2022 年 8 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：Moishsa、Filerec、DON#T (Donut Leaks)、iceFire、CryptOn、BlOOdy、DAIXIN、VSOP 等家族，其中 DON#T (Donut Leaks)、iceFire、CryptOn、BlOOdy、DAIXIN、VSOP 均为双重勒索勒索软件家族。其中 VSOP 勒索软件是 Onyx 勒索软件演变而来，加密大于 2MB 文件时，将使用垃圾数据进行覆盖，因此被该家族加密的文件，购买解密器也只能恢复小于等于 2MB 的文件。

以下是本月最值得关注热点：

一、TellYouThePass 针对中小微企业用户发起大规模勒索攻击。

二、LockBit 勒索软件家族采用三重勒索模式运营。

三、勒索软件买一赠一？新型勒索软件 RoBaj 还未传播先被感染。

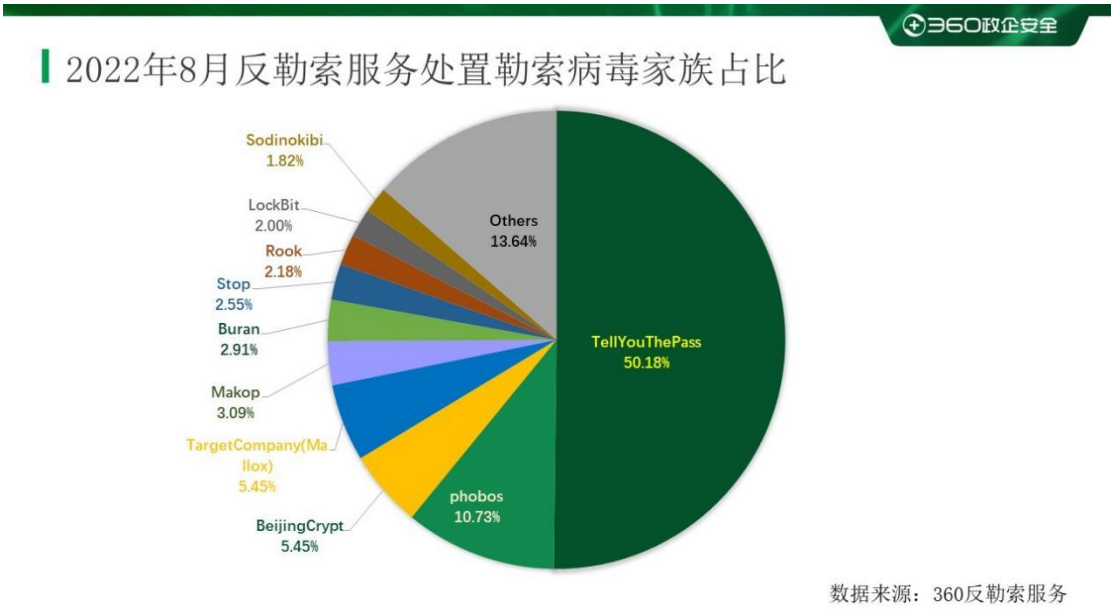
四、Cisco 遭阎罗王勒索软件攻击，2.8TB 数据被窃取。

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。

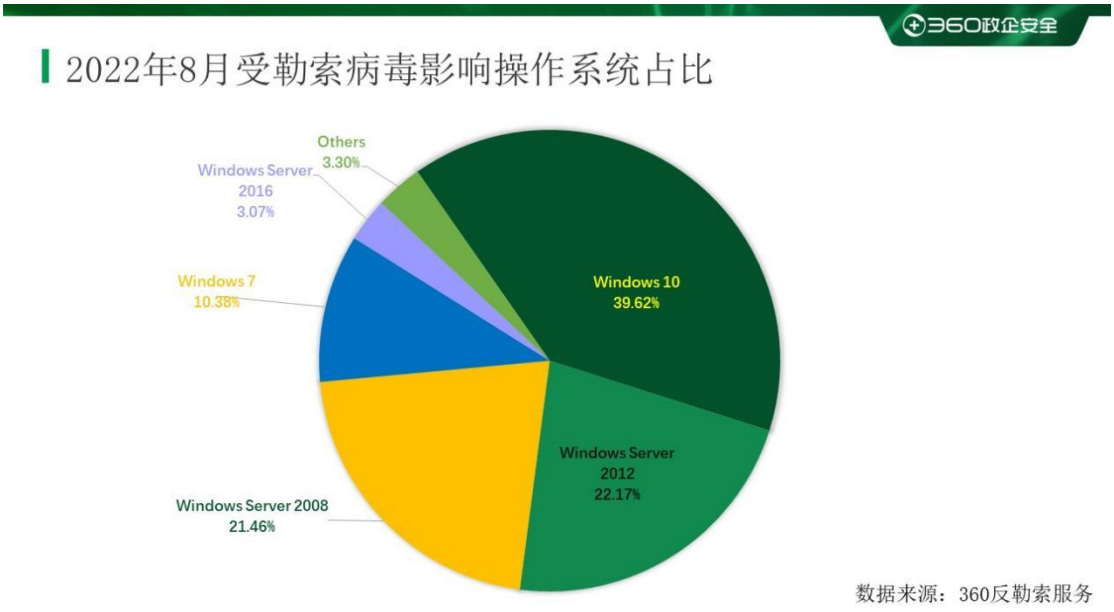
感染数据分析

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 50.18%居首位，其次是占比 10.73%的 phobos，BeijingCrypt 家族以 5.45%位居第三。

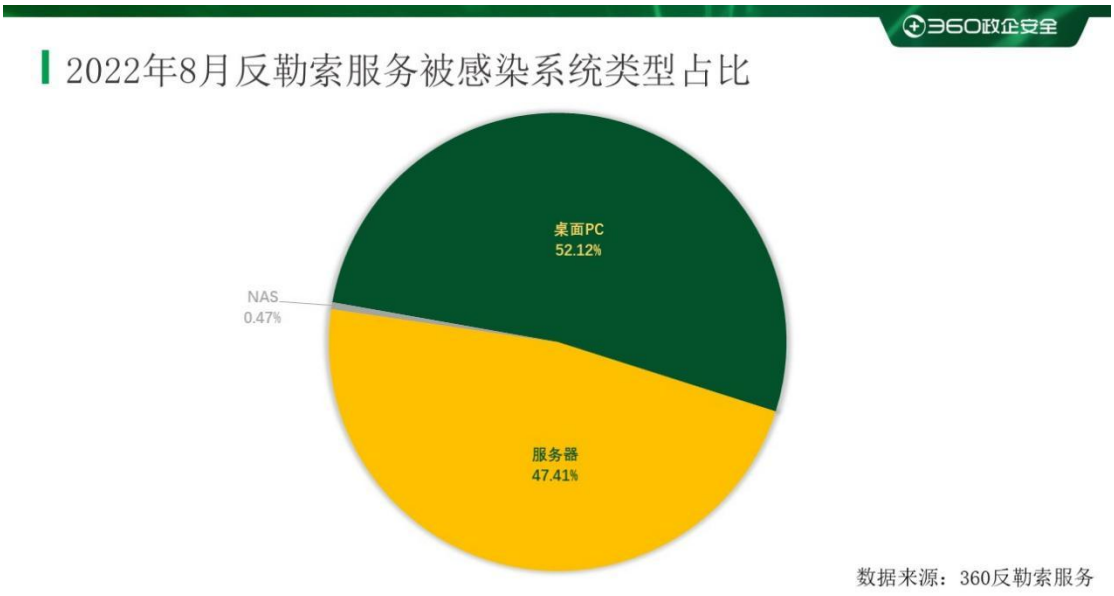
本月 TellYouThePass 利用安全漏洞，对中小微企业发起攻击，短时间的大量传播导致其占比超过了 50%。TellYouThePass 多次对国内用户发起攻击，善于利用各类 nday 漏洞，发起快速攻击。对该家族应该提高警惕。



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。



2022 年 8 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，本月因突发事件影响，导致被勒索软件感染的服务器系统占比上涨近 18%。



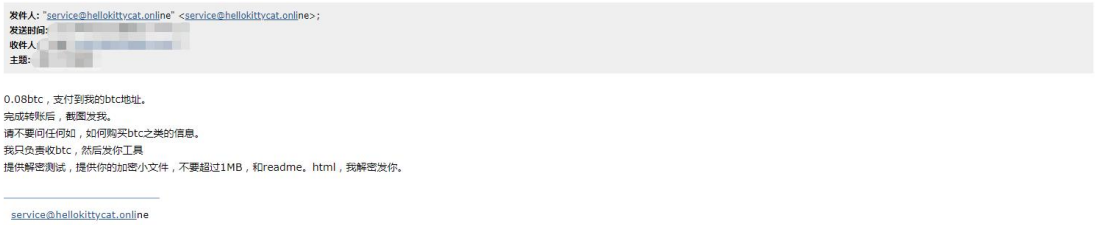
勒索软件疫情分析

TellYouThePass 针对中小微企业用户发起大规模勒索攻击

360 安全大脑监测到，TellYouThePass 勒索软件家族利用安全漏洞针对国内中小微企业用户发起攻击，此次攻击从 8 月 28 日 21 时开始，一直持续到 8 月 29 日 1 时左右，短时间内有较多设备被加密。

被攻击设备中的大部分文件被加密，后缀被添加“.locked”扩展名，并留下勒索信息READ_ME.html，内容为支付 0.2 比特币，并留下联系邮箱。通过与攻击者邮件沟通，对方能够熟练使用中文，对该勒索病毒的分析显示，病毒依然沿用三层加密技术，在没有攻击者私钥的情况下，无法大规模技术破解。

黑客或许是为了躲避追踪，没过多久便不再使用勒索提示信息中留下的邮箱和钱包地址。除此之外黑客索要的赎金也降低至 0.08BTC。有消息称，黑客与第三方协议只需 0.05BTC 即可解密一台设备， 这很大可能是黑客降价的原因。



LockBit 勒索软件家族采用三重勒索模式运营

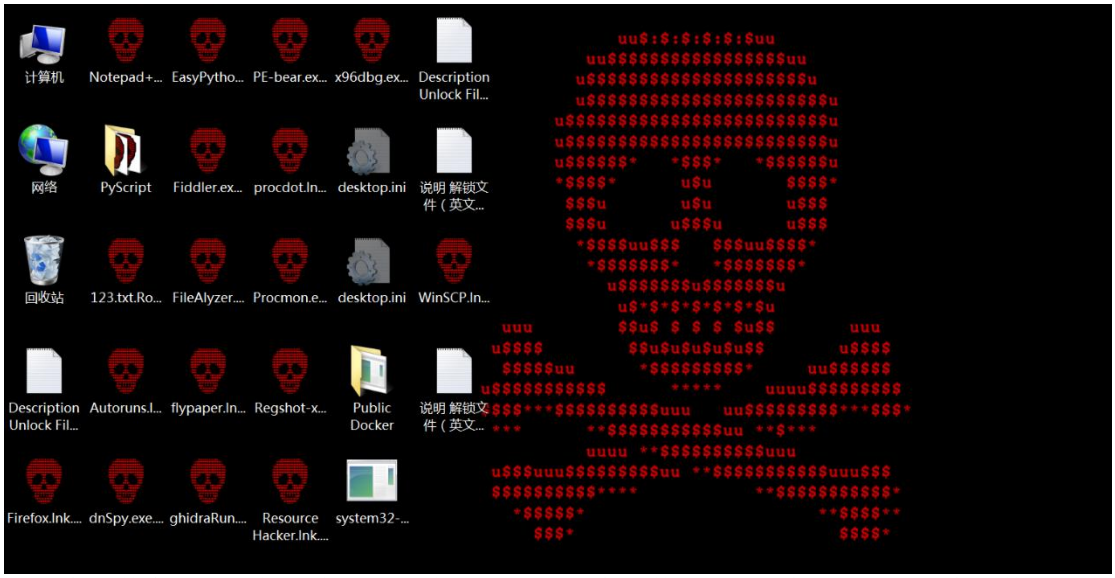
LockBit 勒索软件团伙宣布，它正在改善对分布式拒绝服务（DDoS）攻击的防御能力。同时，他们也受此启发，准备将 DDoS 作为新增的“第三重”勒索手段。

近期，该团伙遭受了来自安全公司 Entrust 的 DDoS 攻击，该攻击的目的是为了阻止外界对该团伙在其泄漏网站上发布的 Entrust 公司相关数据的访问。

而就在 8 月底，LockBit 勒索软件团伙便通过自家的 LockBitSupp 对外宣布，该团伙已通过改进网络设备重新恢复业务，使其泄露能力免受 DDoS 攻击的影响。与此同时，勒索软件运营者现在还寻求在加密数据并泄漏数据的基础上再添加 DDoS 作为新的第三重勒索策略。

勒索软件买一赠一？新型勒索软件 RoBaj 还未传播先被感染。

近日 360 安全大脑监测到一款新型勒索软件 RoBaj。该勒索软件使用 C#编写，通过暴力破解远程桌面登录口令的方式入侵系统并手动投毒。文件被加密后不仅扩展名会被修改为.RoBaj，文件图标会被修改为一个红色的骷髅头。



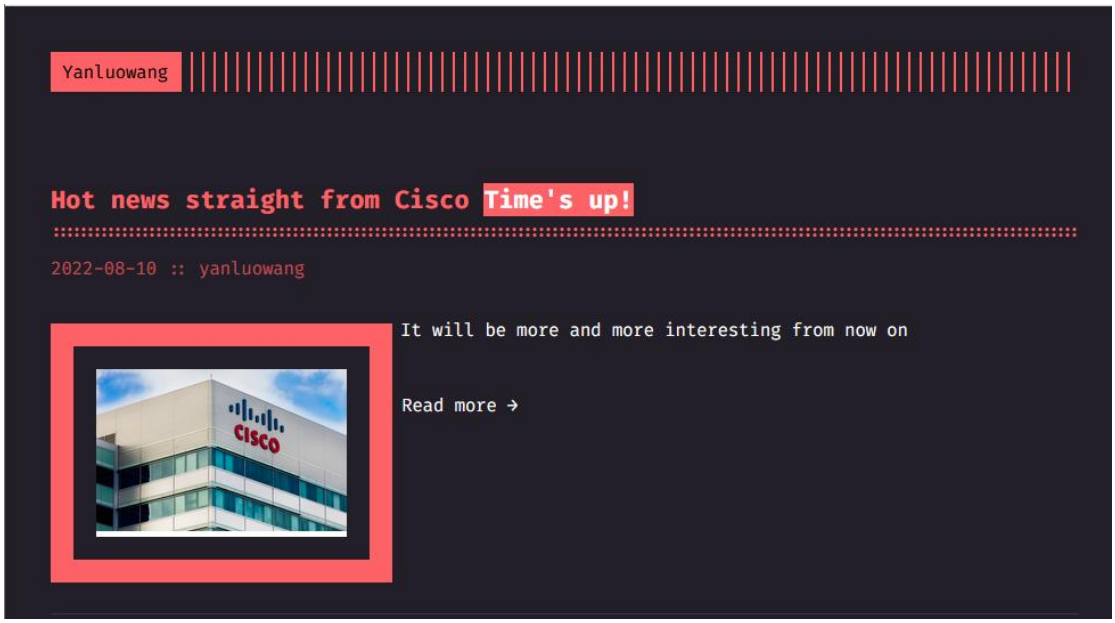
该勒索软件家族是比较少有的支持中英双语的勒索软件，值得注意的是，该勒索软件开发者的环境似乎被 Neshta 蠕虫感染，勒索软件释放的所有可执行程序均感染 Neshta 蠕虫。这让受害者面临更大的威胁。目前 360 高级威胁研究分析中心目前已完成对该病毒的破解，若有用户不幸中招， 可第一时间提交反勒索服务寻求解密帮助。

Cisco 遭阎罗王勒索软件攻击，2.8TB 数据被窃取。

思科公司于 8 月 10 日证实，阎罗王勒索软件组织在 5 月下旬入侵了其公司网络，入侵者试图在网上泄露被盗文件用以勒索他们。该公司透露，攻击者只是从受入侵员工帐户所关联的共享文件夹中收集和窃取到一些非敏感数据。

阎罗王攻击者是在劫持了员工的个人 Google 帐户（其中包含从其浏览器同步的登录凭据）后，使用被盗的凭据访问了思科的网络。而该组织也在 8 月初时发声，表示已窃取了

思科 2.75GB 的数据，其中包括大约 3100 个文件，文件中还包含了许多保密协议、数据转储及工程图纸。



黑客信息披露

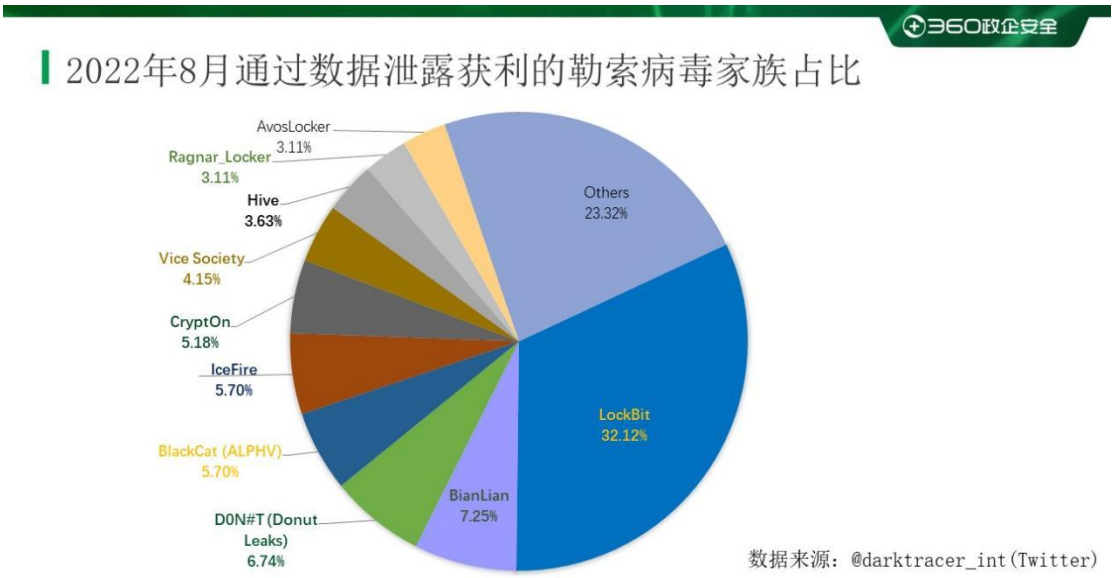
以下是本月收集到的黑客邮箱信息：

2hlkhbebenw@proton.me	2hlkhbebenw@tuta.io	recoversupportman@firemail.cc
thekeyishere@cock.li	blueman5@tutanota.com	Trebaler@goat.si
mssqlppt@tutanota.com	BobyWillson@gmx.com	gotoremote@onionmail.org
buybackdate@nuke.africa	mylastlover@runbox.com	aiimissue2022@proton.me
honestly@onionmail.org	Bluemanteam@my.com	johnson_john_26@aol.com
djek77d@aol.com	SWikipedia@mail2tor.com	swikipedia@onionmail.org
oceannew_vb@protonmail.com	hyakunoonigayoru@yahoo.co.jp	consult.raskey@onionmal.org
angry_war@protonmail.ch	msupport2019@protonmail.com	friendendfriend@cock.li
brittonucgml47@gmail.com	msupport@elude.in	decryptyourfiles007@cock.li
yashinkov007@tuta.io	regina4hgoregler@gmx.com	pansymarquis@ yahoo.com
crioso@protonmail.com	wiruxa@airmail.cc	yongloun@tutanota.com
anygrishevich@yandex.ru	kassmaster@danwin1210.me	kassmaster@tutanota.com
trustdatanswer@tutanota.com	willettamoffat@yahoo.com	uspex1@cock.li
avarious@protonmail.com	uspex2@cock.li	filescrp@420blaze.it
filescrp@yandex.ru	gunsofthepatriots@privatemail.com	udacha123@mail2tor.com
kd8eby0@nuke.africa	kd8eby0@onionmail.org	kd8eby0@inboxhub.net
@udacha123yes	lechiffre@mailchuck.com	lechiffre@india.com
stephenjoffe@privatemail.com	tomas1991goldberg@libertymail.net	backyourfiless@mailfence.com
jackdecrypt@msgsafe.io	gichugre@tfwno.gf	king2022@tutanota.com
usupmail@webmeetme.com	rootma@cyberfear.com	ClaraSchumann1819@gmx.com
backyourfiless@mailfence.com	ClaraSchumann1819@gmx.com	brittonucgml47@gmail.com
friendendfriend@cock.li	allisonmartin813@yahoo.com	allisonmartin813@cock.li

samersby@tuta.io	empress8@protonmail.com	funny385@swisscows.email
funny385@tutanota.com	service@sunshinegirls.space	

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 193 个组织/企业遭遇勒索攻击，其中包含中国 4 个组织/企业在本月遭遇了双重勒索/多重勒索。

Smith brothers	Tap Air Portugal	NCG Medical
MEIJI.COM.SG	Magnachem	Alegria Family Services
WWAY-TV, LLC	Ramada Hervey Bay Hotel Resort	Community Dental Partners
4cRisk	Captec-group	GOV Brazil
ICMPD	Josef Saller Services e.K. - Saller Bau	Laferté
Justman Packaging & Display Information	Skupstina	Spalding Grammar School
Abdulaziz, Grossbart & Rudman	The Preston Partnership	Advance Corporation
International Custom Controls	currierryan.com	nwoods.org
northwoods.church	embalajescapsa.com	accionplus.com
ygboulons.com	uplexis.com.br	Khoemacau Copper Mining
Grande Stevens	Torin Drive	goodwillnm.org
Mount Vernon Mills	perteet.com	canteen.com
trufab.com	kkcsworld.com	cenviro.com
microdepot.com	draperyconceptsny.com	galenica.ma
stjohnvianney.org	stevesilvaplumbing.com	lenax.com
americantilestone.com	statravel.de	thininfra.nl

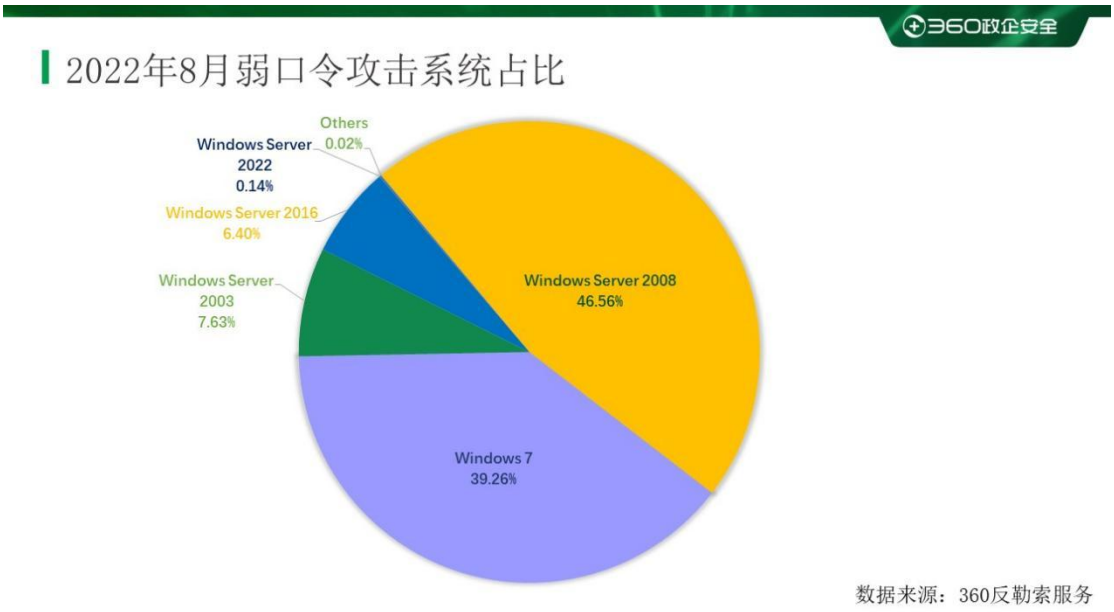
sportlavit.nl	hikadikoy.com	Lampton School
Frances King School of English	Altice International	centrodsr.it
growag.ch	ANGT	vandermaesen-nv.be
Sheppard Robson	Restovichlaw	Pastas capri
Mauritius standards bureau	Epec	DESFA
associes-finance.com	Action Labs	Enso Detego
Sando	CMZ UK	PlanET Biogas Solutions
Los Alamos Nature Center	Olamgroup	Baton Rouge General
GMX	solidatech.com	pinjuhlaw.com
Engine Power	robitgroup.com	destinationhope.com
studiobarba.com	orioninc.com	ruffinlawyers.com.au
barrydowd.com	Bombardier Recreational Products (BRP)	Action Lab
Garnica Plywood	Casa International	WBSCHOOLS
Moskowitz, Mandell & Salim, P.A.	northwestpipe.com	Northern Contours Inc.
Family Medicine CentersFMC Clinics	BSA Hospice of the Southwest	*.algotrader.com
*.bestservers.pro	*.iperactive.com.ar	*.ccol.com
*.vps-vds.com	*.guneshosting.com	*.kodhosting.com
*.kru.ac.th	*.directfn.net	*.feesh.ch
*.skifgroup.com	DESFA	cap***-*****.com
Reiter Affiliated Companies	PROSOL	Shaw & Slavsky
Consejo Superior de Investigaciones Cientificas	Department of Indre-et-Loire	entrust.com
wabteccorp.com	traveldoc.ca	megal.com
Tang Capital	WOOTTON ACADEMY TRUST	burnettefoods.com
Stratford University	Accelya	Apex Capital Corp
AMBE	porcelanosa-usa.com	Vygon Spain
SOUTH-STAFFS-WATER.CO.UK	tierltechs.screenconnect.com	altaadhod.com
Methodist McKinney Hospital	William A. Kibbe & Associates	Calin Group
ELEFONDATI SRL	TriState HVAC Equipment	vsainc.com
qualitymedicalinc.com	pinnick.co.uk	Fast Pace Health
okcu.edu	whitworth.edu	Cisco
Gannon Associates	8 Italy Districts	ah-a.de
ISTA International GmbH	FOSUN.COM	valverdehotel.com
An Turkey Certified Public Accountancy Firms	Freyr Solutions	Artic Building Services
ring-plastik.de	versma.com	www.pcoli.com
oncallpractice.com	unimasters.com	trialpro.com
newwestmetals.com	wrschool.net	hatcherins.com
Wh******* U********	Borough of Union Beach	LYDECKER
AD Consulting Group	SEMIKRON	farralls.co.uk
BEESENSE	Liftow LTD	ENN Group
Fitzgibbon Hospital	Trib Total Media	STTLK
A.B. Florence S.r.l	Sanmarti	Cmtransport
Kampmeier-tietz	Visser Brothers	Ecogest SpA

Domexpats	Geriatrics Management	Guardforce
unisys.com	AIIM	OGLETREE
Boehl Stopher & Graves	Doosan Group	Ethniv.com
MarioSinacola	kangaroo.vn	tekinox.it
obriengroupaustralia.com.au	Puma Biotechnology	casapellas.com
preflooring.com	scohil.com	ARISA CORREDORES DE SEGUROS
shopper360.com.my		

表格 2. 受害组织/企业

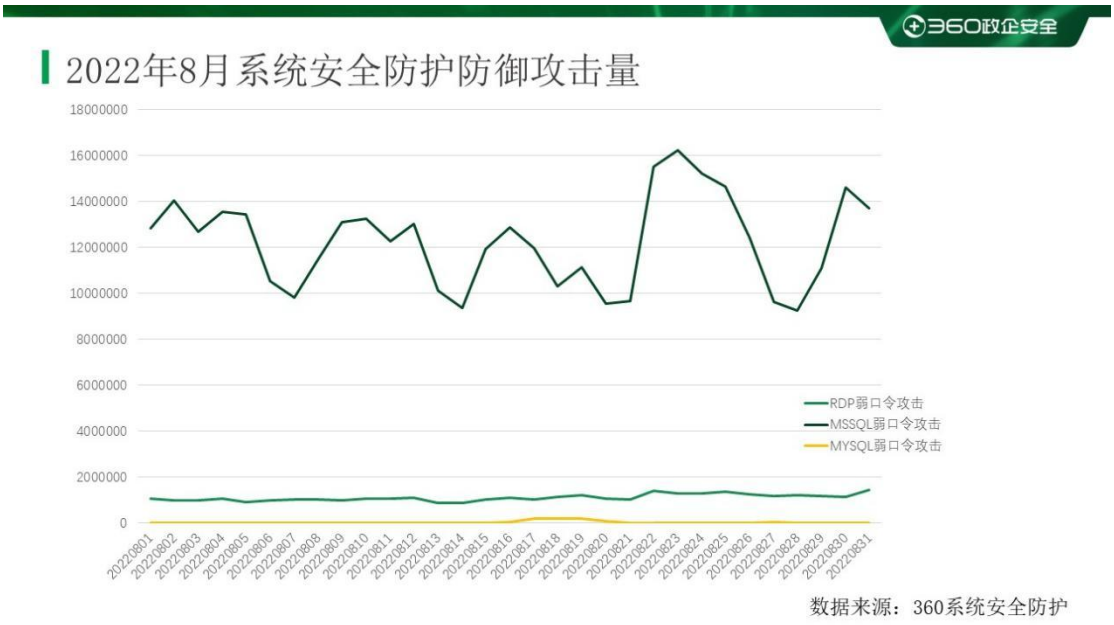
系统安全防护数据分析

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 8 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 2022 年 8 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.



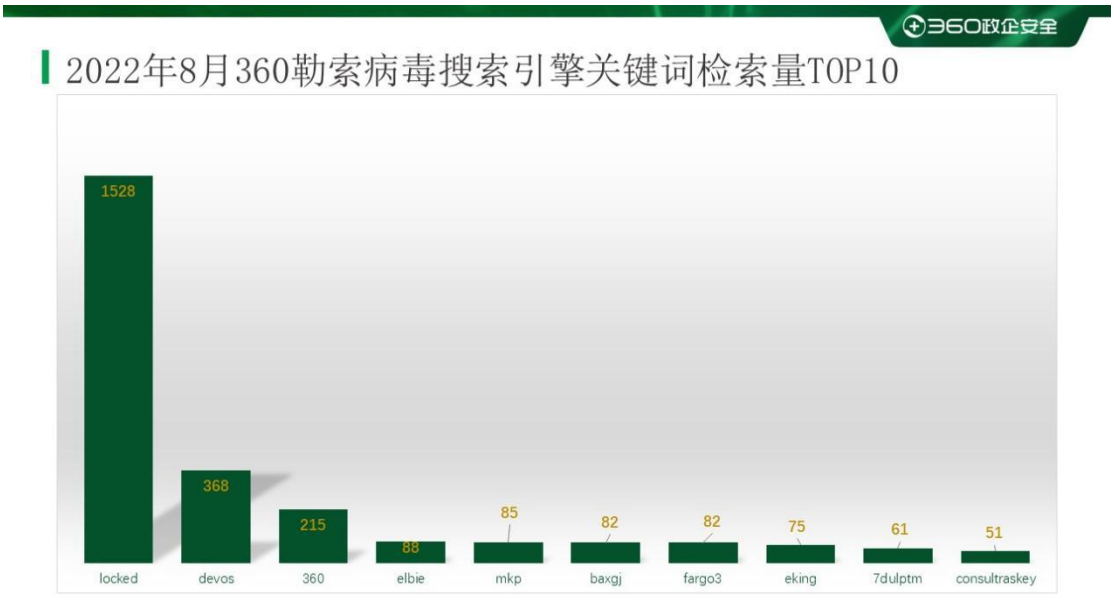
勒索软件关键词

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。

- 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。

- elbie：属于 phobos 勒索软件家族，由于被加密文件后缀会被修改为 elbie 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。
- baxgj：属于 Sodinokibi(REvil)勒索软件家族，由于被加密文件后缀被修改为 baxgj 而成为关键词(一个受害者通过一个后缀，本月搜索量较大主要因为某企业受灾面积广，导致搜索量上涨。）通常加密文件前还会窃取受害企业内部数据。因其采用 RaaS 模式运营，其下附属公司多，因此其传播方式通常非常多样化。
- 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：同 elbie。
- 7dulptm：属于 BlackCat 勒索软件家族，由于被加密文件后缀会被修改为 7dulptm 而成为关键词。通常加密文件前还会窃取受害企业内部数据。因其采用 RaaS 模式运营，其下附属公司多，因此其传播方式通常非常多样化。
- consultraskey：同 fargo3。



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 Coffee。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 Crysis 家族加密的设备。

本月新增对 Robaj 勒索软件家族的解密支持。

2022年8月解密大师解密量

数据来源：反勒索服务统计数据