度活跃，超百家机构成受害者

停更近 2 年的 CL0P 勒索软件再度活跃，此次主要利用 Fortra GoAnywhere MFT 安全文件共享解决方案中存在的 0day 漏洞，对部署了该解决方案的公司展开数据窃取及勒索行动。

今年 2 月，GoAnywhere MFT 文件传输解决方案的开发人员曾警告其客户：该解决方案的管理控制台代码中存在 0day 远程代码执行漏洞 CVE-2023-0669。虽然该开发人员并没有公开分享该漏洞的利用细节，但很快就发布了概念验证漏洞，随后又发布了该漏洞的补丁。

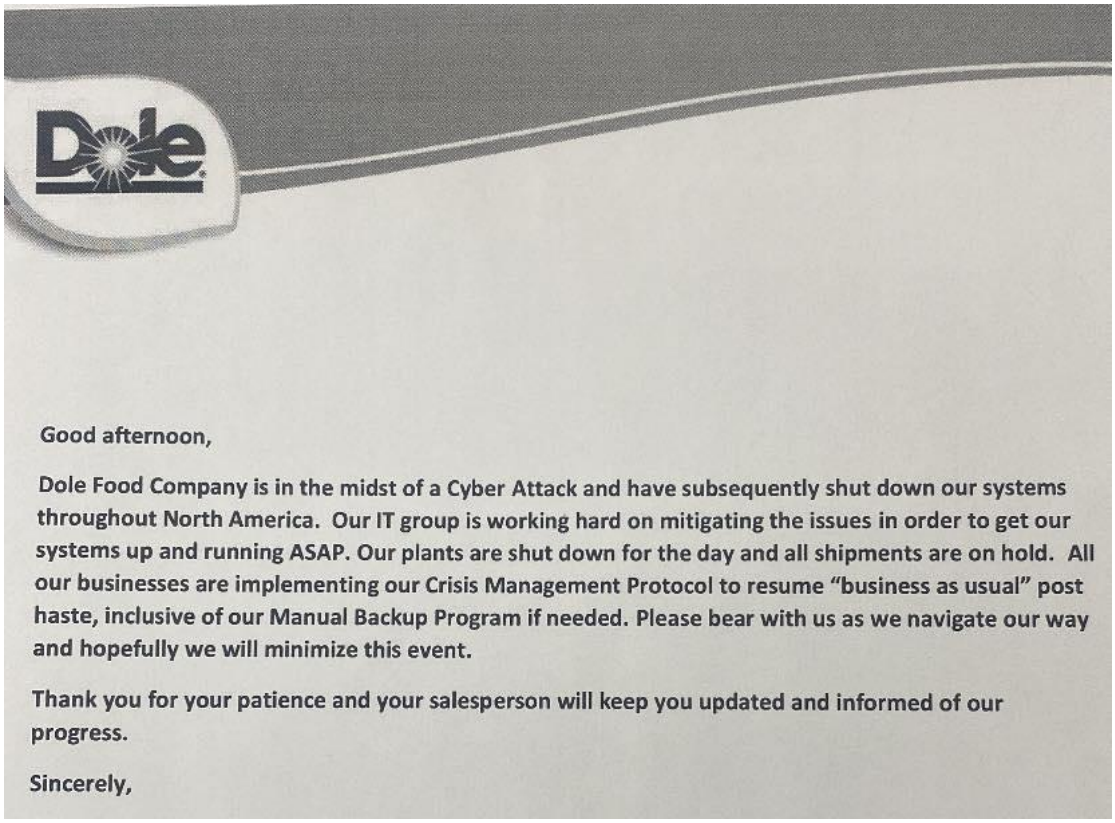
而就在 GoAnywhere 补丁发布后的第二天，Clop 勒索软件团伙便表示他们对这些攻击负责。该组织声称他们利用该漏洞在十天内窃取了 130 家公司的数据。此后，社区卫生系统（CHS）和哈奇银行两家公司披露称存储在 GoAnywhere MFT 中的数据遭到窃取。本月，CL0P 勒索团伙在其"数据泄露网站"上传了包括日立能源、多伦多市等 104 个组织/企业的数据。

水果巨头都乐遭受勒索软件攻击影响运营

全球最大的果蔬生产及分销商都乐食品公司发声明表示受到勒索软件攻击，并正对攻击展开应对。关于此次攻击事件公布的细节很少，都乐仅表示目前正在调查“事件的范围”且“影响有限”。

尽管都乐将影响描述为“有限”，但美国德州一家杂货店在 Facebook 上泄露的一份备忘录表明，这家食品巨头被迫关闭了其在北美的生产工厂并已停止向杂货店发货。

一周以来，北美地区消费者一直在抱怨商店货架上预包装的都乐沙拉短缺。虽然该公司没有透露攻击发生的具体时间，但这很可能是这次勒索软件攻击造成的短缺。



法拉利在收到勒索赎金要求后遭数据泄露。

意大利豪华跑车制造商法拉利确认遭到到了勒索攻击。据法拉利公司称，在攻击者获得对公司部分 IT 系统的访问权限后，收到了赎金要求，同时数据也已遭到泄露。

据公司表示，事件中遭泄露的客户信息包括姓名、地址、电子邮件地址和电话号码。 而到目前为止，法拉利尚未发现付款细节、银行帐号或其他敏感付款信息被访问或窃取的证据。

CLIENT COMMUNICATION

Dear Ferrarista,

We regret to inform you of a cyber incident at Ferrari, where a threat actor was able to access a limited number of systems in our IT environment. As part of this incident, certain data relating to our clients was exposed including names, addresses, email addresses and telephone numbers. Your data may have been included as part of this incident. However, based on our investigation, no payment details and/or bank account numbers and/or other sensitive payment information, nor details of Ferrari cars owned or ordered have been stolen.

黑客信息披露

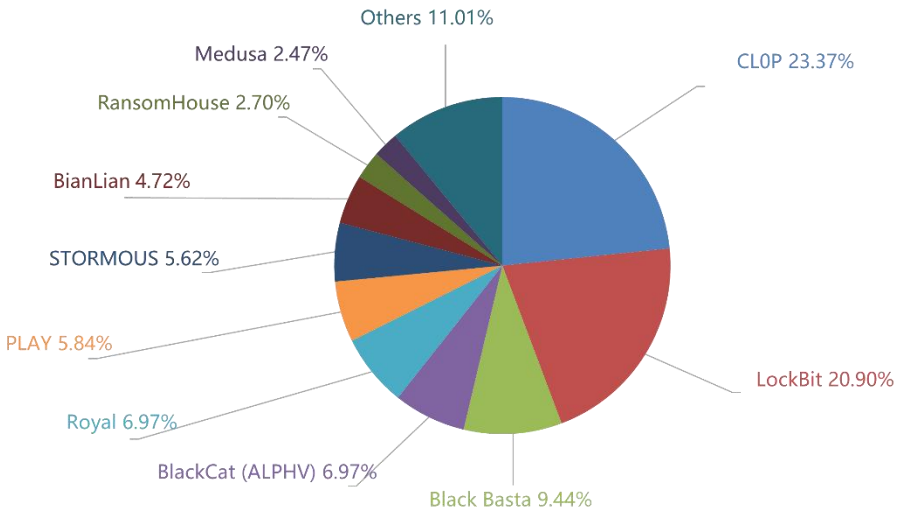
以下是本月收集到的黑客邮箱信息：

filecracker@onionmail.org	filecracker@msgsafe.io	medusa.serviceteam@protonmail.com
xiopjioht@onionmail.org	xiopjioht@mail.ee	ncuedorockla20173@gmail.com
joel.carsel@gmx.com	Helpadmiin@tutanota.com	hotwheels@onionmail.com
doktortalker@cock.li	Helpadmin@mail.ee	johntorrington1843@gmx.com
Lollooki@protonmail.com	department@bingzone.net	Hairysquid@onionmail.org
indianguy@onionmail.org	datahelp321@nigge.rs	jaamesgonzaleswork1972@protonmail.com
laraholmort@protonmail.com	geenakormann@protonmail.com	chiaraKolkmann@tutanota.com
DineshSchwartz1965@protonmail.com	RupertMariner1958@protonmail.com	StephanForenzzo1985@protonmail.com
pretty_hardjob2881@mail.com	dprworkjessiaeye1955@tutanota.com	harrynarson@protonmail.com
Jeremyhilton@mail.com	jamesbrockner@tutanota.com	flydragon@mailfence.com
Seven_Legion2@aol.com	ivanivanov34@aol.com	mserbinov@aol.com
load180@aol.com	trojanencoder@aol.com	vpupkin3@aol.com
base1c1c1c@gmail.com	deskripshen1c@gmail.com	vernutfiles@gmail.com
helpfiledeskript111@gmail.com	watnik91@aol.com	watnik91@gmail.com
systemsinfo32@gmail.com	sishelp100@gmail.com	deskr1000@gmail.com

marvianna1953@gmail.com	moshiax@aol.com	d_madre@aol.com
ninja.gaiver@aol.com	scasiva@aol.com	igor_svetlov2@aol.com
cryptolocker@aol.com	iizomer@aol.com	gcaesar2@aol.com
help163btc@163.com	hontekilla@aol.com	monica.moka@aol.com
eric.decoder10.@gmail.com	madeled@mail.ru	datarestorehelp@airmail.com
dark4wave@yandex.com	mosnar2023@gmail.com	mosnar@msgden.net
doctorhelperss@gmail.com	helpersdoctor@outlook.com	Merlin@outlookpro.net
Merlin@cyberfear.com	Merlin@onionmail.org	abuse@telegram.org
dmca@telegram.org	recover@telegram.org	security@telegram.org
sms@telegram.org	sticker@telegram.org	stopCA@telegram.org
support@telegram.org	@exilenceTG	534411644559@ngs.ru
534411644559@ngs.ru	DavidTIzzo@dnmx.org	ch360@tutanota.com
ch360@mailfence.com	vodaigaz@outlook.com	goodmorningfriends@onionmail.org
emcrypts@msgsafe.io	bimbom123@tuta.io	venolockdate1@rape.lol
decoding24@onionmail.com	decoding141@tuta.io	@decoding24

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 445 个组织/企业遭遇勒索攻击，其中中国有 5 个组织/企业在本月遭遇了双重勒索/多重勒索。此外，有 15 个组织/企业未被标明，因此不再以下表格中。

ativy.com	etkinllc.com	tecnova.com
OptionMetrics	1.com	Armstrong Watson
Lewis & Clark College	groupe-seche.com	Meloc
MULTIPLAN.COM	ieseco	matrixtelecoms
GOV.PL	theus-industries.fr	tharworx.com
WESSEX	Hospital Clinic de Barcelona	Hit Promotional Products
Temporary Leak Page #0013995NTa	CANTALK	hammondlumber.com
psenergy.com	FINANCE INSTITUTION AUCTION	nts.go.kr
Savanna Technical College	The Ultra-met	MERS Missouri Goodwill Industries
BMW France	Oscar Software	Jablite
AV Industries	PCCARX_2	hico-ics.com
grupcovesa.com	swiftatlanta.com	piramal.com
City of Modesto, CA	tecnosysitalia.eu	All4Labels
IRCO	Tanbridge House School	Helmholtz Zentrum Munchen
Wymondham College	OKSGROUP	ARROWAL
Ingersoll Rand	Linx	Furuno
lqtbg.com.cn	islandinsurance.ca	County Materials Corporation
DUKANE	ulmacarretillas.com	ita-moulding-process.com
Ville de Lille	Picou Builders Supply	Kk Mehta Cpa Associates
Lightcast	Optica	Pizza 73
James, McElroy and Diehl	Lysander Associates	TAC
Guyana Goldfields	Turvatehnika	Rob Levine & Associates Lawyers
Socomec	Konica	Polytech
Ngocyenviet	berjayaClubs	giga.com.vc
jubileeinsurance.com	DGCX	La Providence
slipstreaminc.org	demechindia.com	precisionit.co.in
Cesce	Cospec Srl	BISSELL.COM
EMERALDX.COM	CAJASANRAFAEL.COM.MX	TAS.GOV.AU
ENERJISAURETIM.COM	INTELLICARE.COM.PH	CRESCENTHOTELS.COM
COLMAC.COM	INVESTORCOM.COM	Confido
Sun Global	lclattorneys.com	wbactc
Accolade Group Inc Levelwear	Zeller	Tip Top Poultry
CCAA	IMAGINE360.COM	Teklas
Sun Pharmaceutical Industries Ltd.	securens.in	THECYPRINUS.COM
SPI.CO.ZA	DETECH.COM.TR	GRUPOFLORAPLANT.COM
ALTO.US	DAVINCI	Berjaya
Novelis	bianchiindustry.com	GOA.GOV.IN

INTERTERMINALS.COM	GLOBALFARM.COM.AR	ATOS.NET
TGW.COM	DERK.CL	REDBOXVOICE.COM
PROGRESSION.COM	UNIMELB.EDU.AU	Gujarat Mineral
CROWNRESORT.COM.AU	BRIDGEWAY.COM.PH	TLG.COM
HainPureProtein Plainville Farms	Comune Taggia	VLS
Autoridad de Acueductos Y Alcantarillados	bluebirdnetwork	PHOENIX.TECH
SODALESSOLUTIONS.COM	NATIONSBENEFITS.COM	SHOLASTIC.COM
VUMACAM.CO.ZA	TORONTO.CA	CLOUDMED.COM
DPWORLD.COM	SOLPAC.CO.JP	VIRGIN.COM
LEGACY-TECHNOLOGIES.DE	OSHCO.COM	GRAY.TV
ORCAAUDIT.COM	CHEMILAB.COM.CO	PAYBOXAPP.COM
VERRAMOBILITY.COM	BUNZL.COM	FIRST-CENTRAL.COM
ALIVIAHELTH.COM	HORMELFOODS.COM	THECROSBYGROUP.COM
MUNICHRE.COM	GRUPOVANTI.COM	VOLARIS.COM
ACCUZIP.COM	SEPIRE.COM	WVI.ORG
TTBH.ORG	HUMANGOOD.COM	KANNACT.COM
CINEPLEX.COM	AMERIJET.COM	GDI.COM
ZOSKINHEALTH.COM	HRTRANSIT.ORG	PLURALSIGHT.COM
PPF.CO.UK	Graceworks Lutheran Services	LASOLTEL.FR
rockinsurancebrokers	PG.COM	CROSSVILLEINC.COM
LESLIESPOOL.COM	US District Court	Troutman Pepper
Advance America	Dayton Superior	Design CATAPULT
Kress	cabinet-paillet.fr	Yaskawa Motoman
mangiainc.com	SUPPLYCORE	Zeus Energy S.A.C
jenparking.com	transports-douaud.com	bakermech.com
the3rivers.net	stolt-nielsen.com	cityofallenpark.org
ksrsac.karnataka.gov.in	roslevauto.dk	gproulxinc.com
Atlas Security	co.ottawa.oh.us	oaklandca.gov
ALKF+	alyasrafoods.com	Sunward Pharmaceutical (Sunward)
Indonesia Power	emotorsdirect.ca	SAKSFIFTHAVENUE.COM
telepizza.com	National Board of Osteopathic Medical Examiners	Aces Electronic Co Ltd
Desman Design Management	Avila Real Estate	WOODHAVEN
Potandon Foundation	Ennis, Inc.	Sandals Resorts International
Michael & Son	Sound Publishing	ATCDT
PFC Brakes	Bayou Title	NOVATI
Echelon Fitness	clair	Alessi
The Norfolk Capital Group	Macomb Group	Mettis Aerospace
KWS	Newly Weds Foods	XLTRAILERS
VORNADO	CEC ELECTRICAL	MARSHALLAMPS

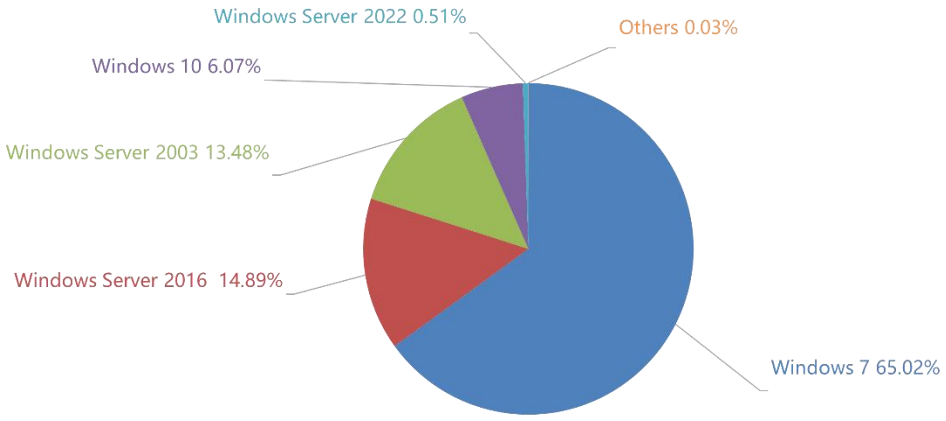
ACEA Energia	Rudman Winchell	Hall Booth Smith
Nor-Cal Beverage	MAKLERSOFTWARE	Mondial and Framec
fflawoffice	Tri Counties Bank	Kittle's
Norman S. Wright Climatec	jaureguy.com.ar	stavinvest.cz
hitzler-ingenieure.de	id-logistics.com	bbsautomation.com
spoormaker.co.za	FABREGA MOLINO (fmm.com.pa)	Law Firm Vazquez Nava Consultores y Abogados, S.C
Sutton and Jacobs	Collins Electrical	James Group
boothtransport.com	Stanley Steemer	A&T group of companies
Berga Recycling	Pine Tree Commercial Realty	Norman Shutters
TaxAssist Accountants	draftPros	DGM Industrie
AAA Energy Service	r-pac.com	Dancenter
Optieng	Guardian Capital	Ring: Security Systems
WALSHALBERT	npauctions.com	Muzzo Group
copart.com	JAYMART.CO.TH	SERVICESTREAM.COM.AU
WORLDMARKET.COM	WILDFIRE-DEFENSE.COM	SWEEPINGCORP.COM
TUEBORA.COM	RATELINX.COM	FERGUSON.COM
ACENURSING.ORG	WELLBE.COM	HELLOBRIGHTLINE.COM
HITACHIENERGY.COM	SAE.ORG	AVIDXCHANGE.COM
GALDERMA.COM	NEWEUROPEANOFFSHORE.COM	MEDEXHCO.COM
INVESTQUEBEC.COM	RIOTINTO.COM	ITXCOMPANIES.COM
HOMEWOODHEALTH.COM	GUINNESSPARTNERSHIP.COM	ALLIEDBENEFIT.COM
USWELLNESS.COM	ktcs.com.my	National Institute of Ocean Technology
Audio Video	buehnen.de	meatel.com
perfectplacement.co.uk	waldogeneral.com	mandirisekuritas.co.id
Ecolog International	regaltax.us	FICHTNER
Liberty Lines	NRG Innovations	essendant.com
kaycan.com	Faraday Technology	fiege.com
dmos.com	St. Kitts & Nevis	RUBRIK.COM
ONEX.COM	Manning Building Supplies	Tarolli
LLPGroup	sabena-engineering.com	maximumind.com
plasticproductsco.com	Royal Dirkzwager	E&S Heating & Ventilation Ltd
Entigrity Solutions	Bishop Luffa School	grupohospitalarvidas.com.br
schradercamargo.com	greggardnergm.com	wyckoffcomfort.com
bonta-viva.it	meinet.com	lubrimetal.com
cqservice.sk	brandywine-homes.com	cktc.edu
omegaservicos.com.br	inphenix.com	favoritefoods.com
Berkeley County Schools	Real Pro	Leemock
The M. K. Morse	Secure Wrap	Russell Finex
Delaware Life Insurance Company	eprinsa.es	techhard.ae

micos.com	drilmaco.com	schauenburg.com
heidelbergbread.com	southamericantours.com	wunan.org.au
alpes-sante-travail.org	kisp.com	KMVP
PEOPLECORPORATION.COM	MEDMINDER.COM	AXISBANK.COM
HOUSELOAN.COM	ALIVIAHEALTH.COM	Highway Equipment
Ferretería EPA	Little Mountain Residential Care and Housing Society	Hard Manufacturing
Materialogic	Jackson Dean Construction	Richard Sanders
Gottschol Alcuilux	sagardoy.com	Methodist Family Health
pmsoffice.de	Garbarino SAICel	National Business Furniture
onyx-pharma.dz	imtenan.com	agados.cz
evant.com.tr	arineta.com	rcc.gob.pe
goliplik.com.tr	mdclone.com	betastree.fr
northgatesd.net	Wellington Power Corporation	Walker SCM
Brauerei Schimpf	Thomaston Mills	audio-technica.com
The WorkPlace	GROUPAMANA.COM	Minneapolis Public Schools
Law Foundation of Silicon Valley	Wilhelm	PROTEKTOR
Krinos Foods	Lehigh Valley Health Network	Los Altos Foods
steico.com	The Institute of Space Technology	Circa Jewels
HATCHBANK.COM	Kventa Kft	HAW Hamburg
AddWeb Solution Pvt	Kimko Realty	Rimex
Victoria Park	tjel.net	Vesuvius
Traffic Ticket Office	egas.no	SkyFiber Networks
CMMG Inc	Welty Building Company	blackswanhealth
AICHELIN UNITHERM	HUNOSA	AASP
ACCSC	Zerbe Retirement Community	PLP Architecture
Kenya Airports Authority	Parques Reunidos	Open MRI Bala
Title Cash Now	6connex	FIMM
Oakland	Bettuzzi And Partners	ascentengrs.com
The Metropolitan Opera		

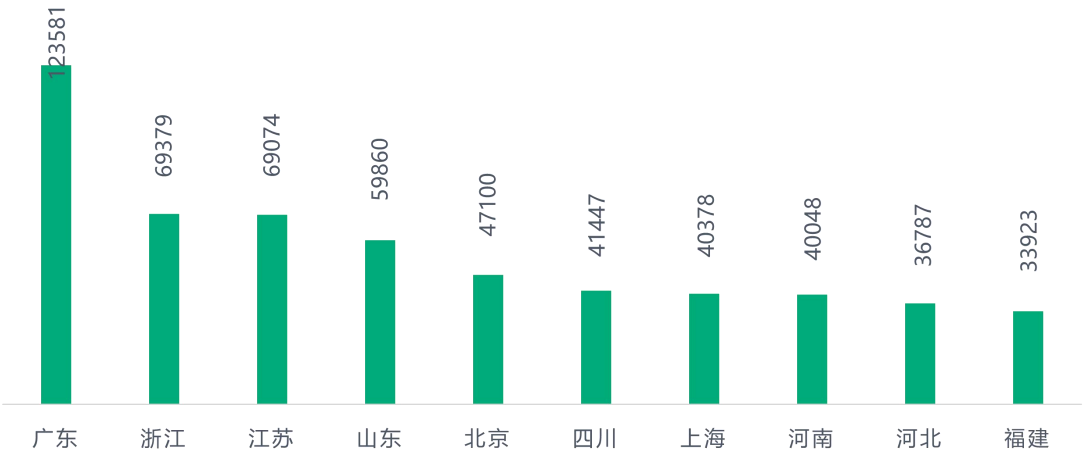
表格 2. 受害组织/企业

系统安全防护数据分析

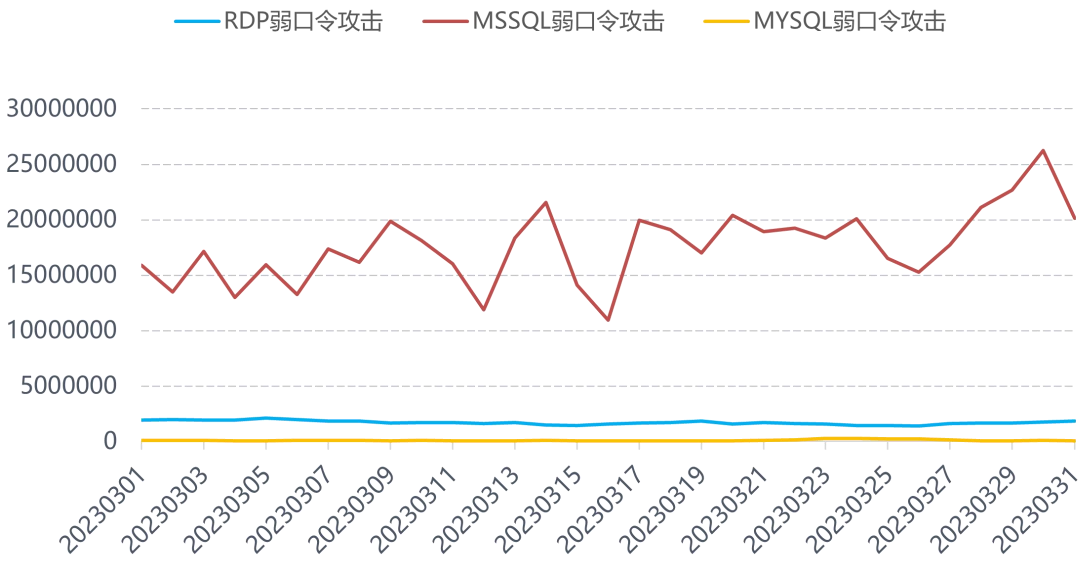
360 系统安全产品，目前已加入黑客入侵防护功能。在本月被攻击的系统版本中，排行前三的依次为 Windows Server 7 、Windows 2016 以及 Windows Server 2003。



对 2023 年 3 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 3 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。

- 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。

- mallox：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。

- halo：同 360。

- faust:属于 phobos 勒索软件家族，因被加密文件后缀会被修改为 faust 而成为关键词。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。

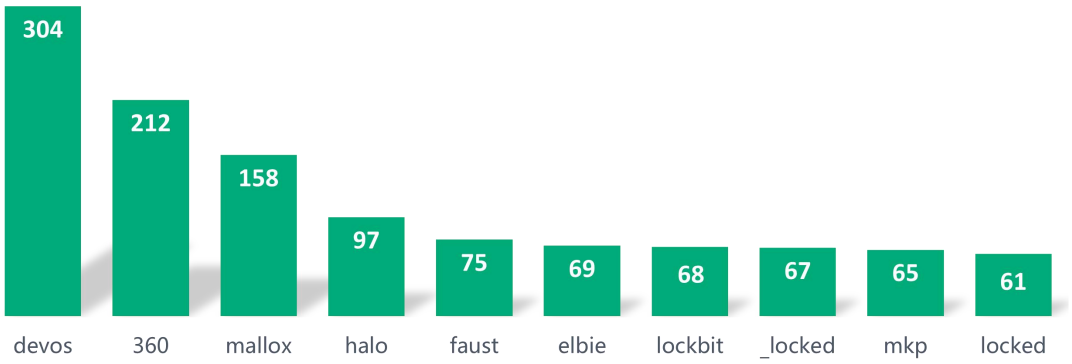
- elbie：同 faust。

- 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。

- _locked:属于 CryLock(Trigona)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。该家族主要的传播方式：暴力破解远程桌面口令成功后手动投毒以及暴力破解数据库密码后远程投毒。

- 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。

- 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数字安全
数 字 安 全 的 领 导 者