2022 年 3 月勒索病毒态势分析

勒索病毒传播至今，360 反勒索服务已累计接收到上万勒索病毒感染求助。随着新型勒索病毒的快速蔓延，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。勒索病毒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 安全大脑针对勒索病毒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 3 月，全球新增的活跃勒索病毒家族有:FarAttack、Venus、Sojusz、KalajaTomorr、GoodWill、Pandora、AntiWar、IceFire、Acepy 等家族，其中 Pandora 是由双重勒索勒索 Rook 家族演变而来目前已有 4 名受害者。

本月最值得关注的有三个热点：

一、TellYouThePass 近期多次活跃，并新增利用 Spring 漏洞和向日葵漏洞发起攻击

二、双重勒索 Cuba 开始攻击国内用户

三、三星、英伟达、微软等大型企业遭遇 LAPSU$数据勒索团伙攻击，大量数据遭遇泄漏。

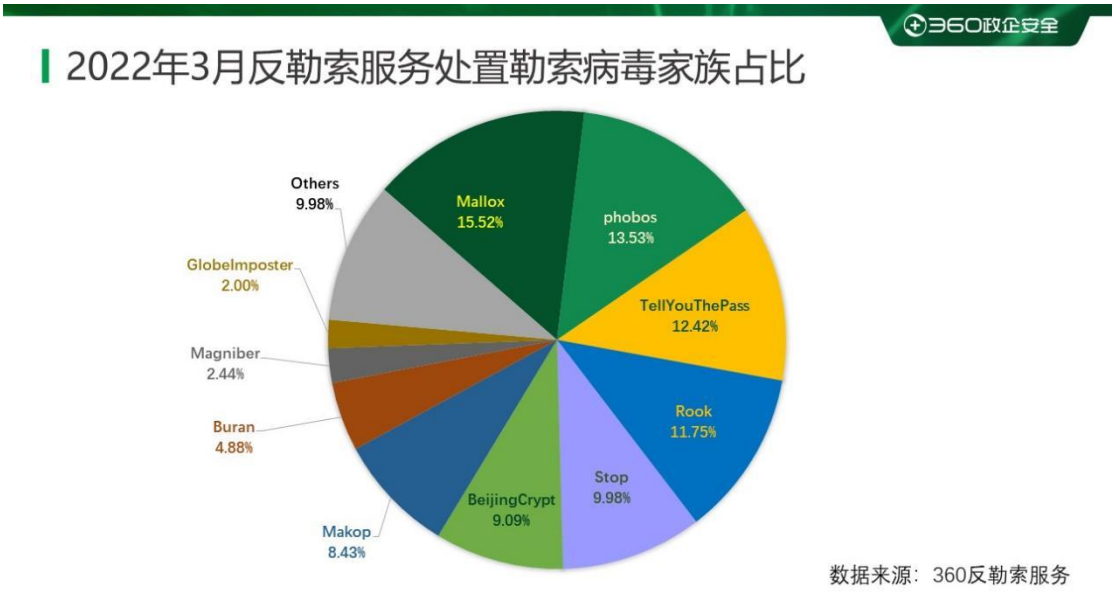
基于对 360 反勒索数据的分析研判，360 政企安全集团高级威胁研究分析中心(CCTGA 勒索软件防范应对工作组成员）发布本报告。

感染数据分析

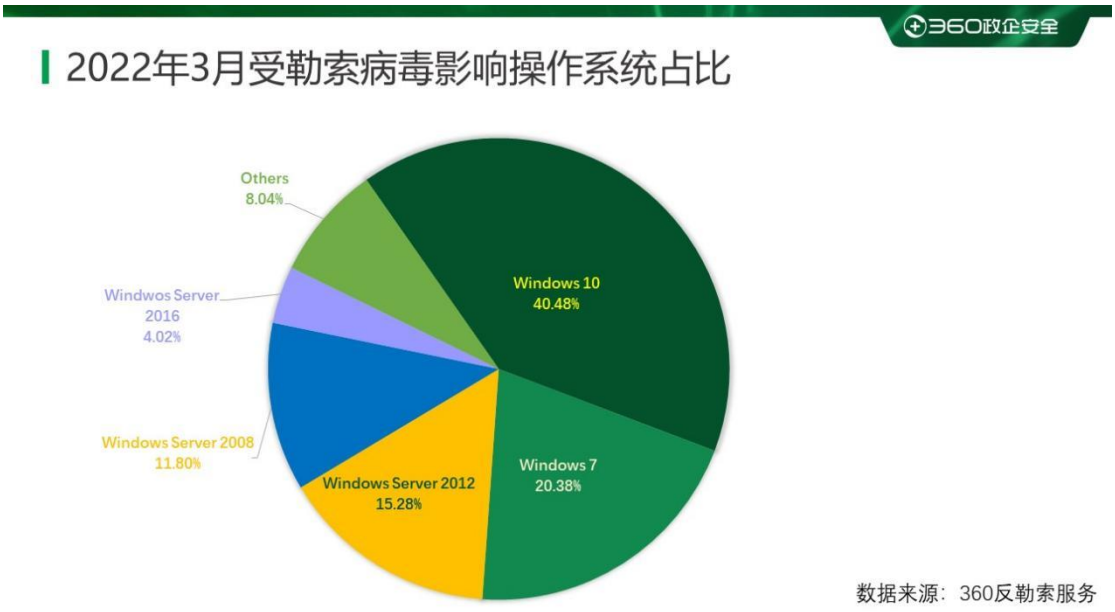
针对本月勒索病毒受害者所中勒索病毒家族进行统计，Mallox(TargetCompany)家族占比 15.52%居首位，其次是占比 13.53%的 phobos，TellYouThePass 家族以 12.42%位居第三。

从 2 月份开始 Mallox(TargetCompany)将内网横向渗透加入到攻击模式中，其感染量开始不断上升，在本月跃升到 TOP 1。

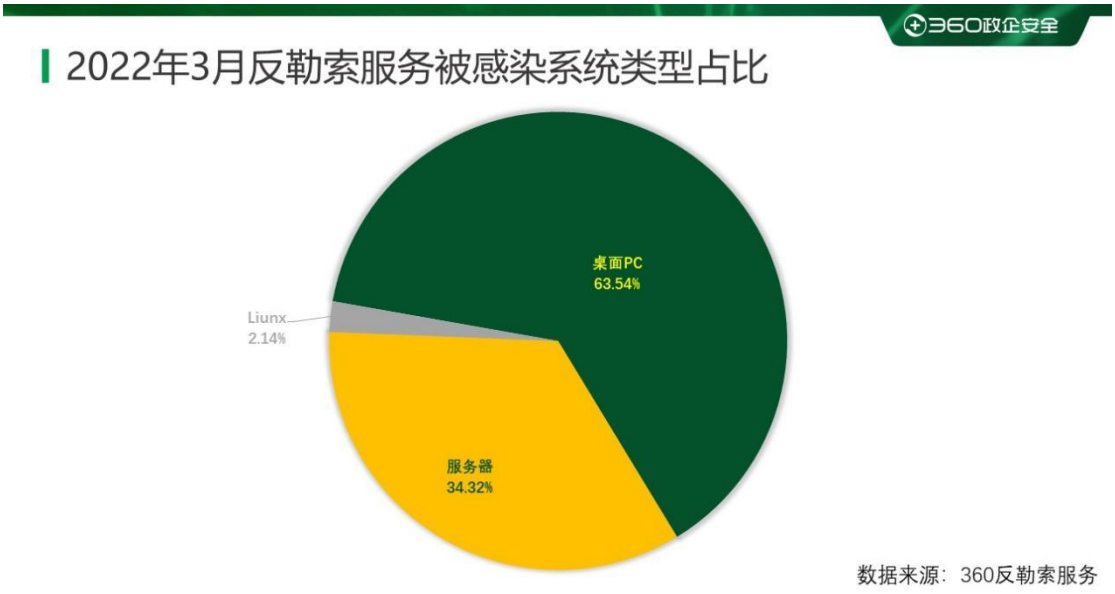
TellYouThePass 家族因本月多次间断性发起攻击，其感染量相比以往也有大幅度的上涨。



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 7、以及 Windows Server 2012。



2022 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。与上个月相比，无较大波动。

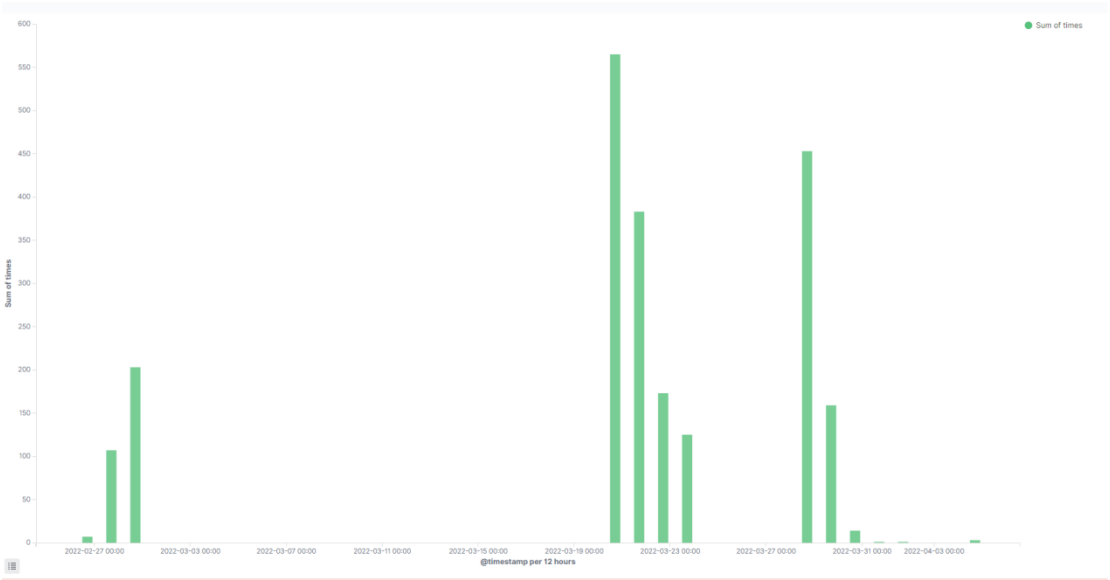


勒索病毒疫情分析

近期多次活跃的 TellYouThePass 勒索病毒家族

360 安全大脑监测到，从 2022 年 2 月底到 3 月，TellYouThePass 间歇性发起过多次勒索攻击。本月该家族继续使用 Log4j2 发动攻击，同时还新增了使用 Spring boot 漏洞和利

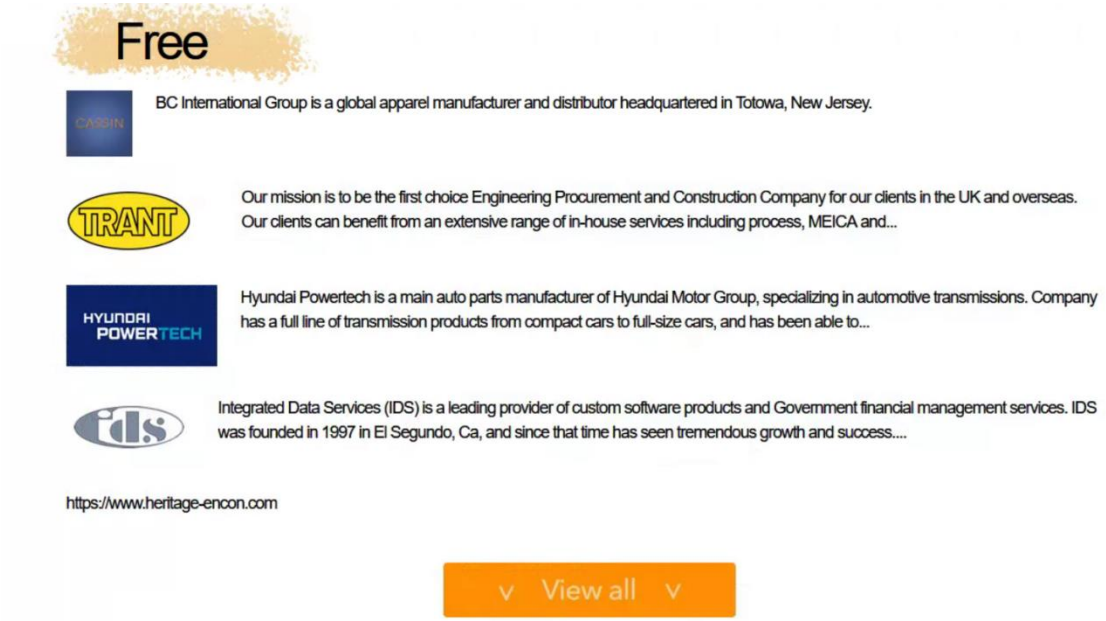
用向日葵漏洞(CNVD-2022-10270 远程代码执行)的攻击。



TellYouThePass 能够同时感染 Windows 和 Linux 操作系统，也使这个家族的危害大大增加，在下发攻击代码时，攻击者并不区分当前被攻击的操作系统。在本月，360 安全大脑也监测到有多个 Linux 设备也被该家族攻陷。

双重勒索 Cuba 开始攻击国内用户

本月监测到多个国内用户遭遇Cuba 勒索病毒攻击事件。Cuba 勒索团伙又被称作 UNC2596 勒索团伙，最早出现于 2019 年，采用双重模式(加密被攻击设备的同时，也窃取有价值的数据作为勒索赎金的重要筹码)。其最为出名的攻击方式为与恶意软件的垃圾邮件运营商 Hancitor 合作针对企业进行攻击，滥用 Microsoft Exchange 漏洞来收集数据、部署各种 Webshell、远程访问木马(RAT)等恶意程序。其受害企业/组织有 80%都来自北美，其中美国最为严重，至少有 49 个组织/企业遭遇该家族攻击。而该团伙则从这些受害者身上谋利近 4400 万美元。通过跟踪发现，该家族并未将所有受害者名单全数发布到数据泄露网站中，因此可以推断其受害者数量远高于 49 个。



LAPSUS$频繁作案，天才少年被捕

Lapsus$是一个来自多个国家组合而成的数据勒索团伙，首次出现于 2021 年 12 月，曾对巴西卫生部发起勒索。近期该团伙又多次发起数据勒索攻击，其成功攻击对象包括英伟达(NVIDIA)、三星、微软以及 Okta 等大型企业，还将 Ubisoft、电信公司 Vodafone 和电子商务巨头 Mercado 作为攻击目标，发起攻击。

在本月末，已有 7 名与该团伙有关的人员（年龄在 16 岁至 21 岁之间，其中一名 16 岁人员来自英国牛津，是 Lapsus$领导人之一，据信他从黑客活动中积累了 300 多个比特币——按今天的价值计算，约为 1300 万美元）被逮捕。

以下是近期该团伙发起的攻击中广受瞩目的案件：

- 2 月 26 日，该组织宣称已盗取知名显卡厂商 NVIDIA 的服务器，并成功窃取了超过 1TB 的内部数据。但不久后该组织又表示遭到了 NVIDIA 的反向入侵，并称对方将通过技术手段将被窃取的数据进行了加密——这一行动主要是为了防止这些敏感数据遭到泄露。但窃取到的数据被该团伙已是先备份，目前已有两个数字签名证书被泄漏，目前已经出现了使用泄露证书签名的在野恶意软件。
- 3 月 4 日，在该组织对外发布新一轮数据，泄露了韩国消费电子巨头三星电子的大量机密数据。其声称，在其发布的代码中包括：三星 TrustZone 环境中安装的所有受信应用源代码，可被用于各种敏感操作；所有生物特征解锁操作的算法；所有最新三星设备的引导加载程序源码；来自高通的机密源码；三星激活服务器的源码；用于授权和验证三星帐户的技术的完整源代码，包括所有 API 和服务。
- 3 月 20 日，LAPSUS$黑客组织在其 Telegram 频道上发布了一张截图，表明其成功入侵了微软的 Azure DevOps 服务器。并获取了其中包含 Bing、Cortana 及其他各种内部项目的源码。随后的 21 日，该组织发布了一个大小为 9GB 的 7zip 压缩包的种子文件，其中包含了 250 多个项目的源码。发布时，LAPSUS$还表示其中包含 90%的被盗 Bing 源码以及约 45%的被盗 Bing Maps 及 Cortana 源码。并声称全部源码大小约为 37GB。

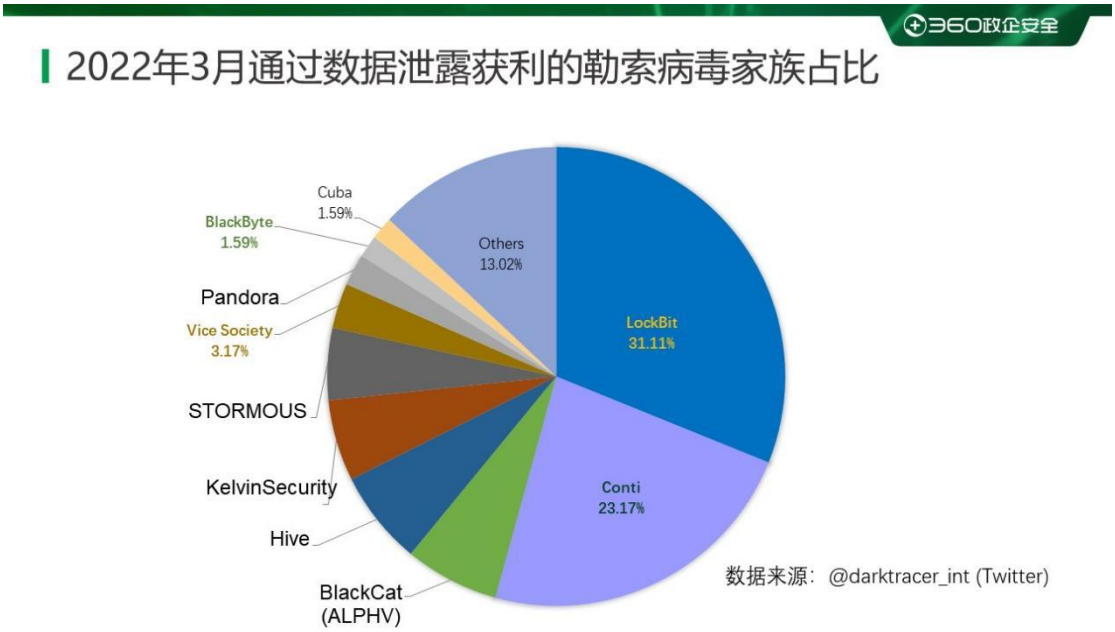
黑客信息披露

以下是本月收集到的黑客邮箱信息：

explus@tutanota.com	devicZz@mailfence.com	Dec_youfile1986@mailfence.com
@Ransome_Decrypters	recohelper@cock.li	jerry@onionmail.org
blackrose786@disroot.org	asgardmaster5@protonmail.com	asgardmaster5@protonmail.com
christian1986@tutanota.com	hello_company@protonmail.com	j.jasonm@yandex.com
melling@confidential.tips	r19nar0k@airmail.cc	ragnar0k@ctemplar.com
ragnar0k@tutanota.com	ragnarok@rape.lol	ragnarok_master@protonmail.com
ragnarok_master@protonmail.com	ragnarok_recover@secmail.pro	yawkyawkyawk@cock.li
emcryptsupport@msgsafe.io	Decryptfiles@goat.siIn	Decoder@firemail.cc
venom@privatemail.com	AcepyRansom@protonmail.com	contact@pandoraxyz.xyz
ust29@aol.com	divevecufa@firemail.cc	prismchigo@tutanota.com
supportsys@airmail.cc	consultransom@tutanota.com	consultransom@protonmail.com
erinalexralf@aol.com	happy2022@tutanota.com	curiosity08@tutanota.com
itlab@techmail.info	antich154@privatemail.com	rikyrankl13@protonmail.com
backmydata@mail.ua	jujumba@tuta.io	jokers777@tutanota.com
itlab@keemail.me	crypt2022@aol.com	antistress.ir@yandex.ru
antistress.ir@keemail.me	oslapisavkusna@onionmail.org	anticrypto@tutanota.com
file.decrypt@onionmail.org	file.decrypt@yahoo.com	crypt22@aol.com
3ncrypter.m4n@gmail.com	3ncryptionfile@gmail.com	fileback@cock.li
help.encryptor@gmail.com	help.encryptorr@gmail.com	bambam988@tutanota.com
recovery2021@msgsafe.io	jiminok31@cock.li	robdasupp@aol.com
recovery_2021@tutanota.com	DecryptionTool2022@protonmail.com	decryptiontool@mailfence.com
honest_decript2022@mail2tor.com	honest_decript2022@jabber.cz	keyforfiles@mailfence.com
alexgroup@onionmail.org	prismchigo@tutanota.com	KalajaTomorr@ctemplar.com
KalajaTomorr@firemail.cc	Bomani@Email.Com	jbomani@protonmail.com
lord_bomani@keemail.me	[Bomani@Email.Com]	recovery2021@onionmail.org
cuba_support@exploit.im	admin@encryption-support.com	snowwind@tutanota.com
snowwind@msgsafe.io	reset@email.tg	

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病毒家族越来越多，勒索病毒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病毒家族占比，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病毒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 315 个组织/企业遭遇勒索攻击，其中包含中国 9 个组织/企业在本月遭遇了双重勒索/多重勒索。

MS	APSM Systems	jlmsolicitors.co.uk
PHC	DC Solutions	progettoedilesrl.it
BDX	japoauto.com	centuryaluminum.com
TIG	redgwick.com	BERITASATUMEDIA.COM
GEBE	Banco Caribe	ROXCEL Trading GmbH
Anac	Wibag Bau Ag	Allied Eagle Supply
CORT	Polynt Group	NSM Insurance Group
eGOV	besp-oak.com	centralaccident.com
Stago	Royal LePage	CARACOL TV COLOMBIA
GomeA	FitFlop Ltd.	Aluminerie Alouette
ANTEL	drory.com.cn	Fuchs North America
denso	Ward Hadaway	jrichard-paysage.fr
SOVOS	scanvogn.com	brownsville-pub.com
Xtera	EUROPA GROUP	Gleason Corporation
IRGiT	Sport Vision	bafokengholdings.com
Hearst	e-fmc.com.ar	grupodeincendios.com
ASPIRO	Buhck Gruppe	burlingtonsafety.com
its.ws	MZ Architects	Neschen Coating GmbH
MIGROS	AB Karl Hedin	Azimut Benetti Group
Nestle	edukgroup.com	Automobil Holding AS
ICONIC	FAIR-RITE.COM	Dayton T. Brown, Inc
M.T.B.	Bradsby Group	STUDIO PEREGO S.R.L.
Migros	Bigmtransport	museum-dingolfing.de

UK GOV	rh-europe.com	megaproductos.com.ec
Ondeck	onglesdor.com	Equicom SAVINGS BANK
Rosewd	HAVI Logistic	Snap-on Incorporated
Aurora	ikk-group.com	yachtcharterfleet.com
INVIMA	sysmac.com.sg	Pakistan Human Rights
CR ASIA	TST Logistics	zentrum-dreilinden.ch
Centris	sapulpaps.org	microflex-services.de
LGE.com	elitecorp.com	UCC COFFEE UK LIMITED
PFC USA	HOL-MAC Corp.	tomlinsonelectric.com
BAUKING	avcimmedia.com	chicagosteelgroup.com
BEXIMCO	DK Engineering	Cellulant Corporation
ihg.com	credenceid.com	orientalaromatics.com
Boralex	ignitarium.com	Carpenter & Zuckerman
Kemutec	WELCOME HOTELS	Rettenmeier Holding AG
SAMSUNG	zabel-group.de	Walsall North Foodbank
bcad.org	connectcec.com	Bounce Interactive Ltd
qarch.nl	jewelry.org.hk	KELLY,REMMEL&ZIMMERMAN
Pollmann	bChannels Ltd.	rebuildingtogether.org
LW Group	specialinc.com	Bullfrog International
crich.it	matteolisrl.it	bedfordshire.police.uk
ICEHOTEL	Get-integrated	Aquatech International
Rotoplas	Cummins-Wagner	Smith Transport company
Okta.com	Assimoco Group	Relationships Australia
stormous	MFT Automation	confindustriacaserta.it
ismea.it	Bcintlgroup.com	ITECOR International SA
denro.ca	Maintainco Inc.	taguefamilypractice.com
Sheppard	Centurion Stone	Empire Electronics Inc.
VadaTech	UCSI University	bridgestoneamericas.com
Viva Air	UAV Engines LTD	RAWLE and HENDERSON LLP
etrps.de	ENOS PROPERTIES	Parker Appliance Company
4A Games	Banco do Brasil	ONCALL Language Services
tccm.com	Argo Turboserve	UNITEK Contracting Group
Imenco AS	rosslare.com.hk	Scott Manufacturing, LLC
Biz Retek	aetnabridge.com	comune.villafranca.vr.it
axessa.ch	unapen.internal	Fuji America Corporation
Asphalion	Milan Institute	Monteleone & McCrory LLP
avidoc.fr	fantasy company	UK's Ministry of Defence
Powertech	Smith Transport	stanthonys.slough.sch.uk
GRS Group	tingtong.com.cn	Fujioka Eletro Imagem SA
solvi.com	Beaulieu Canada	Instituto Federal Goiano
BMW CHILE	Unical Aviation	serilization-services.com
Noble Oil	Ciments Guyanais	Otto Dörner GmbH & Co. KG
vvrmc.org	Critical Content	hilltopconstructionco.com

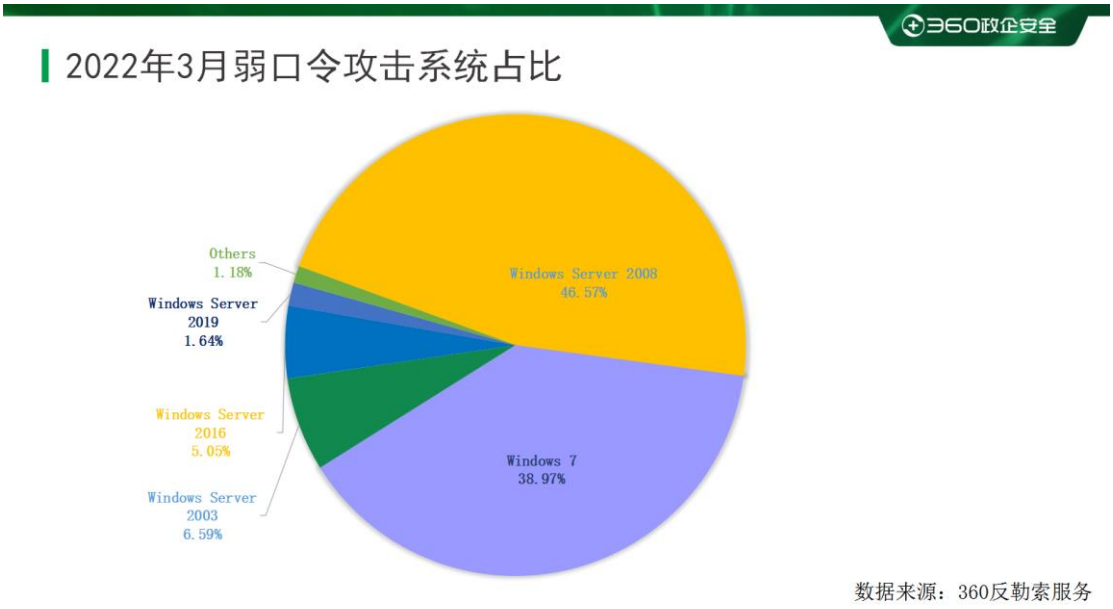
AllOffice	intouchgroup.net	Roosevelt School District
IMT GROUP	Satz Kontor GmbH	United McGill Corporation
BAUCENTER	apec-capital.com	BANQUE CENTRALE DE TUNISIE
A.J. Rose	dgordonlcswr.com	Konradin Mediengruppe GmbH
wimmog.ch	montanarisrl.net	Managed Business Solutions
haeny.com	finances.gouv.cg	snteseccion30sartet.org.mx
Rudsak Inc	ambujaneotia.com	Dick Anderson Construction
ctigas.com	SENADO Argentina	Zeeland Farm Services, Inc.
NetCompany	Blackmon Mooring	Oklahoma City Indian Clinic
LPA Design	Warren Resources	Normandeau Associates, Inc.
Grcouceiro	simatelex.com.hk	OSSEG Obra Social de Seguros
genesis.ky	United Cumberland	I-SEC International Security
draftex.de	Jammal Trust Bank	3S Standard Sharing Software
lawsdn.com	Diamond Pet Foods	Afghanistan Breshna Sherkat
inibsa.com	pirsonholland.com	Sav-Rx Prescription Services
cachibi.co	Hochschild Mining	Centerline Communication Llc
PK Simpson	stt-logistique.fr	Loepthien Maeder Treuhand AG
bioskin.sg	ca.daiyafoods.com	Credit Risk Management Canada
Epic Games	Herbert Slepoy Co	Royal Brunei Airlines Sdn Bhd
Caledonian	MJH Life Sciences	Griggsville-Perry High School
Amtech Llc	Talent Logic Inc.	School District Of Janesville
Yip in Tsoi	vri.maniberia.net	Jaffe Raitt Heuer & Weiss, P.C.
infotech ua	sbctanzania.co.tz	South Africa Electricity company
Trant.co.uk	medinadairy.co.uk	Universidade Federal de Sao Paulo
Globant.com	Great HealthWorks	Waller Lansden Dortch & Davis, LLP
guazzini.it	SRI International	VOYAGER DISTRIBUTING COMPANY PTY. LTD.
Haltonhills	Get Fresh Company	Cabinet médical de groupe de Courtepin
lazpiur.com	Passero Associates	Confederation of Indian Industry (CII)
bbst-clp.de	Sanoh America Inc.	Scottish Association for Mental Health
NORDEX FOOD	Rubinstein Company	Salvadoran Ministry of Foreign Affairs
kbkbcpa.com	Round Oak Minerals	KONICA MINOLTA MARKETING SERVICES LIMITED
gezairi.com	thionvillenola.com	PAN AMERICAN ENERGY S.L. SUCURSAL ARGENTINA
caribetours	danubiushotels.com	Instituto Nacional de Tecnología Agropecuaria
Core Design	GlobalWafers Japan	Cabinet de groupe Dr. Cosandey Tissot / Dr. Nobel
vbsharma.ca	freedomfarmspa.com	CHINA Government and Social Capital Cooperation Center

etg.digital	GRUPPO ANGELANTONI	Ministry For Foreign Affairs Of The Republic Of Indonesia
Myron Corp.	Lifetech Resources	Instituto De Gesto Estratégica De Sade Do Distrito Federal
Prima Power	Shapiro and Duncan	KONECTA SERVICIOS ADMINISTRATIVOS Y TECNOLOGICOS S.L. SUCURSAL ARGENTINA
keypoint.com	omalleytunstall.com	Establishment of the Agency for the Environmental Protection of the Marche Region

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 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。

数据来源：360系统安全防护

通过观察 2022 年 3 月弱口令攻击态势发现，RDP 弱口令攻击和 MYSQL 弱口令攻击整体无较大波动。MSSQL 弱口令攻击虽有波动，但无大的变动，整体呈下降态势。

数据来源：360系统安全防护

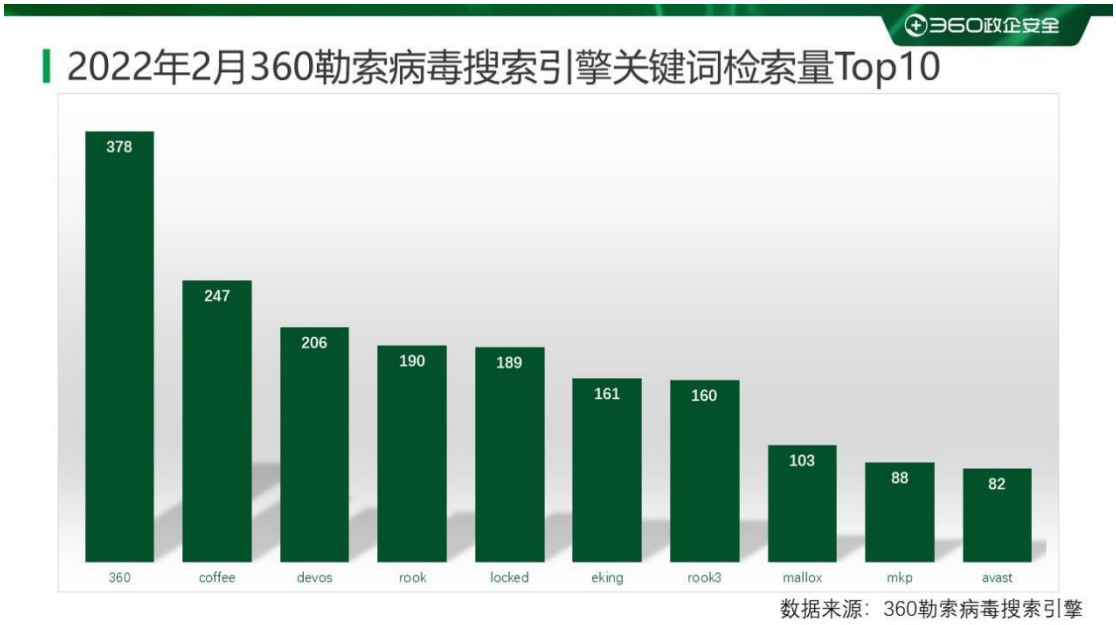
勒索病毒关键词

以下是本月上榜活跃勒索病毒关键词统计，数据来自 360 勒索病毒搜索引擎。

- 360：属于 BeijngCrypt 勒索病毒家族，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。
- coffee：属于 Coffee 勒索病毒家族，由于被加密文件后缀带有 coffee 而成为关键词。

该家族主要传播方式有两种，第一种为通过伪装成具有诱惑性的钓鱼邮件，第二种为蠕虫。

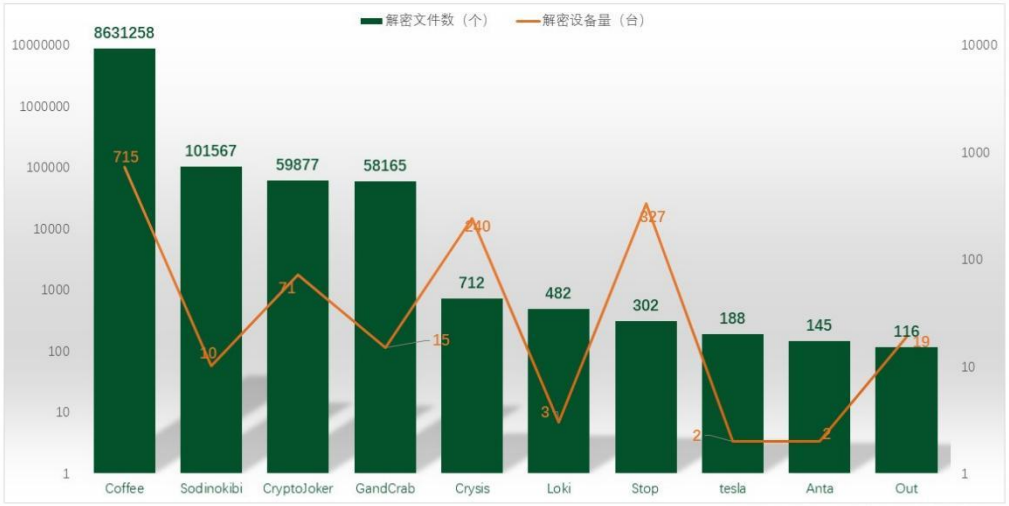
- devos：该后缀有三种情况，均因被加密文件后缀会被修改为 devos 而成为关键词。但本月活跃的是 phobos 勒索病毒家族，该家族的主要传播方式为：通过暴力破解远程桌面口令成功后手动投毒。
- rook:属于 Rook 勒索病毒家族，由于被加密文件后缀会被修改为 rook 而成为关键词。该家族的主要传播方式为：通过匿隐僵尸网络进行传播。本月(2022 年 2 月)受害者大部分是因为到下载网站下载注册机感染的匿隐僵尸网络。
- Locked:locked 曾被多个家族使用，但在本月使用该后缀的家族是 TellYouThePass 勒索病毒家族。由于被加密文件后缀会被修改为 locked 而成为关键词。该家族本月主要的传播方式为：通过 Log4j2 漏洞进行传播。
- eking：属于 phobos 勒索病毒家族，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。
- rook3:同 rook。
- mallox：属于 Mallox 勒索病毒家族，由于被加密文件后缀会被修改为 mallox。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。
- mkp：属于 Makop 勒索病毒家族，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。
- avast：同 mallox。



解密大师

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

2022年2月解密大师解密量



数据来源：反勒索服务统计数据