勒索软件流行态势分析

2023 年 4 月

360数字安全

数 字 安 全 的 领 导 者

近年来，随着新型勒索软件的快速蔓延，企业的数据泄露风险不断上升，高额勒索案件频繁出现。可以说，勒索软件的影响范围越来越广，给企业和个人带来的危害性也越来越大。360 全网安全大脑可以对勒索软件进行全方位的监测与防御，能够为需要帮助的用户提供反勒索服务。目前，360 反勒索服务已累计接收、处理上万起勒索软件感染求助。

2023 年 4 月，全球新增的活跃勒索软件家族有:CrossLock、UNIZA、RTM Locker、DarkAngels、Money Message 等。其中 DarkAngels 是一款双重勒索软件，但尚未在其数据泄露网站公开过受害者信息；RTM Locker 是一款以企业为目标的勒索软件，其 Linux 加密器疑似专门为攻击 Vmware ESXi 系统而创建。

以下是本月值得关注的部分热点：

1. 近期新发现针对 Mac 设备的 LockBit 勒索软件。

2. Google 广告推送被勒索软件团伙使用的 BumbleBee 恶意软件。

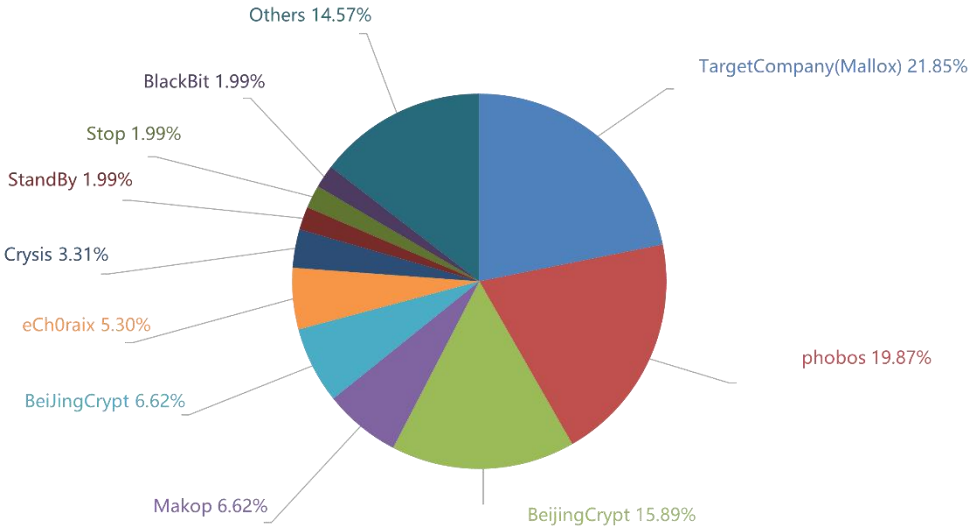
3. 新型勒索软件 Money Message 索要百万美元赎金。

基于近期对 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）特发布本报告。

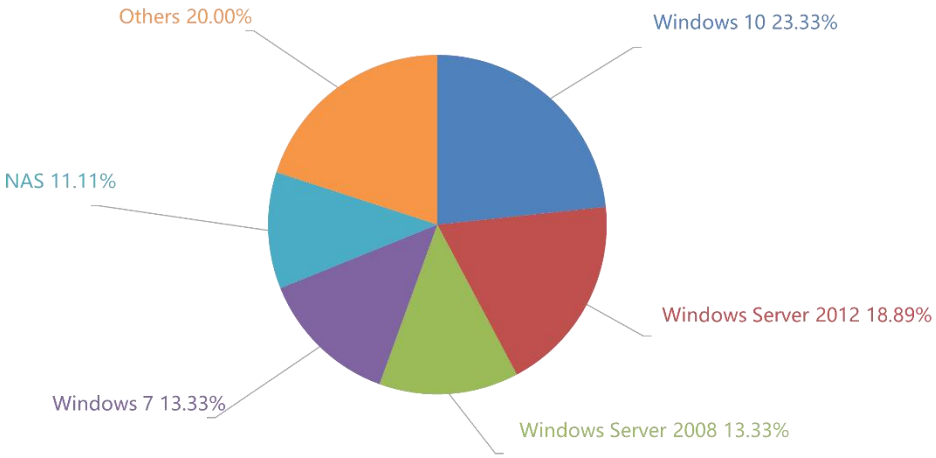
感染数据分析

针对本月勒索软件受害者所中病毒家族进行统计：TargetCompany(Mallox)家族占比 21.85%居首位，phobos 家族占比 19.87%位居第二，BeijingCrypt 家族占比 15.89%位居第三。

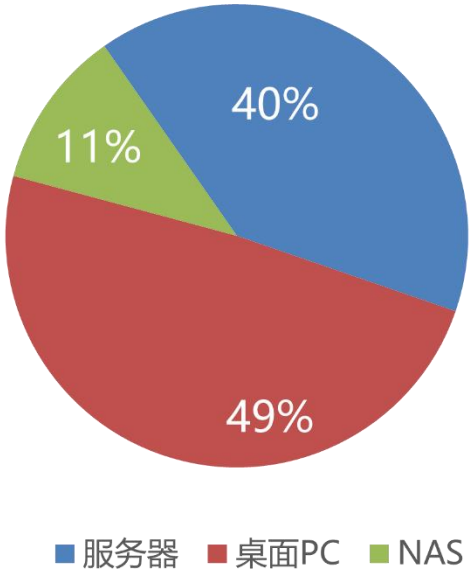
本月针对 NAS 设备进行攻击的 eCh0Raix 勒索软件家族有明显上升。



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 2012 以及 Windows Server 2008。



2023 年 4 月受攻击的系统类型仍以桌面系统为主。

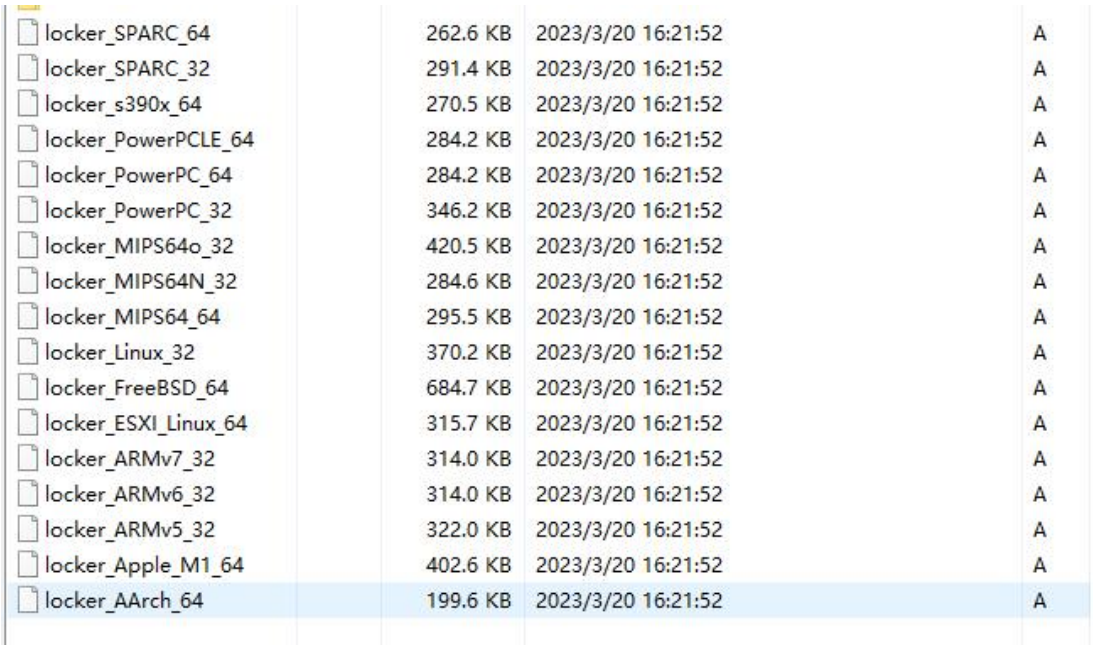


勒索软件疫情分析

近期新发现针对 Mac 设备的 LockBit 勒索软件

LockBit 勒索组织首次创建了针对 Mac 平台的勒索软件，很可能成为第一个专门针对 MacOS 的主流勒索软件。

从历史数据上看，LockBit 组织曾创建使用过专门针对 Windows、Linux 和 VMware ESXi 服务器等平台的勒索软件。近期发现该组织还创建了之前未在野外攻击中出现的，针对 MacOS、FreeBSD 等系统以及 ARM、MIPS 和 SPARC 指令集的勒索软件。



locker_SPARC_64	262.6 KB	2023/3/20 16:21:52	A
locker_SPARC_32	291.4 KB	2023/3/20 16:21:52	A
locker_s390x_64	270.5 KB	2023/3/20 16:21:52	A
locker_PowerPCLE_64	284.2 KB	2023/3/20 16:21:52	A
locker_PowerPC_64	284.2 KB	2023/3/20 16:21:52	A
locker_PowerPC_32	346.2 KB	2023/3/20 16:21:52	A
locker_MIPS64o_32	420.5 KB	2023/3/20 16:21:52	A
locker_MIPS64N_32	284.6 KB	2023/3/20 16:21:52	A
locker_MIPS64_64	295.5 KB	2023/3/20 16:21:52	A
locker_Linux_32	370.2 KB	2023/3/20 16:21:52	A
locker_FreeBSD_64	684.7 KB	2023/3/20 16:21:52	A
locker_ESXI_Linux_64	315.7 KB	2023/3/20 16:21:52	A
locker_ARMv7_32	314.0 KB	2023/3/20 16:21:52	A
locker_ARMv6_32	314.0 KB	2023/3/20 16:21:52	A
locker_ARMv5_32	322.0 KB	2023/3/20 16:21:52	A
locker_Apple_M1_64	402.6 KB	2023/3/20 16:21:52	A
locker_AArch_64	199.6 KB	2023/3/20 16:21:52	A

此次发现的新勒索软件中还存在一款名为 locker_Apple_M1_64 的勒索软件。经分析，该软件运行于 Apple Silicon 最新的 Mac 系统中。此外，该研究人员还发现了针对旧版 PowerPC 平台 Mac 系统的样本。

Google 广告推送被勒索软件团伙使用的 BumbleBee 恶意软件

以企业为攻击目标的 Bumblebee 恶意软件正通过 Google Ads 和 SEO 污染手段进行传播，攻击者以推广 Zoom、Cisco AnyConnect、ChatGPT 和 Citrix Workspace 等流行软件为诱饵进行诱导扩散。

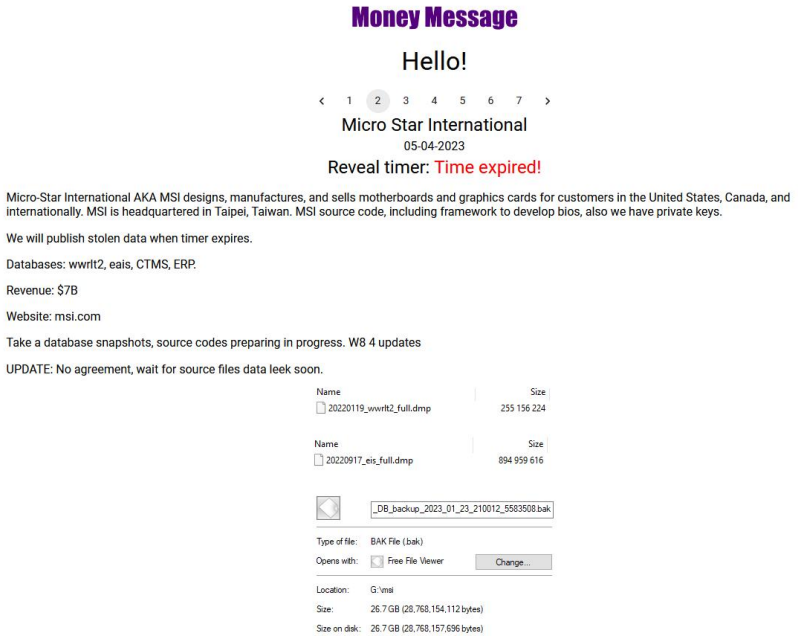
Bumblebee 是一款恶意软件加载器，首次捕获时间为 2022 年 4 月。根据研究，有理由认为其是由 Conti 勒索软件团队主导，用于替代 BazarLoader 后门软件来获取网络的初始访问权限，并为后续的勒索攻击进行铺垫。2022 年 9 月，研究人员发现了该软件的在野攻击案例，主要利用 PowerSploit 框架将反弹 DLL 注入到内存当中发动攻击。

近期，安全人员发现了该软件利用 Google Ads 的新动向——通过宣传流行应用程序的钓鱼版本来将自身恶意软件加载器传播给毫无防备的受害者。

新型勒索软件 Money Message 索要百万美元赎金

3 月底，一款名为“Money Message”的新勒索软件出现在互联网中，该勒索软件针对全球受害者发动攻击并要求支付数百万美元的赎金以防止泄露数据及换取数据解密。

目前，攻击者在其勒索网站上列出了 6 名受害者，其中包括微电子制造商 MSI 及航空公司 Biman Airlines。攻击者在其数据泄露网站上列出了 MSI 的 CTMS 和 ERP 数据库以及包含软件源代码、私钥以及 BIOS 固件等文件的屏幕截图。Money Message 威胁称要在五天内公布被盗 1.5T 大小的数据文件，除非 MSI 满足其高达 400 万美元的赎金要求。



黑客信息披露

以下是本月收集到的黑客邮箱信息：

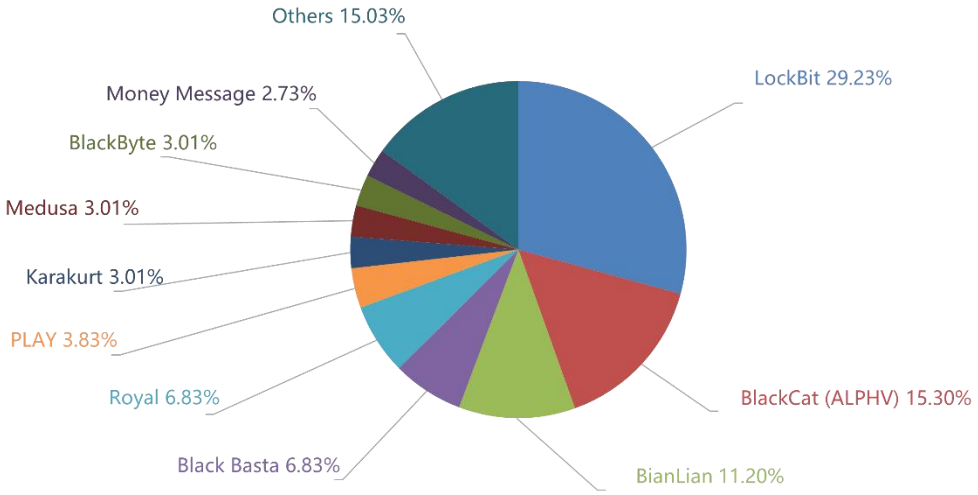
MonaharDecryption@airmail.cc	mallox.resurrection@onionmail.org	lockbitdecrypt@msgsafe.io
lockbitdecrypt@onionmail.org	malloxdata@mailfence.com	malloxdata@tutanota.com
torresproxytg@proton.me	sleepdb@my.com	Sleepdb@tutanota.com
buydecoder@nerdmail.co	@data_decrypt	lockdata@mailfence.com
smbppt@tutanota.com	xhermes@rambler.ru	Johnatannielson@protonmail.com
charlefletcher@onionmail.org	support2022@cock.li	buybackdate@nuke.africa
jackie.ma@tuta.io	xhermes@rambler.ru	falcondal@horsefucker.org
falcondal@tuta.io	D4nte@onionmail.org	Backup@cyberfear.com
bestway4u@mailfence.com	bestway4u@onionmail.com	crypter@firemail.de
helper@firemail.de	dschen010203@gmail.com	baseus0906@goat.si

carlosrestore2020@aol.com	criptoman@mailfence.com	gizmo12@tutanota.com
warthunder089@mailfence.com	warthunder089@tutanota.de	help_havaneza@cryptolab.net
mrbroock@msgsafe.io	carabas1337@proton.me	quickstep@tuta.io
@Stop_24	backjohn131@gmail.com	backjohn@tutanota.com
RavenRestore@yandex.com	fastwindglobe@cock.li	@decryptfastwind
fastwindGlobe@mail.ee	pbs@ciptext.com	pbs24@tutanota.com
lockdata@tutanota.com	lockdata@cyberfear.com	unlockhelppk@xmpp.jp
mallox@onionmail.org	savetime@cyberfear.com	icanrestore@onionmilorg
syntaxerror@firemail.cc	@decryptfastwind	fastwindglobe@cock.li
inter_hunter@tuta.io	jerd@420blaze.it	filesupport@airmail.cc
recoverdata@onionmail.org	recoverlokidata@gmail.com	umbrage@onionmail.org
filesupport@airmail.cc	decgodloki@tutanota.com	decgodloki@onionmail.com
decryptyourfileenvi@onionmail.org	unlockerhelp@onionmail.org	contact03@ tutanota.com
trust03@onionmail.org	endevecsupp@tutanota.com	unlockloki@onionmail.org
unlockloki@mailfence.com	vulcanteam@onionmail.org	vulcanteam@mail2tor.com
decryption.helper@aol.com	antilock@keemail.me	lokiloki@mailfence.com
lokisupp0rt@yandex.com	lokihelp@onionmail.org	lokihelp@mail2tor.com
emeraldcrypt@onionmail.org	decrliv@aol.com	emeraldcrypt@tutanota.com
antilock@cock.li	go.ahead@tutanota.com	anylock@cock.li
anylock@keemail.me	sirhirad@cock.li	sirboz@onionmail.org
main642@ tutanota.com	everythingwillbeok@onionmail.org	winston01@msgsafe.io
winston01@onionmail.org	supporting@firemail.cc	lokisupport@onionmail.org
ghosttm@zohomail.com	ransomware919@zohomail.eu	ransomware919@mailfence.com
lollooki@protonmail.com	lollooki@yandex.com	supploki@ onionmail.org
supploki@mailfence.com	umbrage@cyberfear.com	ghostenc@mailfence.com
ghostenc@tutanota.com	reopen@tutanota.com	mrlokilocker@telegram.me
ransom101@tutanota.com	draculakink99@outlook.com	willbeok1234@tutanota.com
everythingwillbeok@mailfence.com	sirsilent1@onionmail.org	loki_supp@outlook.com
trust003@protonmail.com	trust03@tutanota.com	data2022@aol.com
lokiguide@yahooweb.co	rdpmanager@onionmail.org	sirsilent2@onionmail.org
data2022@onionmail.org	vpsran1fat@cyberfear.com	vpsran1fat@tutanota.com
recoverdata@mail2tor.com	dr.dcrypter@mailfence.com	d4rkw4ve@tutanota.com
irishman@onionmail.com	irishman@tutanota.de	advanceloki@mailfence.com
advanceloki@tutanota.com	roxlock@keemail.me	minioncrypt@tutanota.com
minioncrypt@bingzone.net	rdecrypt@ yandex.com	exploit1@mailfence.com
exploit2@cock.li	dark4wave@yandex.com	rdpmanager@airmail.cc
filemanager@mailfence.com	unlockpls.dr01@protonmail.com	unlockpls.dr01@yahoo.com
ultimatehelp@techmail.info	miracle11@keemail.me	ultimatehelp@keemail.me
decnow@tutamail.com	decnow@protonmail.com	leo.decrypter@protonmail.com
leo.rinse@mailfence.com	decnow@msgsafe。 io	decnow@tutanota.com
dexterxanax@criptext.com	tran9ino00@protonmail.com	anoniran@protonmail.com
miiracle11@yandex.com	falcon9@cyberfear.com	lockirswsuppurt@mailfence。 com
rain_man13@keemail.me	loki.help@mailfence.com	payfordecrypting@gmail。com

payfordecrypting@outlook.com	loki.help@bingzone.net	roxlock@mailfence.com
rain.man13@mailfence.com	decoder@firemail.cc	helpingdecode@tutanota.com
lockteam@keemail.me	rdecrypt@ mailfence.com	lockteam@cock.li
sapphire01@keemail.me	sapphire02@mailfence.com	darksoul@safeswiss.com
prodecryptor@yandex.com	mary2005@onionmail.org	mary2005@mailfence.com
payfordecryption@gmail。 com	payfordecryption@outlook.com	xmaster22@tutanota.com
xmagic22@tutanota.com	helprecoverdata@aol.com	rrdata@aol.com
recovertwilightdata@gmail.com	payfordecryption@gmail.com	recovertwilightdata@ gmail.com

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，数据泄露进一步升级。以下是本月通过数据泄露获利的勒索软件家族情况统计，数据仅包含未在第一时间缴纳赎金或拒缴纳赎金的企业和个人（已经支付赎金的企业或个人，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。尚未发现数据存在泄露风险的企业或个人也请第一时间自查，做好数据已被泄露的准备，及时采取补救措施。

本月总共有 336 个组织/企业遭遇勒索攻击，其中有 6 个中国组织/企业在本月遭遇了双重勒索/多重勒索。由于有 24 个组织/企业未被标明，因此未被列入以下表格中。

100X	SIIX Corporation	Roseman University
CMC Group	Sherman Consulting Services	KMC Savills

Colvillbanks	logicalsolutions.bc.ca	conver-pack.com
ourrelentlesschurch.com	Our Sunday Visitor	McDermott International, Ltd
Albany ENT & Allergy Services	TRUSSWAY	Vending Group
p-and-r.com	LASOTEL.FR	TAMMAC
BLUME	AUTOCAM MEDICAL	DATA MODUL
KLINE-SPECTER	GC-EMPLOYMENT.COM	Anton Paar
hwlebsworth	restorationmanagement	La Red Health Center
mastercorp	COACHCOMM	DiJones Real Estate
Gates Corporation	multimedica.it	ArcWear
e-Hazard	accesscontrolsecurity.com	bg2i.fr
Tranztec Solutions	OMT Officine Meccaniche Torino S.p.A.	cdcbmestihl.com
fsdc.org.hk	silbon.es	Fundação Carlos Chagas
Bevan Group	GTT	Agensi Kaunseling dan Pengurusan Kredit
BERNINA International AG	Transformative Healthcare	CANTALK
ptow.com	sunnydesigns.com	peachtree-medical.com
lhh.com.my	atlanticeye.net	imanor.gov.ma
Dacotah Paper	fabeckarchitectes.lu	ddmontaza.hr
summerweine.at	ewwanfried.de	vcclawservices.com
keystonesmiles.org	Bilstein GmbH	GROUPE ETIC
revvaviation.com	Magnolia Care Center	ultimateimageprinting.com
Encompass Group	goforcloud.com	gruponutresa.com
nagase.co.jp	abro.se	Lifeline Vascular Access
Winona Powder Coating	TransMedics	baffetmateriaux.fr
midipapierspeints.fr	Bentham & Holroyd Ltd	kse.org.kw
tiger.jp	yateemgroup.com	gpglobal.com
apolloscientific.co.uk	esinsa.com	bigc.co.th
fullertonindia.com	Lake Dallas Independent School District	MW Components
Clarke County Hospital	norton.com.ar	NETISGROUP
ECCI	WestcoastSmile Dental Studio	MKU
qcssinc.com	Easy Automation	floraalpina.ch
Pembina County Memorial Hospital	Groupe Gambetta	UECC
stuertz.com	Neptune Lines	Yellow Pages
GKS Hydraulik	Daregal	Groupe ACTIVA
Slade Shipping	Saville Row	AUT-TECH-GROUP.COM
Classic Stripes Pvt	Global Polymers	NAIVAS
Astarc Group	VOPAK	Albert Ziegler
Cementos Progreso	Wynn-Reeth	Banco Comercial do Huambo
Eastern Cape Gambling Board	Lisa Logística	JK Residential Services
CA de Seguros La Occidental	sasa.com	pkffinconta.ro
soapro.ao	soshin.co.jp	ibp.com.br
tubosreunidosgroup.com	Insurance Agency Marketing Services	Laragh Courseware

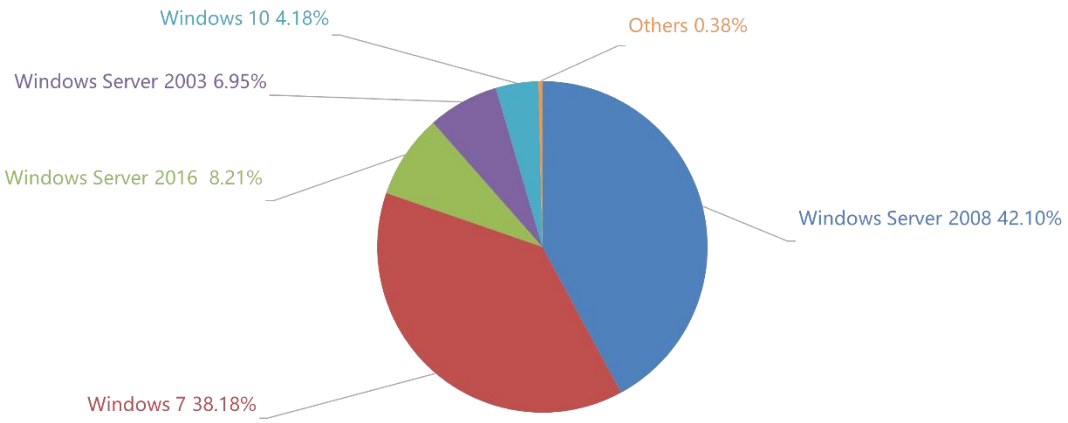
The Shively Bros	Corporate Technologies	Corizon Healthcare
M**** ****	Toho Tenax America	Sonda
Sunstar Americas	Hawaii self storage	Urban Import
Export Hub	intuview.com	crossinggroup.com
5Design	Steve Silver furniture	Precision Fabrics Group
Mutual de Seguros de Chile	Goldenbear.com	Biman airlines
Aero Engine Solution INC	mjhallandcompany.com	Lpa-group.com
Gaston College	jaco.com	gizavc.com
garrotbros.com	The Spooner Risk Control	DOREL Industries
Berlin Packaging	bancodevenezuela.com	sommer.eu
sbhc.us	7G Distributing	Huissiers
Coldiretti	Bang IT Solutions	Corrib Oil
Structab AB (MegTax)	Mainstream Engineering	City of Ballwin
gentex.com	Western Digital	MEADE TRACTOR
Esperanza Viva Jóvenes de México	Gulliver International	Saobacdau Technologies Group
Ozarks Community Hospital	Lakeland Community College	Unique Imaging
thesoftwareconsultinggroup.com	Amouage	Winter Park Construction
Office Notarial de Baillargues	Albany Clinic	McKinney Trailers
hkiff.org.hk	Pharm-Pacc Corporation	pinelandschool.org
joriszorg.nl	SPARTAN Light Metal Products Inc	validcertificadora.com.br
brl.fr	alpine4u.com	Uniondale School District
Swanson Group	Moon Capital	Talon Outdoor
Dataram	Leadway Assurance Company Limited	CommScope
Aloha Enteprise [NCR]	Allimand, France	osg.co.jp
knvb.nl	ktbs.com	homeandhearthealth.com
fameline.com	steel-eye.com	sanden.com.ph
piszcz.pl	Yucatan	SAFHOLLAND
Invenergy	Aerowind	Capstan Atlantic
Faps	Southeastern University	Tennessee State University
Encompass Technologies	IDEXX	Retina and Vitreous of Texas
VMedia Inc	SunPower Marine	GIGATRON.RS
fsmsolicitors.co.uk	Attent Zorg en Behandeling	Sippex
teleferico.com	apro.cl	bcncruiseport.com
fosfa.cz	CH Media	einhaus-gruppe
Petaluma Health Center	Medicalodges, Inc	David S. Brown Enterprises
PESA Bydgoszcz	servex-us.com	conseildelentente.org
irda.com.my	comacchio.com	robovic.com
medmark.eg	uhloans.com	cezam.net
grouplease.co.th	Nobiskrug Yachts GmbH	Flensburger Schiffbau Gesellschaft mbH & Co.
Smith Industries	manfil.com.br	Crown Grinding & Machining
Cementos Bio-Bio	City of Collegedale	Creation Baumann
valleywomenshealth	arcc.org	Incredible Technologies

Stanley Electric U.S.	Harvard Energy	bsw-architects.com
Nature Path Foods	disltd.ca	artri.net
euromotors.com.pe	agp.ph	gregoire.fr
fiamma.com.my	Big Ass Fans	Alvaria
Tom Duffy Company	mundocuervo.com	aek.mk
don-PC	DESKTOP-8CASIND	desktopforcool123
Scantibodies Laboratory, Inc.	Palo Alto County Sheriff	PKF Antares
Legion Aero	Vleeswarenfabriek Jac Michiels	Schirm
baysideinteriors.com	DCI-ENGINEERS	The Zalkin Law Firm P.C.
BrightSpring Health Services	Pharmerica.com	coremain
SIVSA	sxi.com.ph	baughmanco.com
HEICO	b&h pattern.inc	Raymond Storage Concepts
Atlantic International University	Beghelli USA	Kretek International
Americana Restaurants	bhrcorp.org	HIGHLANDHOMES
Officeworks Inc	Meriton	Quad-County Ready Mix
Ruekert & Mielke	Arandell Corp	Open University of Cyprus
quilts,inc	nautic.com	Micro Star International
PALM HILLS DEVELOPMENT	nestseekers.com	UnitedLex
Noteboom	Hull Property Group	turncommerce.com
The Sage Next	tf-amd.com.my	tf-amd.com
Tarolli, Sundheim, Covell & Tummino LLP	Joy Cone Co, Joy Baking group, BoDeans Baking, Altesa	NGS Super
Intrasect Technologies	Moore Engineering	olympia.org
Etex Communications	Kelly Group	tvh.com
masrl.com	omscomponents.it	Electronic SYSTEMS S.p.A.
Dalumi Group	garrottbros.com	HUSKY
TWHOUSE	METALWORK	OCEAN
TREENOVUM	ARCHI+	SAGE
Guess who!	vernegroup.com	thened.com
Cameron Memorial Community Hospital	errebielle.it	midamericanglass.com

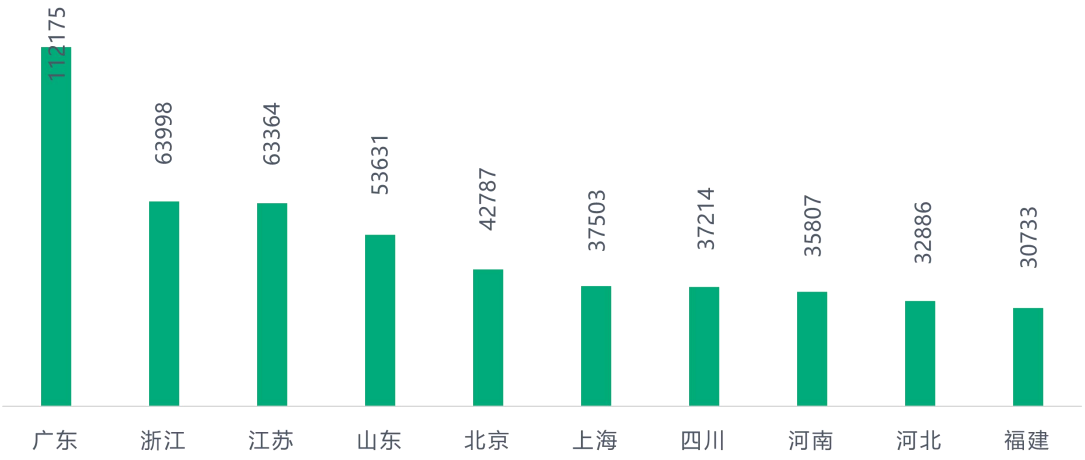
表格 2. 受害组织/企业

系统安全防护数据分析

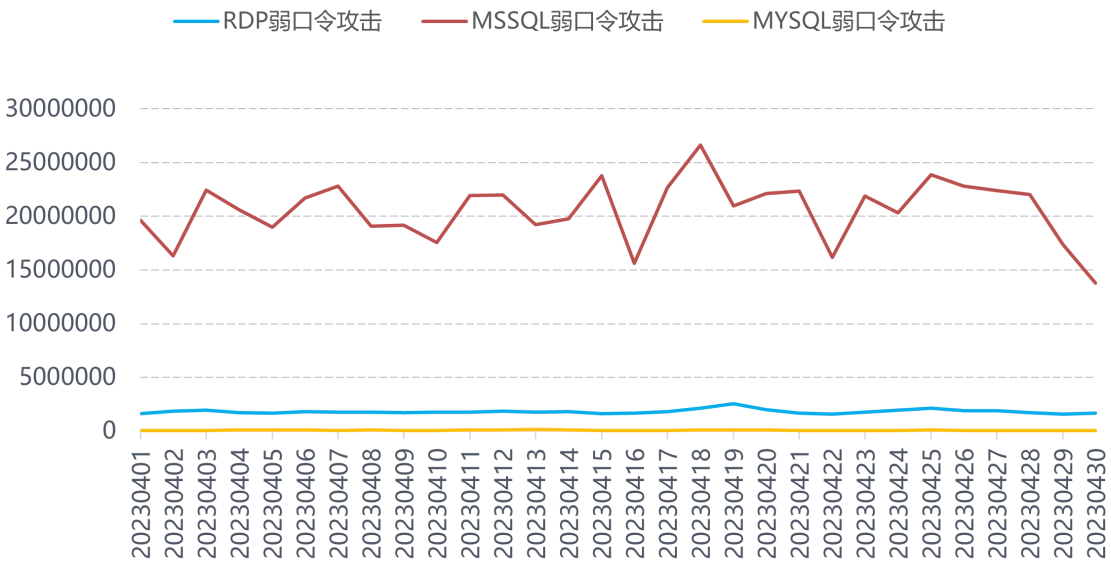
360 系统安全产品已新增黑客入侵防护功能。在本月被攻击的系统版本中，排行前三的依次为 Windows Server 2008、Windows 7 以及 Windows Server 2016。



通过对 2023 年 4 月被攻击系统所属地域的统计发现，数字经济发达地区仍是攻击的主要对象，与之前几个月的情况相比，变化并不大。。



通过观察 2023 年 4 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。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，本月新发现还可以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。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和 SQLGlobeImposter 渠道进行传播。此外 360 安全大脑监控到该家族曾通过匿影僵尸网络进行传播。

- 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。

- malox：同 mallox。

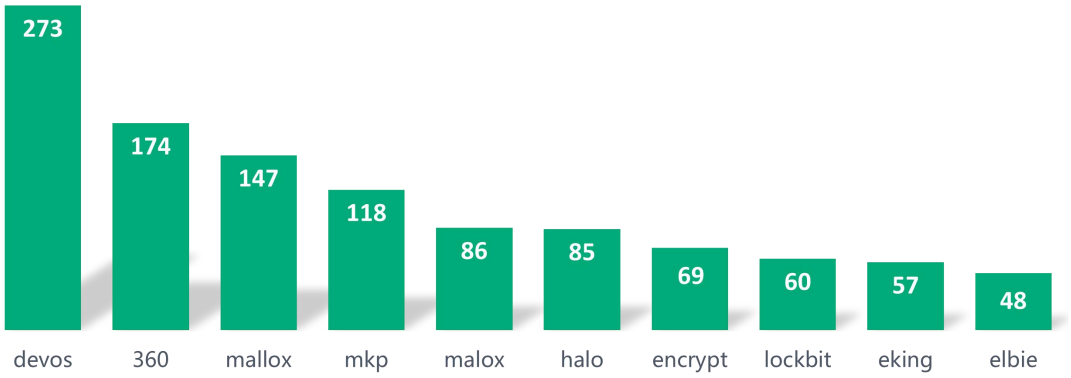
- halo：同 360。

- encrypt：该后缀虽被多个勒索软件家族使用，但在本月活跃的仅有 eCh0Raix 勒索软件家族，因被加密文件后缀会被修改为.encrypt 后而成为关键词，该勒索软件家族还可以利用桌面弱口令和漏洞对 NAS 设备发起针对性攻击。

- 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。

- eking：phobos 勒索软件家族，因被加密文件后缀会被修改为 eking 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 eking。




360数字安全
数 字 安 全 的 领 导 者