勒索软件流行态势分析

2023 年 8 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数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 8 月，全球新增的活跃勒索软件家族有 INC Ransom、RansomedVC、Cloak、Peace Tax Agency、Metaencryptor 等家族。

以下是本月值的关注的部分热点：

1. TellYouThePass 再度来袭，集中攻击 OA 及财务类系统平台

2. Rhysida 勒索软件被锁定为近期针对医保系统的攻击事件幕后黑手

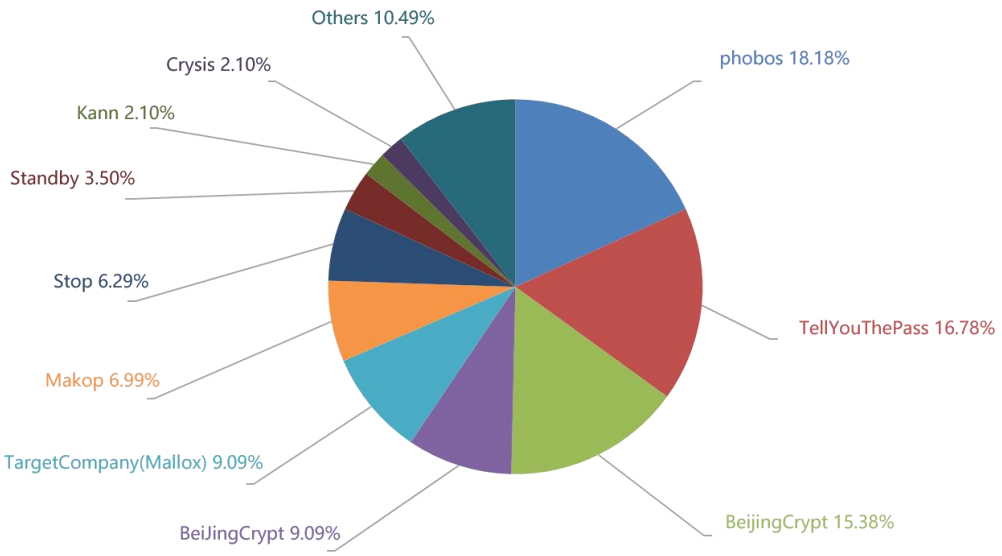
3. 日本钟表制造商精工遭 BlackCat 勒索软件团伙攻击

基于对 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）发布本报告。

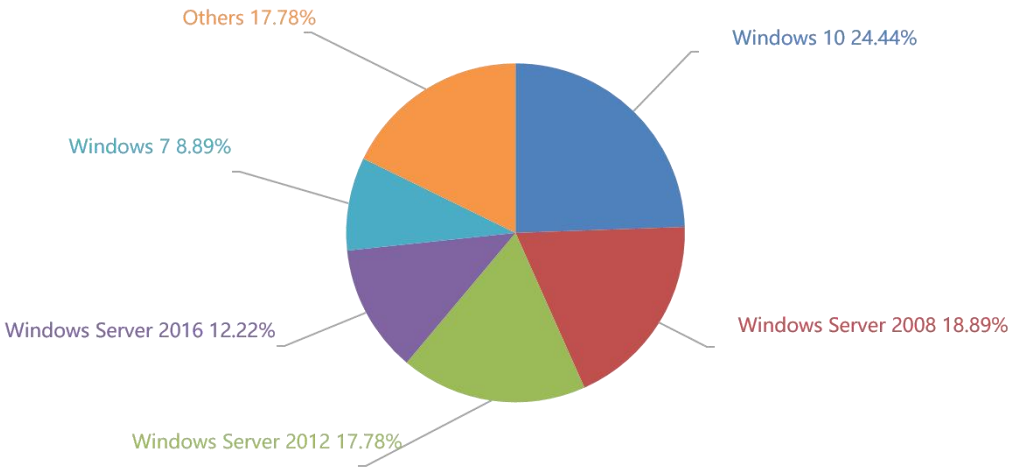
感染数据分析

针对本月勒索软件受害者设备所中病毒家族进行统计：Phobos 家族占比 18.18%居首位，第二的是占比 16.78%的 TellYouThePass，BeijingCrypt 家族以 15.38%位居第三。

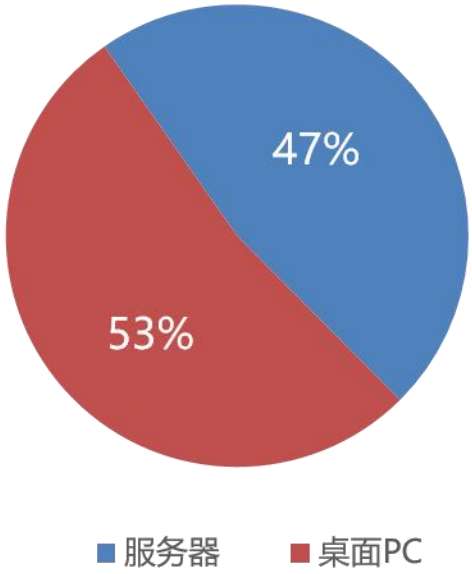
其中，位居第二的 TellYouThePass，在 8 月最后一个周末，利用 web 漏洞发动大面积攻击。



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。



2023 年 8 月被感染的系统中，桌面系统和服务器系统占比显示，受攻击的系统类型占比基本相当。

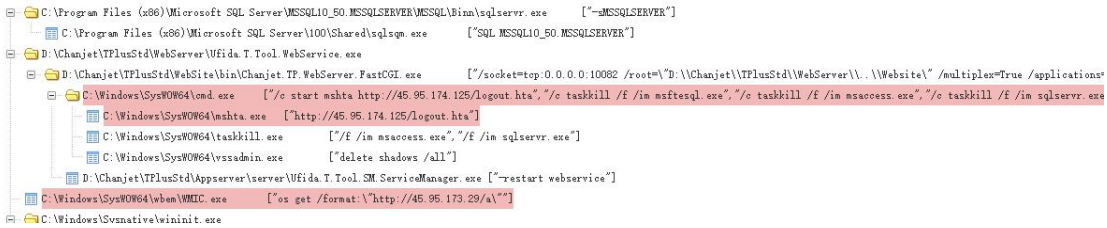


勒索软件热点事件

TellYouThePass 再度来袭，集中攻击 OA 及财务类系统平台

8 月 27 日，发生一起针对 OA、财务类系统平台的勒索投毒攻击事件，攻击目标主要为畅捷通财务管理软件，投递病毒为“TellYouThePass”勒索病毒。此次攻击的范围波及大约 1000 台服务器，目前攻击所使用的载荷已下线，但攻击本身仍在自动执行中。

攻击现场如下:



目前已发现的攻击载荷如下（目前均已下线）：

hxxp://45.95.174.125/logout.hta

hxxp://45.95.173.29/a

“TellYouThePass”勒索病毒家族是一种勒索软件，最早于 2019 年 3 月出现。由于其背后始终是由单一黑客组织运营，因此该黑客组织也同样被称为 TellYouThePass。根据现有线索推断，该组织为国内黑客团伙，其惯于在高危漏洞被披露后的短时间内利用漏洞修补的时间差，对暴露于网络上并存在有漏洞的机器发起攻击。

其曾经使用过的代表性漏洞有：“永恒之蓝”系列漏洞、WebLogic 应用漏洞、Log4j2 漏洞、用友 OA 漏洞、畅捷通漏洞等。而一旦攻击成功后，便会投递勒索病毒实施加密，并向被加密的文件添加后缀名为“.locked”。

该家族在去年发动了几轮攻击后，已经逐渐销声匿迹。但今年 6 月初，TellYouThePass 再次卷土重来，利用畅捷通 T+财务管理系统中存在的命令执行漏洞发起攻击发起了一波较为强势的攻击。而本轮攻击是今年其“重出江湖”后的第二次大规模勒索攻击。希望广大政企单位对各类网络服务、OA 及财务类应用的安全问题提起重视，及时修补漏洞并进行有效的安全监控和管理。

Rhysida 勒索软件被锁定为近期针对医保系统的攻击事件幕后黑手

近期针对医疗机构的一波攻击迫使美国政府机构和网络安全公司更加密切地关注 Rhysida 勒索软件。在美国卫生与公众服务部(HHS)发布安全公告后，CheckPoint、思科 Talos 和趋势科技均发布了有关 Rhysida 的报告，对其攻击者进行密切关注。今年 6 月，Rhysida 在其数据泄露网站上泄露了从智利陆军（Ejército de Chile）窃取的文件后首次进入公众视野。在当时，安全人员对 Rhysida 的初步分析表明，该勒索软件正处于早期开发阶段，缺少大多数病毒株中常见的标准功能。如持久性机制、卷影复制擦除、进程终止等。

而近期 Rhysida 在暗网数据泄露网站列出了澳大利亚的一家医疗机构，并在对外宣称这些数据被盗之前曾给对方一周的时间支付赎金。根据美国卫生与公众服务部(HHS)8 月初发布的一份公告警告称：虽然 Rhysida 仍在使用较为基础的加密程序，但其扩散规模已发展到了非常危险的程度。最近，攻击者更是表现出对医疗保健相关机构的特别关注。

据消息人士透露，Rhysida 是近期 Prospect Medical Holdings 遭受网络攻击的幕后黑手。该公司的系统目前仍然因受到攻击而中断，并已影响了美国各地的 17 家医院和 166 家诊所。 但 Rhysida 尚未宣布对此次攻击负责，PMH 也没有公布有关勒索软件团伙是否是此次攻击幕后黑手的电子邮件。

日本钟表制造商精工遭 BlackCat 勒索软件团伙攻击

2023 年 8 月 10 日，精工公司曾发布了一份数据泄露通知，通知称未经授权的第三方获得了对其 IT 基础设施至少是部分的访问权限，并可能窃取了内部数据。精工的声明中写道：“似乎在 2023 年 7 月 28 日，一股身份不明的团体在未经授权的情况下获得了对我们至少一台服务器的访问权限。”……“随后的 8 月 2 日，我们委托外部网络安全专家团队对情况进行调查和评估。”……“因此，我们现在可以合理地确定存在被入侵的情况，并且我们公司及集团公司存储的一些信息可能已遭到泄露。”据此，精工向可能受影响的客户及业务合作伙伴道歉，并敦促他们警惕可能冒充精工的电子邮件或其他信息。

而在 8 月 21 日，BlackCat 勒索软件组织声称是精工遭到攻击事件的幕后黑手，并发布了他们声称在攻击期间窃取到的数据样本。在发布页中，攻击者一并嘲笑了精工的 IT 安全性，并泄露了疑似是生产计划、员工护照扫描件、新型号发布计划和专项实验室测试结果等内容。最令人担忧的是，攻击者泄露了他们声称是机密技术原理图和精工手表设计的数据样本。

目前，精工方面尚未对当前发生的数据泄露事件发表回应。

黑客信息披露

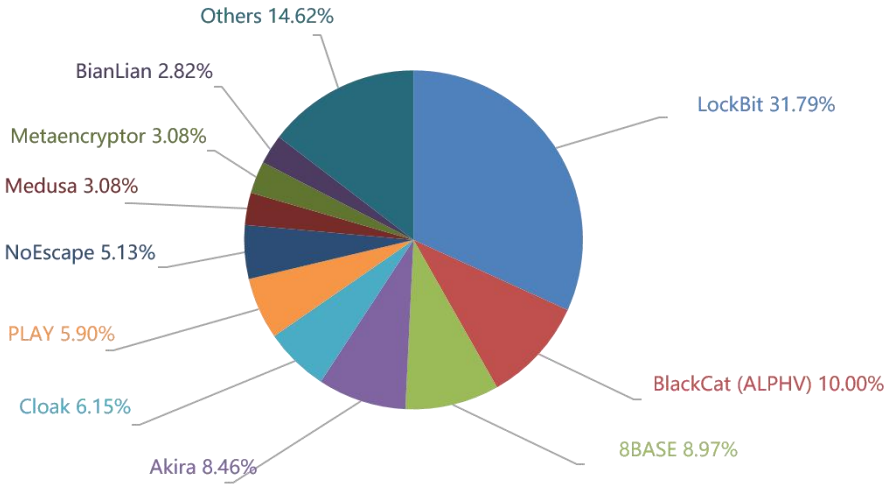
以下是本月收集到的黑客邮箱信息：

nztz@tuta.io	bob1997marley@firemail.cc	decvvv110@tutanota.com
datukraine@tuta.io	bob1997marley@zohomail.eu	criptor@tutanota.com
datukr@onionmail.org	cris_nickson@xmpp.jp	bitencrypt@mailfence.com
kazinbekdutch@tutanota.com	piltecheesig1973@protonmail.com	bkpsvr@firemail.cc
kazinbekdutch@cock.li	NoLock@keemail.me	pcsupport@skiff.com
kazinbekdutch@protonmail.com	NoLock@mailfence.com	pctalk01@tutanota.com
BM-2cT72URgs1AWGV6Wy6KBu2yuj3ychN5vxC@bitmessage.ch	WoundedOwl@onionmail.org	legion@tfwno.gf
krize@onionmail.com	WoundedOwl@cyberfear.com	henderson@cock.li
globalkrize@proton.me	leejohn@inboxhub.net	myfile@waifu.com
support.antimalware@onionmail.com	leejohn@cryptolab.net	shonpen@mailfence.com
upport.antimalware@msgden.com	network@outlookpro.net	taxasfshwkasjfbuwbsja@protonmail.com
haymaker@qq.com	networks@onionmail.org	a_princ@aol.com
medusa.support@onionmail.org	mallox.ressurection@onionmail.org	help@assistrecovery.pw
aisaragpt@tuta.io	RealWorld44@Tutanota.com	unrasolo1970@proton.me
aisaragpt@proton.me	MerlinWebster@aol.com	solo@proton.me
toridastford@zohomail.com	topcorp@usa.com	teodorcarrida@tuta.io
LettoIntago@onionmail.org	topcorp24@mail.com	cybcyb123@tutanota.com

protec5@onionmail.org	freeworld7001@gmail.com	3cfxg@onionmail.org
goodwork2020@mailfence.com	decrypt2023@cock.li	quvn5llxk@mailfence.com
protonis2023@tuta.io	decrypt2023@cyberfear.com	emcrvpts@msgsafe.io
DoraRec@onionmail.org	ware_house@tuta.io	helpsendmemessage@xmpp.jp
DoraRec@msgsafe.io	exezez@blaze420.it	duan77194@tutanota.com
Kigatsu@onionmail.com	helze@cyberfear.com	acbc@tutanota com
Kigatsu@mailo.com	exezaz@msgden.com	datasecurity@cock.li
helpbit911@onionmail.org	bkpsvr@proxy.tg	decrypt.tm@zohomail.eu
helpbit911@tuta.io	petinjon@vpn.tg	protonis@skiff.com
blackhathacker234@proton.me	petinjon@gmail.com	zinok19899@tuta.io
alvarodecrypt@gmail.com	darkflare@mailfence.com	filerecorder@hotmail.com
alvarodecrypt@outlook.com	helper2023@onionmail.org	theniklaus@cyberfear.com
iamaduck7@onionmail.org	dontcrylol@mailfence.com	tjjc110@outlook.com
mastadonster@onionmail.org	drdecrypt@onionmail.org	decryptor@cyberfear.com
54783@thesecure.biz	cryptrd@msgsafe.io	briandatahelp@onionmail.org
Decepticon@cock.li	crypjo@mailfence.com	briandatahelp@dnmx.org
test@test.com	OnionRansom@Tutanota.com	ffreefix@outlook.com
back2up@swismail.com	OnionRansom@Decoymail.com	chinahelp2023@nigge.ns
sunsunteam@tuta.io	shotgune@onionmail.org	incomings99112@onionmail.com
sunsunteam@jabb.im	shotgune@mailfence.com	sourcehack@nigge.rs
datastore@cyberfear.com	suppdecrypt@onionmail.com	arsupp@tutanota.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，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 390 个组织/企业遭遇勒索攻击，其中包含中国 5 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 9 个组织/企业未被标明，因此不再以下表格中。

chevalerias.com	deschamps.fr	guyer.com.uy
vodatech.com.tr	mayair.com.my	abzarsara.com
Valley Mountain Regional Center	Pifer's Auction & Realty	Tisher Liner FC Law Australia
Wilder & Co	Alpizar Law Firm	Eckell Sparks Attorneys at Law
millwgs.com	biso.at	syntech.com.sg
Fenn Termite and Pest Control	antioch.edu	Fenn Termite & Pest Control
zep.it	skystar.it	tlip2.com
rydershealth.com	greensboro.edu	mariocoelho.com
alpepipesystems.com	losh.com	grebe-korbach.de
optoflux.com	feuille-erable.fr	nieul-sur-mer.fr
tavlit.co.il	dollinger-pierre.fr	annals.edu.sg
inouemfg.com	potenciamaquinaria.com	locaparc.fr
auto-pieces.fr	guillerm-habitat.fr	acolea.org
otltd.co.uk	emec.com.eg	texline-global.com
O'Brien Steel Service	Renton School District	Aranui Cruises
Skynet	Felling Trailers, Inc.	Brooklyn Premier Orthopedics
lhvisionclinic.com	PRIDE GLOBAL CONSULTING SL	Petkus Brothers
Pasquale Bruni Ltd	Ningbo Yinzhou Vocational High School	uprepschool.org
sherwin-electric.com	beniculturali.it	jamaicainn.com
wkclawfirm.com	greenside-sch.org	casa-andina.com
renaultinantwerpen.be	ukseung.co.kr	cloverbrook.com
carolfoxassociates.com	mergerecords.com	fimadev.fr
immoselekt.be	distribuidoradavidsa.com	cm.gov.nc.tr
younghomes.com	Forsyth County, GA	Jacklett Construction LLC
PT. Cahaya Benteng Mas	esprigas.com	University of the West of Scotland
persingerlaw.com	Kendrion.com	Pierce College
PSM	QI Holdings Ltd.	Iina Ba Inc
Cutler-Smith, P.C.	Jasper High School	Penny Publications
Divvies	Voss Enterprises	Intertek
Superior Communications	Asian Network Pacific Home Care & Hospice	GYP New Tree SA
Prince George's County Public Schools	State Farm	S&P
Metropolitan Club DC	grupomartex.com	jhilburn.com
purever.com	Shanghai FRP Research Institute Co., Ltd.	Fullerton India (SMFG India Credit)

Community Council of South Central Texas	Gujarat Industries Power Company Ltd.	SKYROOT
Varna Packaging	KLM Laboratories Pvt. Ltd	Argus Fluidhandling Ltd
Alfagomma	Trimaran Capital Partners	Demcointer
EPF	LEN Italia	Durham Fasteners
Axis Elevators	HFH Capital	Community Action
INSTITUTO NACIONAL DE ELECTRIFICACION	FA Foundry	Sydenham Laboratories
Fiocruz	senacrs.com.br	Edmonds School District
Storm Tight Windows	Groupe Marchand Architecture & Design Inc	Bahamas Medical and Surgical Supplies
Ontellus	MBS Equipment TTI	Pea River Electric Cooperative
Constellation Kidney Group	Hoosick Falls Central School District	Royal Oak Pet Clinic
Mil-Ken Travel	Kevills Solicitors	The Law Offices of Steven H. Heisler
Bahamas Medical & Surgical Supplies	Arus-gmbh	Sportlab-srl
BONI-PASSAU.DE	lusis-avocats.com	werk33.com
GRIDINSTALLERS.com	surapon.com	mps-24.com
gruppomoba.com	stshcpa.com.tw	ihopmexico.com
Nicer technology	binhamoodah.ae	first-resources-ltd
Sbs-Berlin	imtmro.com	INCOBEC
still95.it	gsh-cargo.com	flamewarestudios.com
ALEZZELPOWER.com	Notaires.fr	Sonabhy.bf
KVFCU.ORG	Prospect Medical Holdings	qintess.com
iledefrance-nature.fr	newsupri.com.br	decrolyamericano.edu.gt
mcnamaradrass.com	Transunion	Jhookers
I&G Broker House	A1	Optimity
gerb.bg	IMS Computer Solutions	Atlantic Federal Credit Union
NE-BIC	Heidelberg Materials	FYTISA Industrial Felts and FabricsSL
Softverg Co., Ltd.	Infuance Communication Inc	Department of Defence South African (DARPA)
apdparcel.com.au	TRIUNE TECHNOFAB PRIVATE LIMITED	Davidoff Hutcher & Citron
Seiko Group Corporation	stockwellharris.com	equip-reuse.com
cochraninc.com	cloudtopoffice.com	hallbergengineering.com
Novi Pazar put ad	The International Civil Defense Organization	Sartrouville France
Econocom	Gold Medal Bakery	s3groupltd.com
macuspana.gob.mx	phitoformulas.com.br	National Institute of Social Services for Retirees and Pensioners
Municipality of Ferrara	ABS Auto Auctions	DSA Law Pty Ltd
Miami Management	BTC Power	Stanford Transportation Inc
Bolton Group	Legends Limousine	Oneonline
gh2.com	au Domain Administration Ltd	Dillon Supply
Epicure	Coswell	BOB Automotive Group

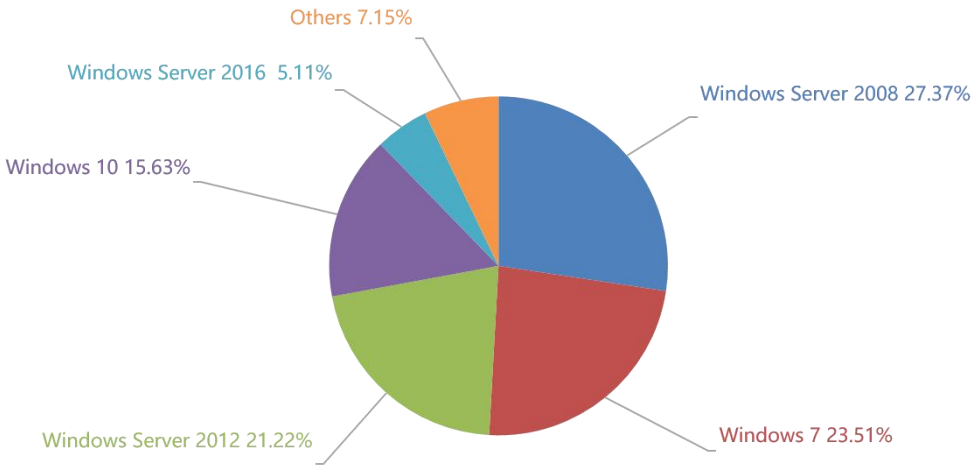
Seoul Semiconductor	Kraiburg Austria GmbH	Autohaus Ebert GmbH
CVO Antwerpen	ICON Creative Studio	Heilmann Gruppe
Schwälbchen Molkerei AG	Münchner Verlagsgruppe GmbH	Contact 121 Pty Ltd
umchealth.com	sgl.co.th	RIMSS
Pemberton Fabricators, Inc	ALLIANCE	DEUTSCHELEASING
VDVEN	SYNQUESTLABS	TWINTOWER
The Clifton Public Schools	Camino Nuevo Charter Academy	kriegerklatt.com
SFJAZZ.ORG	mybps.us	Smart-swgcrc.org
MBO-PPS.COM	MBOAMERICA.COM	KOMORI.COM
Cequint	Tally Energy Services	CORDELLCORDELL
Optimum Health Solutions	Hemmink	Tennis Canada
Ramtha	ToyotaLift Northeast	FTRIA CO. LTD
Recaro	Postel SpA	ABA Research
Keystone Insurance Services	ANS	Aspect Structural Engineers
Fondation De Verdeil	Freeport-McMoran	jhillburn.com
qbcqatar.com.qa	leecorpinc.com	John L Lowery & Associates
Federal Bar Association	econsult.com	Saint Xavier University
Agriloja.pt	CB Energy Australlia	Borets
luterkort.se	majan.com	zaun.co.uk
rappenglitz.de	siampremier.co.th	roxcel.com.tr
meaf.com	stmarysschool.co.za	difccourts.ae
Armortex	Don's Mobile Glass	arganoInterRel
Rite Technology	zain.com	Top Light
Algorry Zappia & Associates	EAI	The Belt Railway Company of Chicago
Optimum Technology	Boson	United Tractors
Stockdale Podiatry	oneatlas.com	Lower Yukon School District
Thermenhotel Stoiser	sekuro.com.tr	asfcustomers.com
TIMECO	csem.qc.ca	octoso.de
ricks-motorcycles.com	janus-engineering.com	fashions-uk.com
cbcstjohns.co.za	el-cerrito.org	chula.ac.th
etisaleg.com	2plan.com	unitycouncil.org
independenceia.org	Batesville	ZESA Holdings
Magic Micro Computers	Emerson School District	CH informatica
Thonburi Energy Storage Systems (TESM)	Räddningstjänsten Västra Blekinge	G***** *******
KIMCO Staffing Service	Avertronics Inc	Republican Vilnius Psychiatric Hospital
Kreacta	Papel Prensa SA	varian.com
Delaney Browne Recruitment	IBL	premierbpo.com
Sports Medicine Oregon	SatCom Marketing	Rayden Solicitors
haynesintl.com	Henlaw	atser.com
Galicia en Goles	scottevest.com	mipe.com
armortex.com	iqcontrols.com	tetco.com
P****X	Zurvita	SBS Construction

Koury Engineering	Pharmatech Repblica Dominicana	Grupo Garza Ponce
ESKA Erich Schweizer	Studio Domaine LLC	Ofimedic
THECHANGE	Abatti Companies	HealthIndia TPA Services Pvt Ltd
Spokane Spinal Sports Care Clinic	pointpleasant.k12.nj.us	Roman Catholic Diocese of Albany
Venture General Agency	Datawatch Systems	INSULCANA CONTRACTING LTD
admsc.com	riggsabney	RevZero, Inc
Rossman Realty Group, inc.	Tempur Sealy International	bestmotel.de
constructioncrd.com	Helen F. Dalton Lawyers	Grupo SCA
TGRWA	Guido	Optical Cable Corporation
Burmeister & Wain Scandinavian Contractor	Bickel & Brewer	COSI
ohiohistory.org	University of Salerno	unicorpusa.com
SHERMAN.EDU	Garage Living	Aapd
Birch, Horton, Bittner & Cherot	DAL-TECH Engineering	The Dispenser USA
Coral Resort	Professionnel France	ACTIVA Group
Aquatlantis	Parathon by JDA eHealth Systems	Ultimus

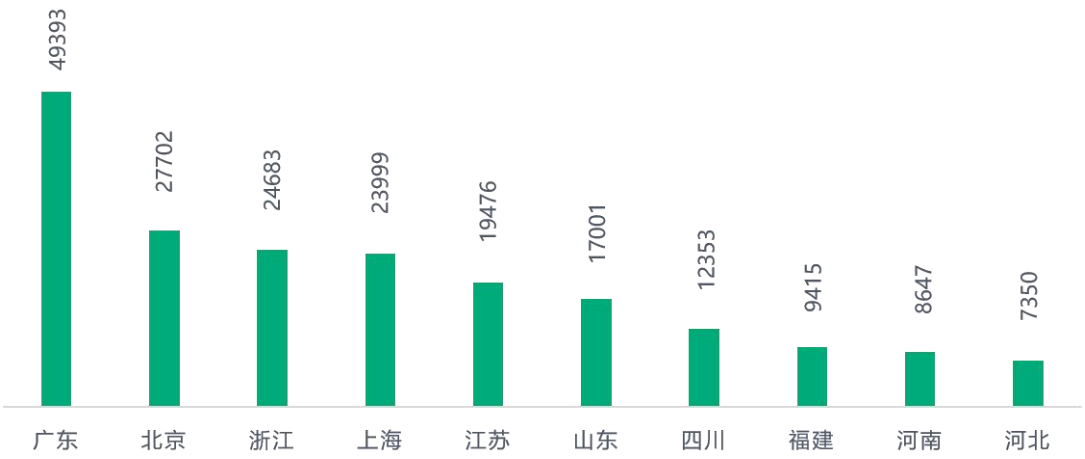
表格 2. 受害组织/企业

系统安全防护数据分析

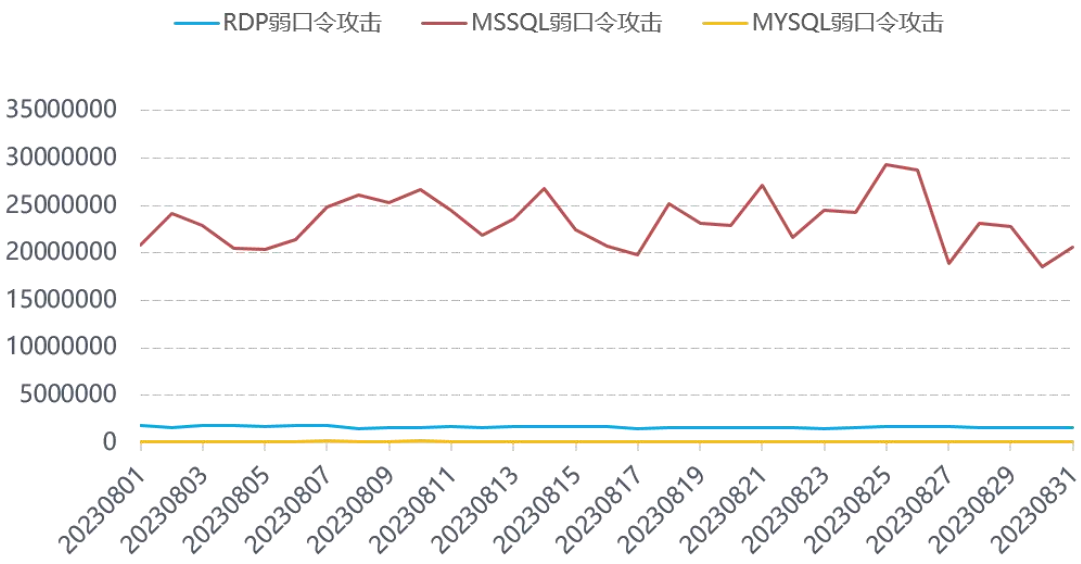
360 系统安全产品，目前已加入黑客入侵防护功能。在本月被攻击的系统版本中，排行前三的依次为 Windows Server 2008、Windows 7 以及 Windows Server 2012。



对 2023 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 2023 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。

- 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。

- 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。

- halo：同 360。

- 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。

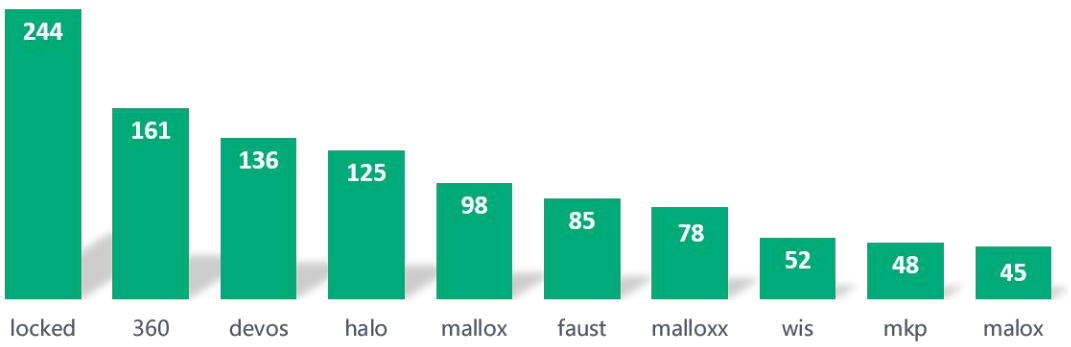
- faust：同 devos。

- malloxx：同 mallox。

- wis：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。

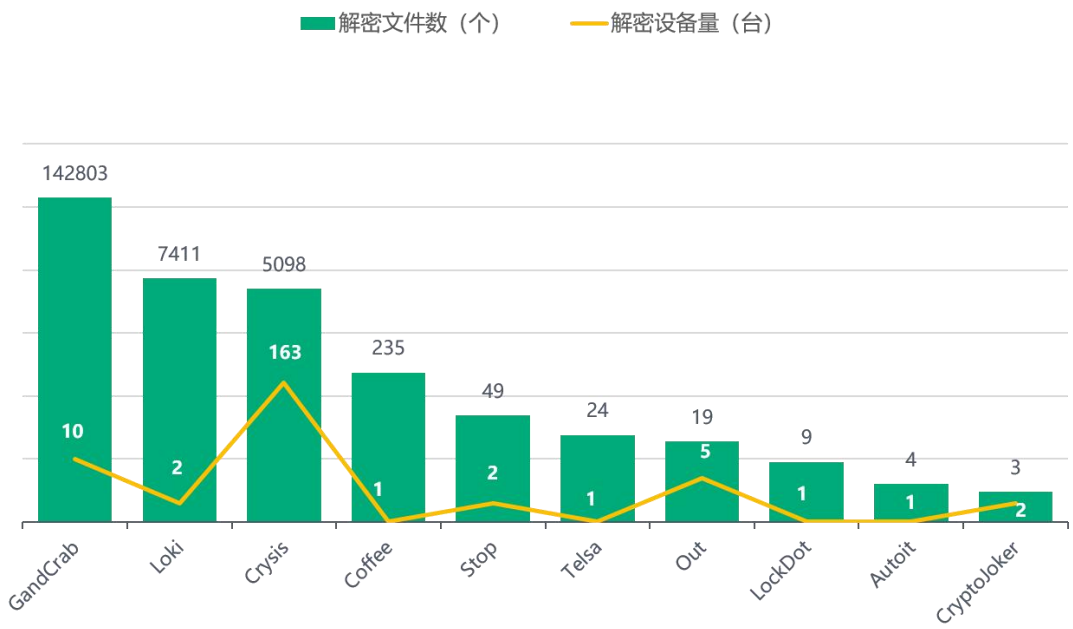
- mkp：同 wis。

- malox：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 GandCrab，其次是 Loki。使用解密大师解密文件的用户数量最高的是被 Crysis 家族加密的设备。




360数字安全
数 字 安 全 的 领 导 者