2022 年 9 月勒索软件态势分析

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 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。

2022 年 8 月，全球新增的活跃勒索软件家族有：Ballacks、BlackBit、DoyUK、Royal、z6wkg、Sparta 等家族。其中 z6wkg 与 Sparta 均为双重勒索勒索软件家族；Ballacks 勒索软件是 VoidCrypt 勒索软件家族的最新变种；Royal 勒索软件虽然声称采用双重勒索模式运营，但尚未发现其拥有数据泄露站点，该家族是一个不招募附属机构的独立运作团体，通常勒索赎金价格在 25 万美元到 200 万美元之间。

以下是本月最值得关注热点：

一、Lockbit 勒索软件编译器遭“愤怒的开发者”在线泄露

二、MSSQL 服务器被 TargetCompany 勒索软件攻陷

三、Cisco 确认阎罗王勒索软件泄露了其被盗的公司数据

基于对 360 反勒索数据的分析研判，360 政企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

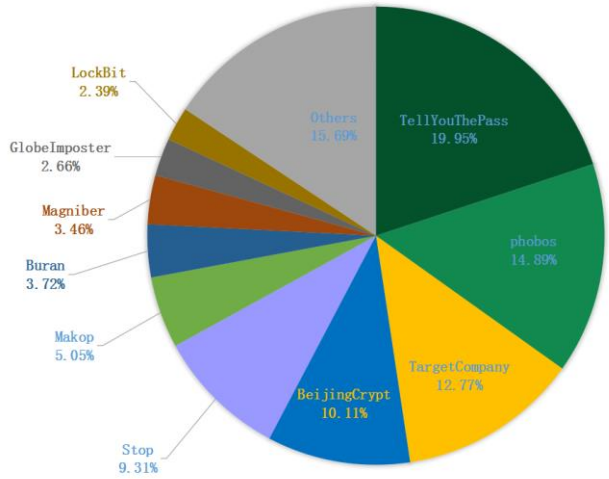
针对本月勒索软件受害者所中勒索软件家族进行统计，TellYouThePass 家族占比 19.95%居首位，其次是占比 14.89%的 phobos，TargetCompany(Mallox)家族以 12.77%位居第三。

TellYouThePass 虽然在本月没有继续大规模发起攻击，但是之前的中招反馈仍持续一段时间。

Phobos 做为国内老牌勒索家族，流行热度一直比较高，主要通过暴破远程桌面传播。

LockBit 勒索软件因招募大量附属机构，因此其攻击目标广泛，在国内不止针对中大型企业发起双重勒索攻击，还会对小型企业发起纯勒索攻击。

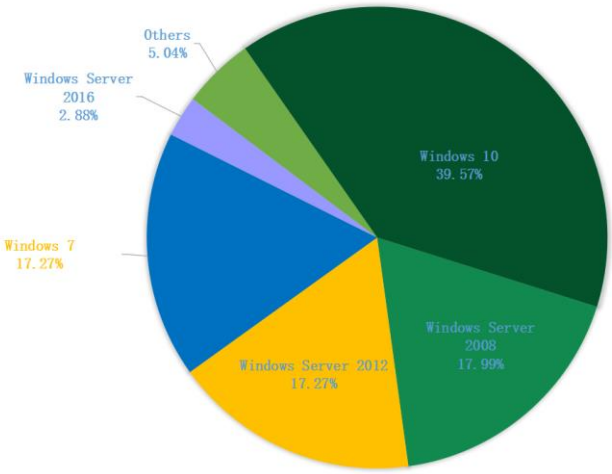
2022年9月反勒索服务处置勒索病毒家族占比



数据来源：360反勒索服务

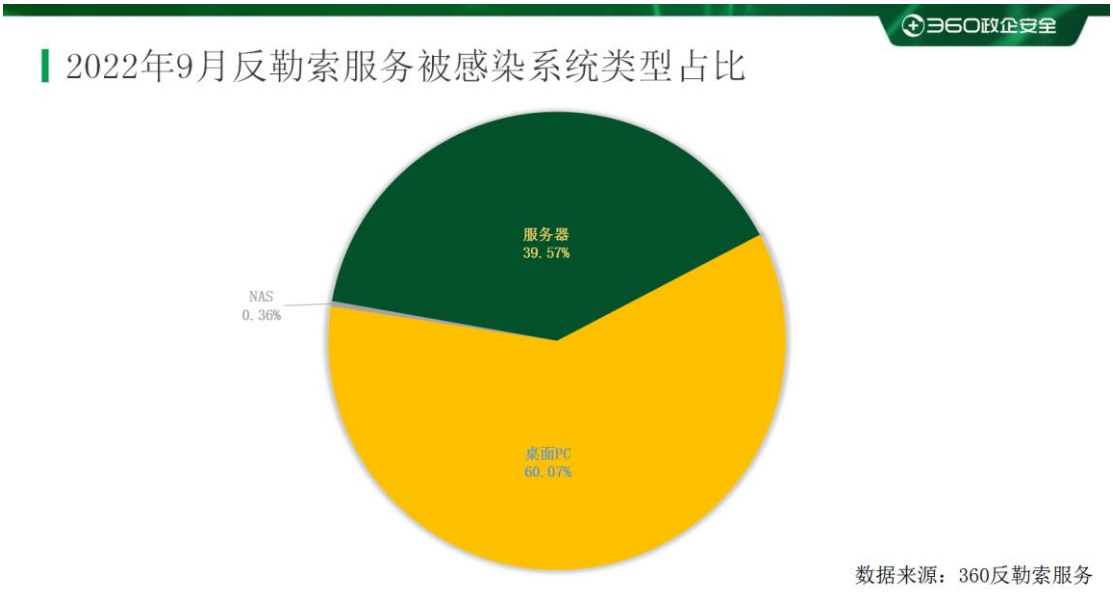
对本月受害者所使用的操作系统进行统计，位居前三的是：Windows 10、Windows Server 2008 以及 Windows Server 2012。

2022年9月受勒索病毒影响操作系统占比



数据来源：360反勒索服务

2022 年 9 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。



勒索软件疫情分析

Lockbit 勒索软件编译器遭“愤怒的开发者”在线泄露

LockBit 勒索软件遭到破坏，据称该团伙最新生成被心怀不满的内部开发人员泄露了。

今年 6 月，LockBit 勒索软件发布了他们的 3.0 版加密器，代号为 LockBit Black，目前已经经过了两个月的测试。

而该版本勒索加密器则承诺“让勒索软件再次伟大”。其中添加新的反分析功能、勒索软件漏洞赏金计划和新的勒索方法。

然而，目前有两个 Twitter 账号在 Twitter 上泄露了 LockBit 3.0 主程序的生成器。据称，泄密者是 Lockbit 勒索软件小组雇用的程序员，他们对 Lockbit 的领导层感到不满，于是决定泄露了该程序的生成器。

MSSQL 服务器被 TargetCompany 勒索软件攻陷

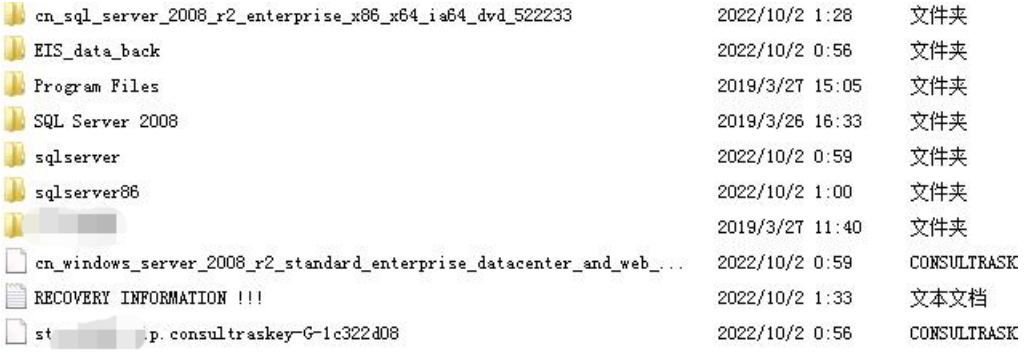
研究人员称，在新一波 TargetCompany(Mallox)勒索软件攻击中，易受攻击的 Microsoft SQL 服务器正成为攻击目标。

安全研究人员表示，TargetCompany(Mallox)是目前主流的勒索软件之一，该家族过去被称为“Mallox”，着是由于被其加密的文件会被添加“.Mallox”作为新扩展名而得名。此外，该勒索软件也可能与二月份发现的“TargetCompany”勒索软件同族。

勒索软件感染始于被攻击机器上的 MS-SQL 主程序通过 cmd.exe 和 powershell.exe 命令行来下载.NET 文件。这让攻击者可以利用有效载荷获取其他恶意软件（包括加密器），生成并运行终止特定进程和服务的 BAT 文件。

接下来，勒索软件载荷将自己注入 AppLaunch.exe——一个合法的 Windows 进程中，并尝试删除名为 Raccine 的开源勒索软件免疫注册表项。

此外，恶意软件会停用数据库恢复功能并终止数据库相关进程，使其内容可用于加密。

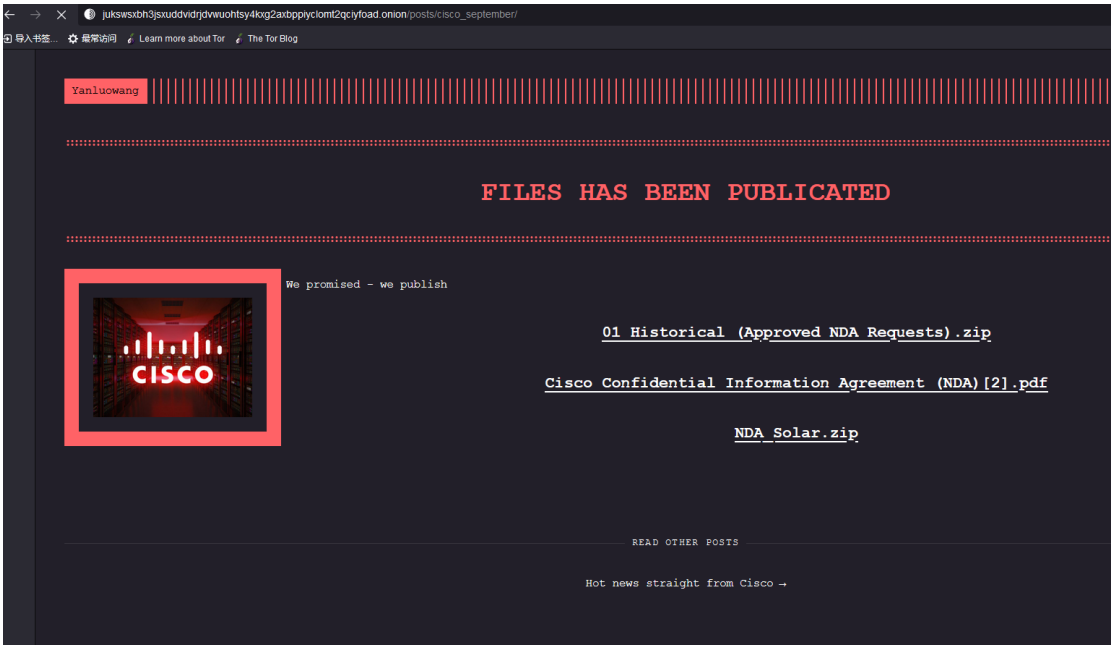


Cisco 确认阎罗王勒索软件泄露了其被盗的公司数据

Cisco 已证实，“阎罗王”勒索软件团伙昨天泄露的数据是其在 5 月的网络攻击中从该公司网络窃取的。但 Cisco 同时表示，泄漏不会改变该事件对业务没有影响的初步评估。

此前，在八月份的一份报告中，Cisco 曾承认黑客入侵了其一名员工的 VPN 帐户后导致其网络被“阎罗王”勒索软件破坏。但被盗数据均为来自员工 Box 文件夹的非敏感文件，并且在“阎罗王”勒索软件开始加密系统之前就已经遏制了攻击。

而“阎罗王”勒索软件方面则声称并非如此——但并没有提供任何明确的证据，只分享了一个屏幕截图来表现其对似乎是开发系统的平台具有访问权限。



黑客信息披露

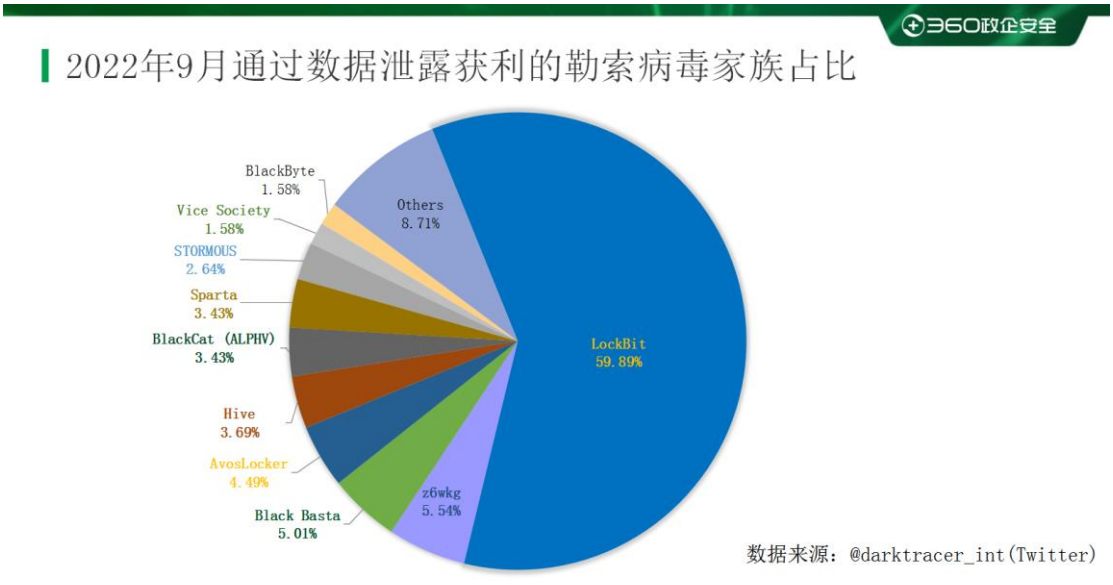
以下是本月收集到的黑客邮箱信息：

vyndinostrov@morke.org	vyndinostrov@cock.li	consul.raskey@onioinmail.org
service@hellokittycat.online	dateshell@protonmail.com	trueman@cock.li
jack.stress@keemail.me	Writemel00@tuta.io	khgurwte@tutanota.com
regyhny@tutanota.com	LordCracker2@aol.com	KingMail7@cock.li
dateshell@protonmail.com	datarestorehelp@airmail.cc	support@bestyourmail.ch
dino@rape.lol	comingback2022@cock.li	newfact@rape.lol
regyhny@tutanota.com	khgurwte@tutanota.com	poshix@tfwno.gf
Ez.decrypt@msgsafe.io	samercin1@tuta.io	KalajaTomorr@ctemplar.com
KalajaTomorr@firemail.cc	vyndinostrov@cock.li	vyndinostrov@morke.org
helprecovery@gnu.gr	kedrovak@tfwno.gf	lemordewn@gmail.com
helprecovery@gnu.gr	rdpmanager@onionmail.org	RandyJackson1961@gmx.com
pcrec@tuta.io	perettosup@proton.me	qui_medicus@aol.com

hero77@cock.li	deportdgrrg@outlook.com	finibutrile@tutanota.com
mssqlppt@tutanota.com	08don_juan_1970689@mail.ru	pplit@protonmail.com
decryptydata@gmx.net	zdarovachel@gmx.at	cyberlock06@protonmail.com
biggylockerteam@yandex.com	AstraRansomware@protonmail.com	ramilo2122@yandex.com
chinadecrypt@msgsafe.io	decryptydata@gmx.de	decryptydata2@gmx.net
lettoindago@tutanota.com	dataabcdof@tutanota.com	idemitsu122@cyberfear.com
helprequest@techmail.info	internationalassistance@tutanota.com	reasonablehelp@outlook.com
uncrypt2022@outlook.com	sendr@onionmail.org	sendr@tutanota.com
itsupport831@reddithub.com	support007@mailfence.com	help@inboxhub.net
cang.leen@mailfence.com	carbonayra@mailfence.com	recoverservice2@onionmail.org
alabacoman@tutanota.com	alberttconner2021@protonmail.com	AndryCooper1988@tutanota.com
CharlesSLewis1987@onionmail.org	DavidSchmidt1977@protonmail.com	DorothyFBrennan1992@tutanota.com
dwaynehogan33@onionmail.org	ElizabethAntone1961@protonmail.com	EndryuRidus@tutanota.com
fionahammers1995@onionmail.org	JamesHoopkins1988@onionmail.org	jasonchow30@onionmail.org
JerseySmith1986@onionmail.org	Kirklord1967@tutanota.com	leonardred1989@protonmail.com
Leslydown1988@tutanota.com	leticiaparkinson1983@onionmail.org	MarkHuntigton1977@tutanota.com
Mikedillov1986@onionmail.org	noreywaterson1988@protonmail.com	ollivergreen1977@protonmail.com
richardbrunson1892@protonmail.com	rickysmithson1975@protonmail.com	VinceGilbert@tutanota.com
recoverservice3@onionmail.org	skynetwork@cock.li	skynetwork@onionmail.org
skynetwork@tutanota.com	anigma@cock.li	anigma@tutanota.de

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 379 个组织/企业遭遇勒索攻击，其中包含中国 14 个组织/企业在本月遭遇了双重勒索/多重勒索。

seaviewresortkhaolak.com	kimed.pl	hriindia.com
aidsalabama.org	Mansfield Independent School District (MISD)	toyotaalabang.com.ph
Tanzania Telecommunications Company	Bay Crane	Deerberg
Los Angeles Unified School District	Abdullah Al-Othaim Markets	Rick Shipman Construction
Stages Pediatric Care	bew.co.th	samyang.com
Karl Gemünden GmbH & Co. KG	Health Care Solutions Group	Evo exhibits
DLS Motors	Cosmopoint College	Southwell, Inc.
hdhopwood.com	vitalityhp.net	Ministerio de Relaciones Exteriores
TAKAO-UK	GFG	TSMTU
JANMARINI	Hendry Regional Medical Center	Ginspectionservices
Etna GmbH	Associated Bag	melorita.com
Nihonsakari Co. , Ltd	yehu.org	multicareinc.com
bliss-d.com	STADLER	AES Clean Technology
Samuel Ryder Academy	KOLLITSCH	mdmprint.ru
smartschoiceit.com	croninfotek.com	rakinformatics.com
Control	SolarCraft	Hughes Systems Industrial
ifwglobal.com	uide.edu.ec	yourprivateitaly.com
webnordeste.com.br	idtech.com.tw	scrd.ca
thorguard.com	congerbuilt.com	rbroof.com
parrottsims.com	Cornerstone Insurance Group	Longhorn Investments
GSE - Gestore Servizi Energetici	Boyes Turner LLP	GRUPO COPISA
School of Oriental African Studies	Ministerio de Economía Argentina	www.bbadmin.com
BHARBERT	atlantisholidays	archimages inc
ALTITUDE AEROSPACE INC	Fonderia Boccacci	Zelena Laguna Hotel
LEGAZPIBANK	MCCLEAN16	lawtrade
Autosoft company	BIOPLAN	Dyatech
DGLEGAL	emscrm	MIDAS
AURIS KONINKLIJKE AURIS GROEP	fidelityunited.ae	goldcreekfoods
exheat.com	hwrpc.com	Salmon Software
tristatefabricators_inc	Admiral Merchants	Foreman Watson Land Title, LLC.
Mainstream Global Inc.	CORNERSTONE	Sierra College
Sigmund Software	elementnor.no	CARITAS
okibrasil.com	ducanh.com	psi.com.tw
mts.mektec.com	franckbeun.fr	Carmen Copper Corporation
Zeus Scientific Inc	New York Racing Association	hering-heinz.de
South Pacific Inc	Biggest News	TOR VERGATA
Laddawn Inc.	software-line.it	equatortrustees.com
scottobrothers.com	kaffeeberlin.com	ces-conditionneur.fr

American International Industry	HT Ports Services Pte Ltd (HTPS)	Emtec Inc
asecna.org	County Suffolk and contractors	midlandplastics.com
dss-cz.com	Bell Technical Solutions	Nextlabs
nakamuracorp.co.jp	FONTAINEBLEAU	Tri-Supply
Triten	aliat.group	medical69.com
d-securite.com	southamptoncounty.org	Northwest University
cnachile.cl	independence.com.co	makler.com.ve
markherder.com	inspecshawaii.com	DYNAM JAPAN HOLDINGS CO., LTD
MR. WONDERFUL	AUTO88	quintal.com.co
cityofbartlett.org	aipcenergy.com	kcgreenholdings.com
maisonloisy.fr	maleosante.fr	mj-donnais.fr
pays-colombey-sudtoulois.fr	sarassure.fr	sva-avignon.concession-landrover.fr
ville-faulquemont.fr	cultivar.net	camdomain.com
kwp.at	artdis.fr	cmb-artimmo.com
daune.org	euro-modules.fr	euromip.fr
jt-engineering.com	lagence33.com	idealtridon.com
taxprepandmore.com	mackenzie-law.co.uk	thezincgroup.com
Daydream Island Resort & Spa	bakkerheftrucks.com	groupg4.com
Font Packaging	Ferrer&Ojeda	Tema Litoclean Group
Grupo Galilea	Fundació Sant Francesc d'Assís	INDIBA
RIVISA	RABAT	COMSA CORPORATION
SERCOM	ORDEREXPRESS.COM.MX	LOESCHGROUP.DE
PCSupport	Fiveninefive	Elmbrook Schools
The Checker Transportation Group	Hayat	OakBend Medical
omegaservices.com.au	frigobandeira.com	ch-sf.fr
Our Lady of Lake University	Paul Smiths College	hamiota.com
aralaw.cr	canadiansolar.com	TIB Development Bank
Davin Industries Ltd	Xybion	Ipca Laboratories
connectvitypoint.com	marugokiso.co.jp	lacalera.pe
kisan.com.tr	diakonissen-riehen.ch	kortrijkserijschool.be
Ministry of National Education	UVT	Phu Hung
BND	midway	Stratford University
MGSMFG	EMEPLATING	STEVENG
SHI	marcopolohotels.com	hunters.com
California-Oregon Telecommunications Company	TeladanPrima Argo Group	Sunland Asphalt And Construction
crownuniform.com	metaage.com.tw	misumi.com.tw
gavresorts.com.br	lafondasantafe.com	tapcocu.org
monnensenpartners.be	pdh.com.tw	sbr-zwiesel.de
finnco.eu	ADTRANSPORT	cleantech
sportscity.com.tw	VANICREAM	kamut.com
www3.comune.gorizia.it	divultec.pt	comune-italia.it

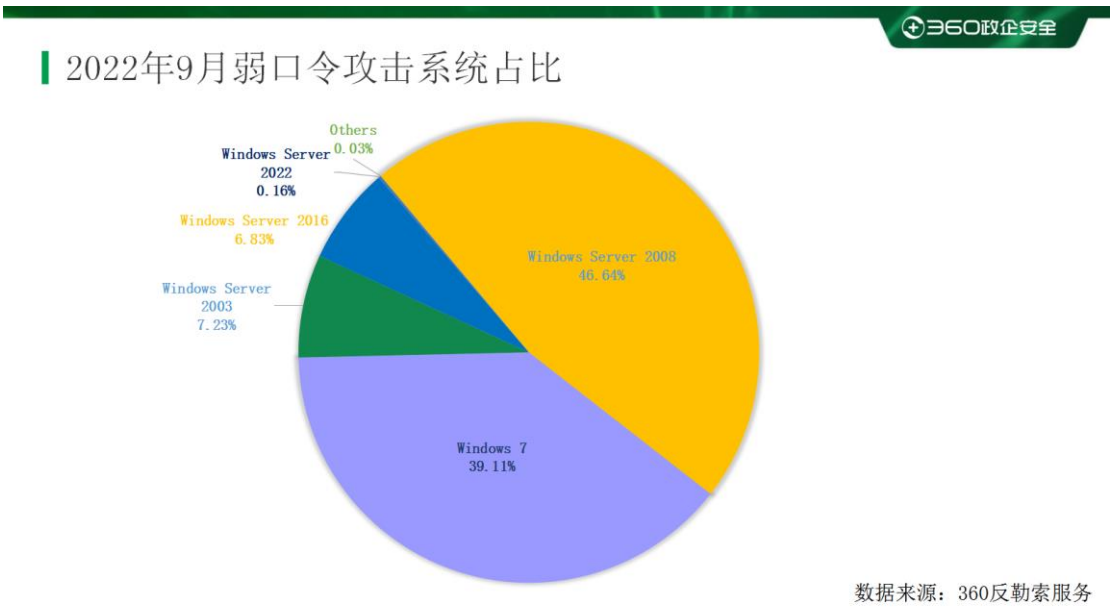
eneva.com.br	Truckslogic	peakinternational.com
hmets.com	floresfunza.com	Speed-Buster
Baer's	Infinitely Virtual	Transform Data Into Insight
The Brigantine	SCAD EDU	Fundo Nacional de Desenvolvimento da Educação
Eurocell	zgoda.ad	zentrumdreilinden.ch
ymcawashdc.org	wsretailers.com	worldnetlogistics.com
workcrossing.it	wolfbergalvarez.corp	whse.iibg.ca
vvrmc.org	unified-it.com	tojin.com.tw
terminal.com	teleprocorp.com.mx	stocker.ora
standard-furniture.ba	stairs.rintal.com	spherechina.com
soenen-golfkarton.lan	smjcorp.net	smd.shimamura.gr.jp
sheraton.marriott.com	sefnet.rj	securedoffers.com
sbc.com	salumificiovenegoni.it	roteritaly.com
rosslare.com.hk2	roma.enit	reust.ads
ptilhk.com	prefimetal.int	prairie.prairiesedgecasino.com
poultry.loc	plumascounty.countyofplumas.com	orchestra.net
optimissa.into	opt.com	office.athesis.org
nwtf-ho.org	northernins.ca	mypolyplastics.com
murrays.cheese.com	ms-hosted-tse.priv	moci.int
mkbrokers.fin	mfidallas.com	meritservices.org
medman.com	malle.clozdloop.com	logistia.net
litto.lan	lapostermobile.fr	knx.lan
kmalawfirm.com	jps.cr	janspec.com
it-root.com	ismea.int	intranet.hoffsuemmer.de
intern.liceubarcelona.com	ikkgroup.com	ifis.com.sg
hxlife.com	hsvgroup.com.vn	hotelluzeiros.fla.br
honsha.hanshin-dp.co.jp	holding.loc	hlc.bike
hkdml.wik	hinaka.corp	gruppoathesis.it
gruges.com.mx	gov.oak-brook.org	gla.net
giovanardi.it	genpl.com	fusesandliberty.com
fupite.com.tw	fsd.com	focusadventure.com
fmc.ar	etggs.net	equisfg.efg
edtec.biz	edgoldner.com	dsoler.soler.com
domain.itsoft.com	dmn-vitalprev.net	dgimali.org
danubius-exim.ro	crich.loc	coteg-toulouse.dom
corp.kuwaitairways.com	corp.keypoint.net	corp.fehrs.com
comune.crispiano.ta.it	codisel.com.mx	cobbengr.com
christianvillage.org	cheyenne.k12.ok.us	ceratube.net
cepi.int	cczstattonequities.com	castro.net
cachibi.com.co	bredinprat.fr	bredinprat.com
boxmarche.it	billycraiginsurance.com	bbst.clp

barcelona.jbc.es	auras.com.tw	ats.lab
arcelor-sztg.hu	alhajery.com.kw	alaliengineering.net
ah-babelsberg.net	ad.jamailconstruction.com	ad.bennetts.com.au
Instituto Agrario Dominicano	Moon Area School District	Avante Ultrasound
An Japan Game Halls Operator	Moscone Center	Monarch
Alan Smith Pools	Midea Group	GHT CORP
hspatent.com		

表格 2. 受害组织/企业

系统安全防护数据分析

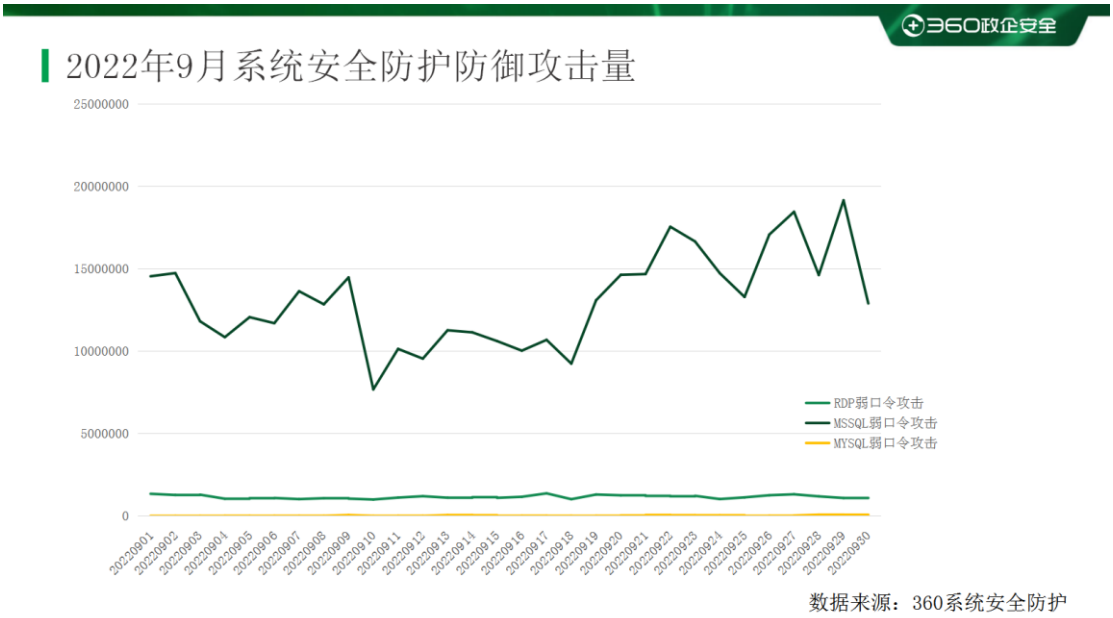
360 系统安全产品，针对服务器进行全量下发系系统安全防护功能，针对非服务器版本的系统仅在发现被攻击时才下发防护。在本月被攻击的系统版本中，排行前三的依次为 Windows Server 2008 、Windows 7 以及 Windows Server 2003。



对 2022 年 9 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。

数据来源：360系统安全防护

通过观察 2022 年 9 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。



数据来源：360系统安全防护

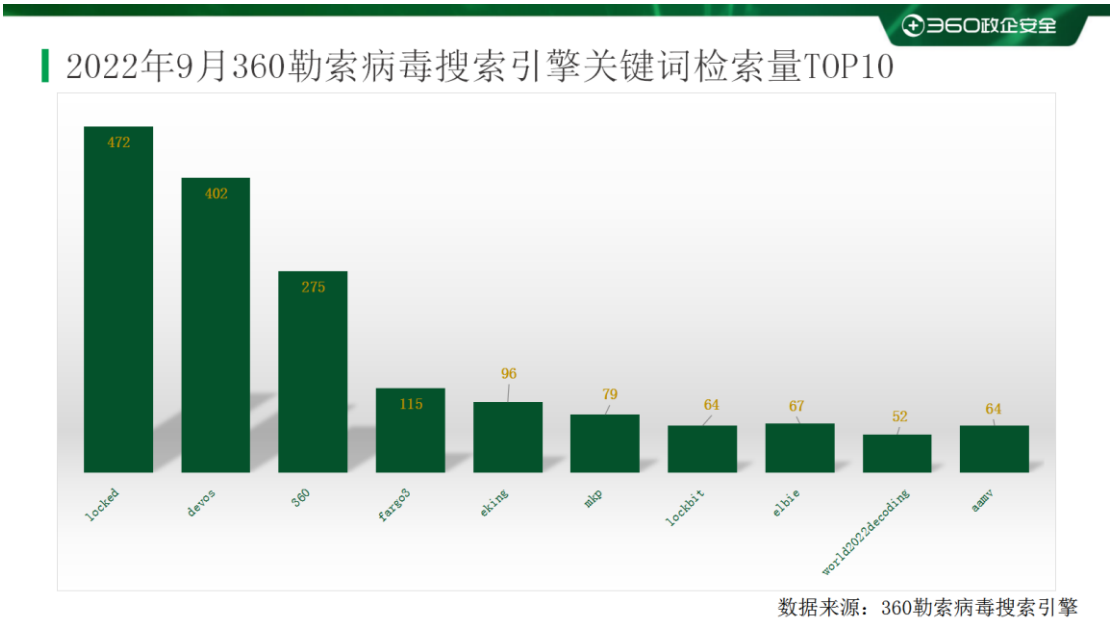
勒索软件关键词

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。

- 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。
- 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。
- fargo3：属于 TargetCompany(Mallox)勒索软件家族，由于被加密文件后缀会被修改为 fargo3。该家族传播渠道有多个，包括匿隐僵尸网络、横向渗透以及数据库弱口令爆破和远程桌面弱口令爆破。
- eking:属于 phobos 勒索软件家族，由于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。
- 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。
- Lockbit:属于 LockBit 勒索软件家族，早期被该家族加密的文件扩展名会被修改为 lockbit,但从 LockBit3.0 版本后,扩展名采用随机字符串,同时其文件名也将被修改。由于 LockBit 家族是一个非常庞大的团伙，招募了大量附属机构， 因此其传播方式通常无固定的渠道，不仅限于远程桌面爆破、数据库弱口令攻击、漏洞利用、钓鱼邮件等均可作为该家族的传播渠道。
- elbie: 同 eking。
- world2022decoding:属于 Honest 勒索软件家族，由于被加密文件后缀会被修改为 world2022decoding 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。
- aamv：属于 Stop 勒索软件家族，由于被加密文件后缀会被修改为 aamv 而成为关键词。该家族主要传播方式为：通过伪装成破解软件或者激活攻击，诱导用户下载运行。

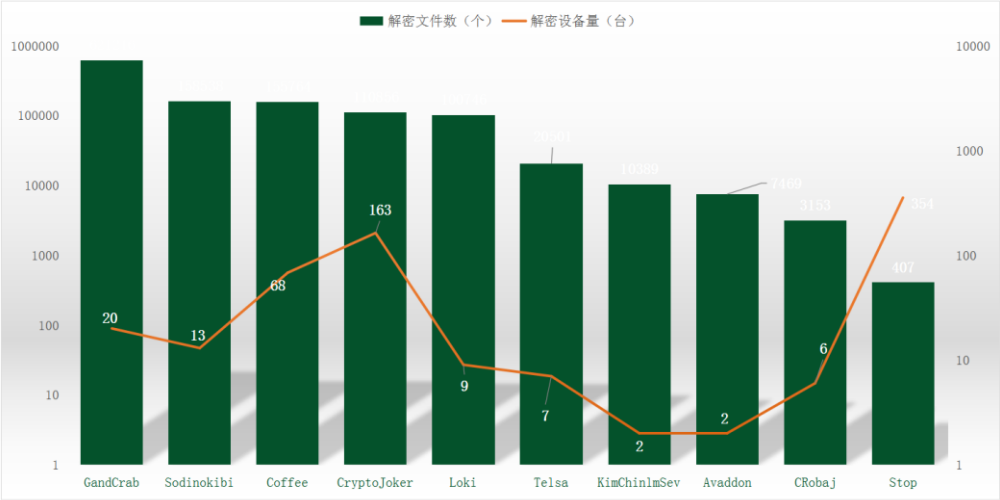


数据来源：360勒索病毒搜索引擎

解密大师

从解密大师本月解密数据看，解密量最大的是 GandCrab，其次是 Sodinokibi。使用解密大师解密文件的用户数量最高的是被 Stop 家族加密的设备，其次是被 CryptoJoker 家族加密的设备。

2022年9月解密大师解密量



数据来源：反勒索服务统计数据