勒索软件流行态势分析

2023 年 9 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 9 月，全球新增的活跃勒索软件家族有 ThreeAM、Knight、CiphBit、LostTrust 等家族。

以下是本月值的关注的部分热点：

1. Cisco 警告称其 VPN 的 0day 漏洞被勒索软件团伙利用

2. 凯撒娱乐确认因客户数据被盗而向勒索软件支付赎金

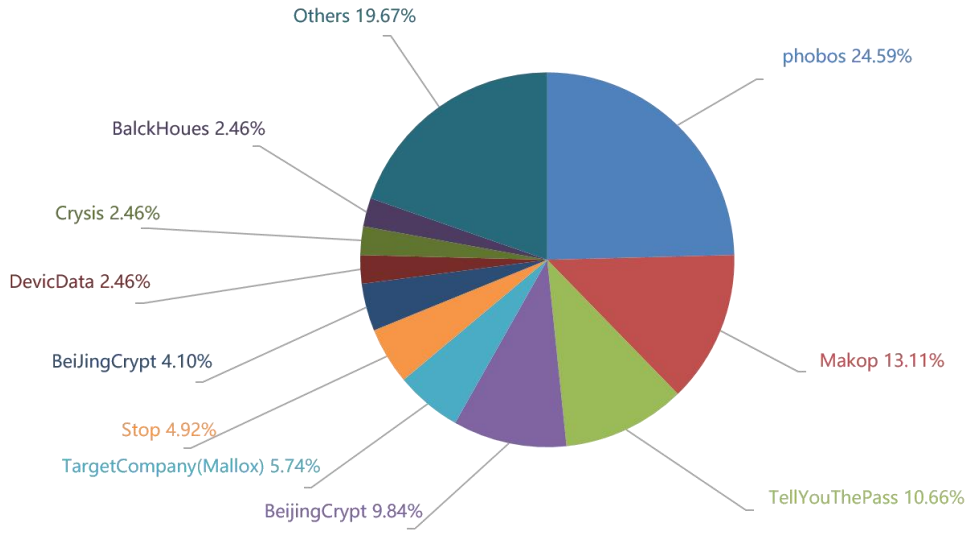
3. 黑客积极利用 Openfire 漏洞来加密服务器

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。

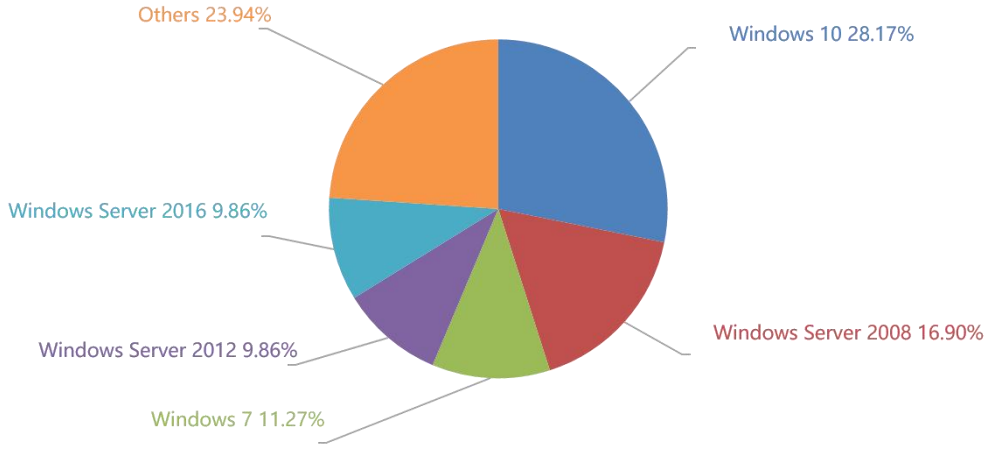
感染数据分析

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 24.59%居首位，第二的是占比 13.11%的 Makop，TellYouThePass 家族以 15.38%位居第三。

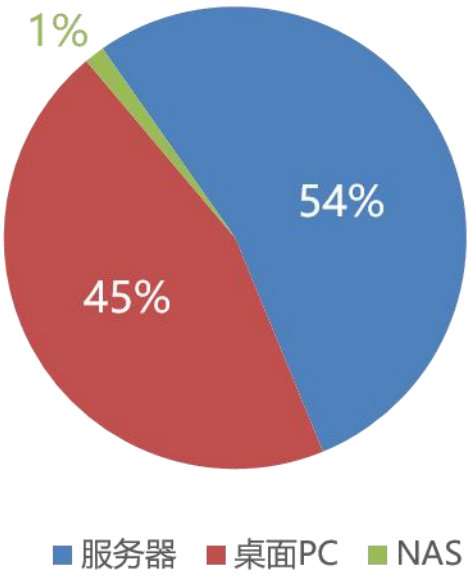
其中位居第三的 TellYouThePass 持续通过 web 漏洞利用发动攻击。



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 7。



2023 年 9 月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型占比基本相当，偶有 NAS 平台感染。



勒索软件热点事件

Cisco 警告称其 VPN 的 0day 漏洞被勒索软件团伙利用

思科警告称，思科自适应安全设备(ASA)和思科 Firepower 威胁防御系统(FTD)中存在编号为 CVE-2023-20269 的 0day 漏洞，而勒索软件组织会利用该漏洞来获取对企业网络的访问权限。该漏洞允许未经授权的远程攻击者对现有帐户进行暴力攻击。通过访问这些帐户，攻击者可以在受攻击的网络中建立无客户端的 SSL VPN 会话，而根据受害者的具体网络配置差异这一攻击也会产生不同级别的威胁。

在今年 8 月，就有报道称 Akira 勒索软件团伙利用 Cisco VPN 设备的未知漏洞入侵企业网络。在这次攻击发生的一周后，Rapid7 报告称除了 Akira 之外，Lockbit 勒索软件也利用了 Cisco VPN 设备的安全漏洞。9 月初，思科确认了这些勒索软件团伙利用的 0day 漏洞的存在，并在临时安全公告中提供了解决方法。但目前尚未发布受漏洞影响的产品的安全更新。

香港数码港遭勒索攻击致 400GB 数据泄露

安全内参 9 月 8 日消息，香港科创中心数码港已就网络安全漏洞向警方和香港隐私监管机构上报。勒索软件组织 Trigona 声称，已从数码港窃取超过 400GB 数据，要求支付 30 万美元（约合港币 235 万元）才能归还。

周四，一位 IT 专家查阅了暗网相关材料，发现包括银行账户信息和身份证复印件在内的被窃数据正在竞价售卖，起价定为 30 万美元。

香港网络安全公司 VX Research 的安全专家 Anthony Lai Cheuk-tung 分析称，“假设一个人的信息是 1GB，那就至少有 400 名受害者。”

数码港商业园区有 140 名员工，是 1900 家初创企业和科技公司的运营基地。警方表示，已将此案移交网络安全及科技罪案调查科进行调查，目前尚未有人被捕。

数码港在周三发布声明，谴责未经授权的第三方攻击者入侵其部分计算机系统，并表示他们在发现入侵后迅速采取了行动。但是，声明并未点出谁是可能的肇事者。

凯撒娱乐确认因客户数据被盗而向勒索软件支付赎金

美国最大的赌场连锁品牌凯撒娱乐表示：为避免近期的一次网络攻击中遭窃取的客户数据在网上泄露，该公司已向黑客支付了赎金。

凯撒娱乐于 9 月 7 日发现有攻击者窃取了其“忠诚度计划”数据库，该数据库中存储了许多客户的驾照号码和社会安全号码。在凯撒娱乐向美国证券交易委员会提交的一份 8-K 表格中显示：“我们仍在调查攻击者获得的文件中包含的敏感信息的范围。”……“到目前为止，没有证据表明任何会员的密码/PIN 码、银行账户信息或支付卡信息（PCI）已被攻击者获取。”

此外，表格内容中还暗示向攻击者支付赎金是为了防止被盗数据在网上泄露。据媒体透露，该娱乐公司支付了大约 1500 万美元的赎金，这一金额大约是攻击者最初索要的 3000 万美元的一半。尽管如此，凯撒明确表示，它无法就“应对事件负责的攻击者”的潜在行动提供任何保证，包括他们仍可能出售或泄露客户被盗信息的可能性。

黑客积极利用 Openfire 漏洞来加密服务器

黑客正在积极利用 Openfire 的消息传递服务器中的一个高严重性漏洞传播勒索软件用以加密服务器并部署加密挖矿程序。

Openfire 是一种被广泛使用的基于 Java 的开源聊天服务器，此次被利用的漏洞编号为 CVE-2023-32315，是一种影响 Openfire 管理控制台的身份验证绕过方式，该漏洞允许未经身份验证的攻击者在易受攻击的服务器上创建新的管理员帐户。攻击者通常使用这些帐户安装恶意 Java 插件。

该漏洞影响几乎所有当前主流的 Openfire 版本，从 3.10.0 到 4.6.7，以及 4.7.x 中的 4.7.0 到 4.7.4 版本。尽管 Openfire 在 5 月发布的版本 4.6.8、4.7.5 以及最新的 4.8.0 中修复了该问题，根据统计：到 8 月中旬，仍有超过 3000 台 Openfire 服务器仍运行着易受攻击的版本。

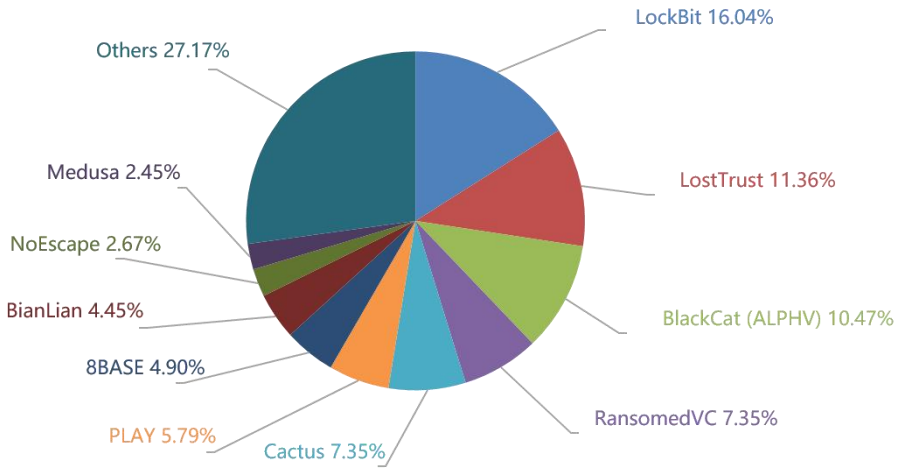
黑客信息披露

以下是本月收集到的黑客邮箱信息：

henderson@cock.li	decryptor@cyberfear.com	mpfiledec@msgsafe.io
ihavenobackup@gmail.com	anna.brown.la.ca@gmail.com	infohelper@onionmail.com
911files@onionmail.org	f3d0r4@proton.me	fileassistant@proton.me
Django@onionmail.org	dectokyo@onionmail.org	savetime@cyberfear.com
Django23@msgsafe.io	dectokyo@cock.li	savetime4u@outlook.com
vilisol@msgsafe.io	DataLock@onionmail.org	EldritchTeam@proton.me
vilisol@tutanota.com	datalocked@nerdmail.co	wang_fang@zohomail.com
recoveryanti@gmail.com	Blackbit_sup@mailfence.com	wang.fang@onionmail.org
ransupport@onionmail.org	blackbit.sup@onionmail.org	nowil24701@armablog.com
protexdamaraij5@gmx.de	azadibtc1@elizamail.site	cryptonic@onionmail.org
shonpen@mailfence.com	azadi3@keemail.me	captain-america@tuta.io
decryptmenow@onionmail.org	Zero.Cool2000@onionmail.org	cyber34229@gmail.com
helpdecrypt@dnmx.org	Zero.Cool2000@skiff.com	malloxxhelp@cock.li
datacentreback@msgsafe.io	Eliberansmoware@outlook.com	malloxxhelp@proton.me
moriartydata@onionmail.org	recoveryfile7@gmail.com	Recoverifiles@gmail.com
submarine@cyberfear.com	reopenran2023@firemail.de	Recoverifiles@protonmail.com
submarine2@cyberfear.com	backbackup@onionmail.org	nightcrowsupport@protonmail.com
vpsadminmain12@onionmail.org	databackup@msgsafe.io	venolockdate1@rape.lol
vpsadminmain13@onionmail.org	edcvbghjikm@protonmail.com	Alexdec23@aol.com
loki@decoperator.org	decryption38@gmail.com	Alexdec23@cock.li
decoperator@cock.li	decryption38@gmail.com	gotis@tuta.io
deep_77@tutanota.com	exezez@420blaze.it	gotis@onionmail.org
cp00pc1@proton.me	dompio@privatemail.com	returnback@cyberfear.com
datarecoverycenterOPG@onionmail.org	dompio@msgsafe.io	returnbac@onionmail.org
datarecoverycenterOPG2023@onionmail.org	recoverybpanther@proton.me	ithelp15@yousheltered.com
balckhoues@onionmail.com	fixfilesystemhelpers@mail.ee	electronicrans@gmail.com
balckhoues@tutanota.com	fixfilesystemhelpers@onionmail.org	electronicrans@outlook.com
bitsupport@onionmail.org	mpfile_dec@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 449 个组织/企业遭遇勒索攻击，其中包含中国 7 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 19 个组织/企业未被标明，因此不再以下表格中。

Betton France	Smead	Saint Mark Catholic Church
Jules B	clearwaterlandscape.com	WEBBER RESTAURANT GROUP
VV&A	MGM Resorts International	Pond Security
Prodegest Assessors	etsi.uy	SUD TRADING COMPANY
marianoshoes.com	American Steel & Aluminum Co., Inc.	ZZColdstores
gosslaw.com	Ja Quith	NTT Docomo
Arkopharma	East Baking	Nusmiles Hospital
DDB Unlimited	carthagehospital.com	Ministry Of Finance (Kuwait)
Rick Ramos Law	Fondation Vincent De Paul	Praxis Arndt und Langer
Riverside Logistics	EDUCAL, SA de CV	PRETZEL-STOUFFER
Estes Design & Manufacturing	EnPOS	J.T. Cullen Co., Inc.
Aiphone	Harmonic Accounting	Springer Eubank
Newton Media A.S.	Imperador S.R.L	MNGI Digestive Health
phms.com.au	Waterford Retirement Residence	epson.es
paynesvilleareainsurance.com	Shelly Engineering Metal Work	altmanplants.com
SKF.com	RSV Centrale Bvba	SONY.COM
Lawsonlundell	Soprovise	Phil-Data Business Systems

TissuPath Australia	clearcreek.org	bnm.bg
Strata Plan Australia	Dpc & S	mango.bg
glprop.com	Carpet One	ebag.bg
Barry Plant Real Estate Australia	Elwema Automotive	popolo.bg
ramlowstein.com	Tanachira Group	andrews.bg
scottpartners.com	Solano-Napa Pet Emergency Clinic	ardes.bg
nerolac.com	Morgan Smith Industries LLC	myshoes.bg
seasonsdarlingharbour.com.au	Decarie Motors Inc	ecco.bg
neolife.com	Financial Services Commission	districtshoes.bg
sterncoengineers.com	Accuride	footshop.bg
attorneydanwinder.com	SAC Finance	Punto.bg
designlink.us	Abbeyfield	arelion.com
dasholding.ae	M-Extend / MANIP	Clarion
DOIT	sinloc.com	interep.com.br
Statefarm.com	BF&S Civil Engineers	Franktronics, Inc
SKF.com	Dee Sign	Philippine Health Insurance
Powersportsmarketing.com	Credifiel	FabricATE Engineering
Taylor University	Derrimon Trading	The Envelope Works Ltd
cc-gorgesardeche.fr	Alps Alpine	Ort Harmelin College of Engineering
Rs Logistics Ltd	CORTEL Technologies	marshallindtech.com
GORDON, MUIR & FOLEY LLP	International Joint Commission	precisionpractice.com
cciamp.com	AdSage Technology Co., Ltd.	CLX Logistics
Lutheran Church and Preschool	deeroaks.com	Agilitas IT Solutions Limited
Templeman Consulting Group Inc	Altmann Dental GmbH & Co KG	Progressive Leasing
Firmdale Hotels	Cmranallolaw.com	Pik Rite
Hawaii Health System	Wardlaw Claims Service	COMECA Group
hamilton-techservices.com	Unimarketing	Carlo Ditta
aquinas.qld.edu.au	Leekes	SK Accountants & Tax Consultants
konkconsulting.com	My Insurance Broker	SPEC Engineering
Piex Group	ZILLI	Jersey College
Israel Medical Center	Florida Department of Veterans' Affairs	JSM Group
I Keating Furniture World	CITIZEN	Key Construction
It4 Solutions Robras	First Line	Leiblein & Kollegen Steuerberatungsgesellschaft
Ayass BioScience	Rea Magnet Wire	Liberty Lines
Energy One	RTA	LoopLoc
FRESH TASTE PRODUCE USA AND ASSOCIATES INC.	TSC	Reload SPA
Chula Vista Electric (CVE)	PASCHAL - Werk G Maier	Ananda Temple
Precisely	Vucke	Omniatel
Kikkerland Design	Fuji Seal International	Paradise Custom Kitchens
Markentrainer Werbeagentur	Glovis America	The WorkPlace
Winshuttle	Elemetal	Professional Moving Company - Mackie

		Group
Master Interiors	Hoteles Xcaret	Mexican Government
Bordelon Marine	Grupo Boreal	Central Trenching
Majestic Spice	Lopez & Associates Inc	Immanuel Christian School
Infinity Construction Company	Auckland Transport	Cullum Services
Seymours	Araújo e Policastro Advogados	Gold Coin Restaurant
Promotrans	Retail House	Marlboro Township Public School
MINEMAN Systems	Delta Group	Carmocal
Maxxd Trailers	TransTerra	Johnson Boiler Works
Marfrig Global Foods	Marston Domsel	EnCom Polymers
Treadwell, Tamplin & Company, Certified Public Accountants, Madison, GA	faithfamilyacademy.org	Ambrosini Holding
Flamingo Holland	piramidal.com.br	Colors Dress
Aria Care Partners	commercialfluidpower.com	THEATER LEAGUE INC
Cedar Holdings	ipsenlogistics.com	GI Medical Services
Unimed	glat.zapweb.co.il	Gordon Law Firm
Cyberport	michalovich.co.il	Contraband Control Specialists
Lagarde Meregnani	motsaot.co.il	I&Y Senior Care
Hornsyld Købmandsgaard	gsaenz.com.mx	EWBizservice
Foroni SPA	eljayoil.com	Center Township Trustee
Barsco	energyinsight.co.za	Garlick & Markison
spmblaw.com	mehmetceylanyapi.com.tr	Double V Construction
godbeylaw.com	aeroportlleida.cat	Swann's Furniture & Design
wantager.com	lamaisonmercier.com	Gateseven Media Group
easydentalcare.us	neolaser.es	Asia Vegetable
quantinuum.com	perfectlaw.com	Carnelutti Law Firm
laasr.eu	milbermakris.com	Foundation Professionals of Florida
medcenter-tambov.ru	FinDec	Acoustic Center
makflix.eu	gov.la	Siamese Asset
nucleus.live	pelicanwoodcliff.com	GCserv.com
Mulkay Cardiology Consultants	hillsboroughschools.org	Orthum Bau
HBME LLC	hollandspecial	Astro Lighting
Northwave s.r.l.	St Margaret's Prep	Prestige Care
Barco Uniforms	SMWLLC.COM	Nordic Security Services
Balcan	Steelforce	Woody Anderson Ford
Swipe.bg	wdgroup.com.my	BestPack Packaging
Balmit Bulgaria	pvbfabs.com	Istituto Prosperius
Knight Barry Title	intechims.com	Network Pacific Real Estate - Leak
cdwg.com	zero-pointorganics.com	Astre - Leaked
Levine Bagade Han	visitingphysiciansnetwork.com	Motel One
cfsigroup.ca	pelmorex.com	INC RANSOMWARE...
KUITS Solicitors	Yusen Logistics	MNGI Digestive Health (TIME IS UP)
Wave Hill	Hospice of Huntington	mclaren health care

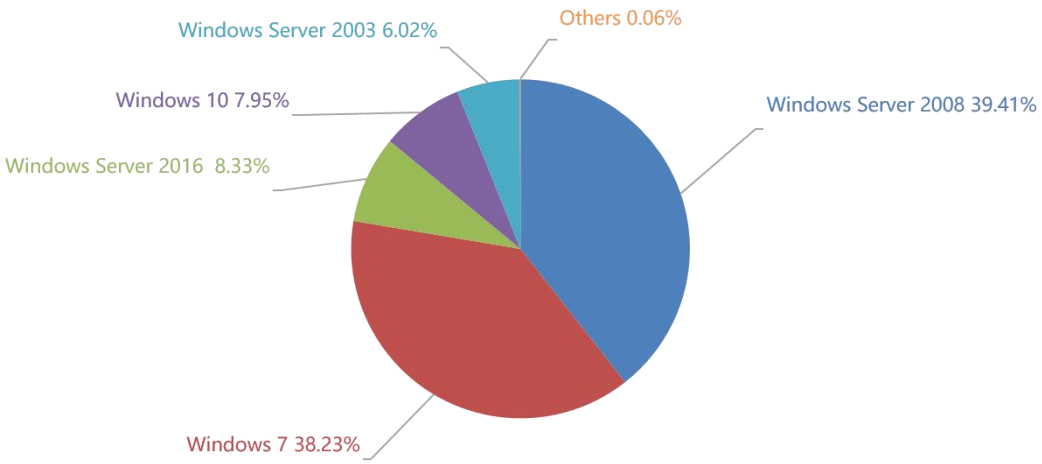
Steripharma	Yakima Valley Radiology	palaciodosleiloes.com.br
co.grant.mn.us	haciendazorita.com	New data leak. IT company from California
Ford Covesa	fi-tech.com	solveindustrial.com
Linktera	Holon Institute of Technology	Garn Mason Orthodontics was hacked. All insurance and personal data of customers was stolen
airelec.bg	neuraxpharm.com	Belzona UK Ltd
pilini.bg	PainCare	Andalusia Group
kasida.bg	TAOGLAS	MNGI Digestive Health
proxy-sale.com	Auckland University of Technology	C.F. Service and Supply
Core Desktop	ruko.de	C.F. Service & Supply
Singing River Health System	Mole Valley Farmers	Kona Equity
Kirby Risk	ende.co.ao	!!!WARNING!!!
IT-Center Syd	Cosal	Robuck Homes
Low Keng Huat	Unique Engineering	Webb Landscape
sd69.org	Arail	Amanzi Marble & Granite
monaco-technologies.com	Stratesys solutions	BAMO
UNIVERSAL REALTY GROUP	Road Safety	Van Eck Transport
Geo Tek	Smartfren Telecom	Terralogic
hanwha.com	DM Civil	Kessler Collins
JSS Almonds	Hawkins Delafield Wood	Plumbase
BRiC Partnership	NOVEXCO	Wexas
Custom Powder Systems	Radley and Co	fdf.org.uk
atWork Office Furniture	messner.com	ezpaybuildings.net
PAUL-ALEXANDRE DOICESCO	compass-inc.com	rexgroup.co.uk
WACOAL	bauscherhepp.com	Jacobsen Construction
24/7 Express Logistics	constantinecannon.com	simmonsequip.com
PetroVietnam Metallic Structures & Erection Joint Stock Company (PVC-MS)	Chait	Hochschule Furtwangen University
Chambersburg Area School District	Gulf American Lines	Notel
FOCUS Business Solutions	Leoch Battery	UTC Overseas
toua.net	hwwealth.com	Unitex Textile Rental Services
Omniatel	Federal Labor Relations Authority	Muenz-Engineered Sales
Conselho Superior da Justiça do Trabalho	ENTRUST Solutions Group	Arazoza Brothers
Kramer Tree Specialists, Inc	Spuncast	Popovici Niu Stoica & Asociaii
Sebata Holdings (MICROmega Holdings)	Bacon Universal	Procab
West Craft Manufacturing	payrollselectservices.com	Hoosier Uplands Economic Development
Trimaran Capital Partners	Portesa	Oasys Technologies
TORMAX USA	Al Ashram Contracting	Merced City School District
Specialised Management Services	University Obrany	Morgan School District
ragasa.com.mx	fersan.com.tr	Ferguson Wellman
qsoftnet.com	Groupe Fructa Partner	TORMAX
protosign.it	American University of Antigua	Brown and Streza

concrejato.com.br	Agilitas IT Solutions Limited	Bit
meroso.be	Gossler, Gobert & Wolters Group.	Glassline
nobleweb.com	Peacock Bros	SydganCorp
gormanusa.com	Hacketts printing services	CEFCO
onyx-fire.com		

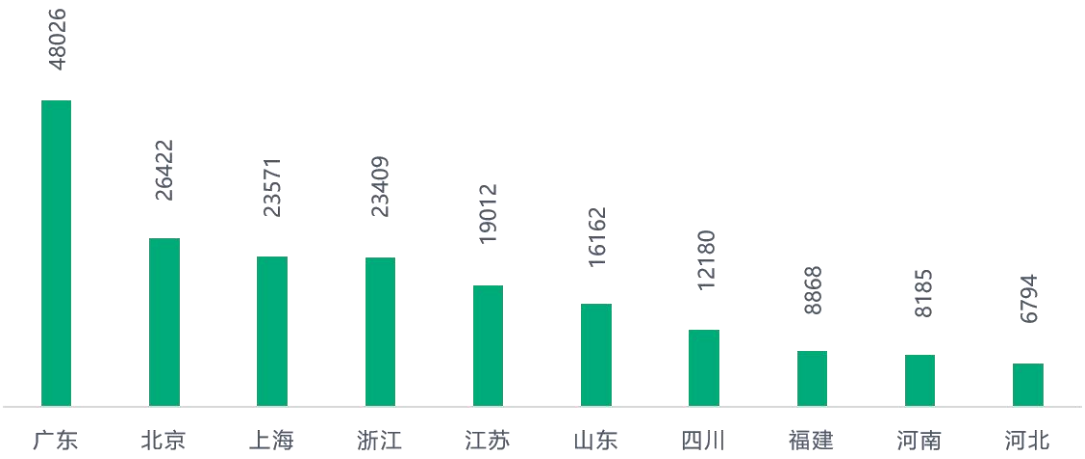
表格 2. 受害组织/企业

系统安全防护数据分析

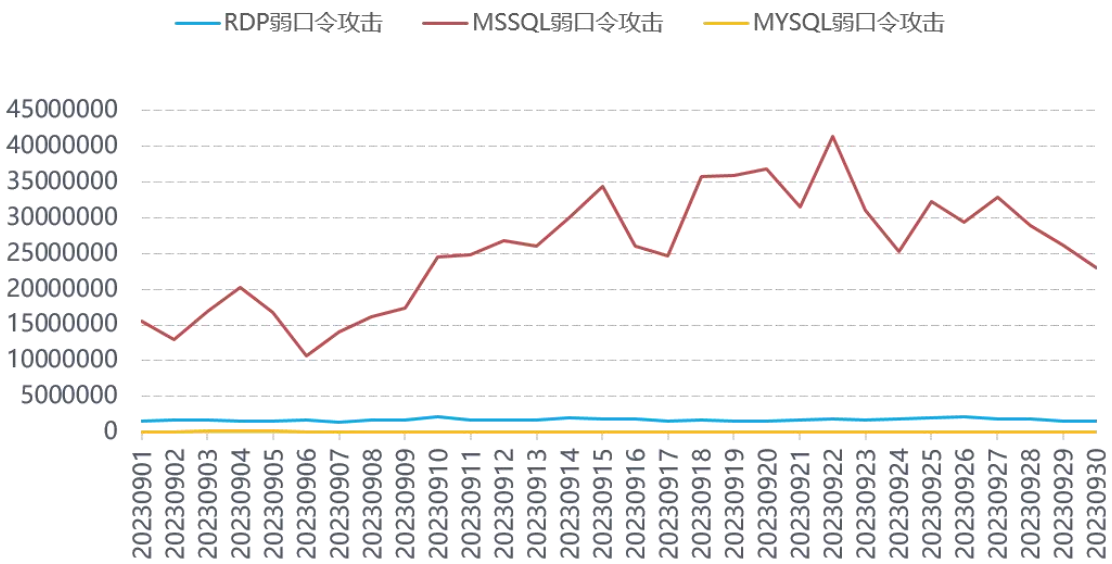
360 系统安全产品，目前已加入黑客入侵防护功能。在本月被攻击的系统版本中，排行前三的依次为 Windows Server 2008、Windows 7 以及 Windows Server 2012。



对 2023 年 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。



通过观察 2023 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。



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。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。

- 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。

- halo：同 360。

- malloxx：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。

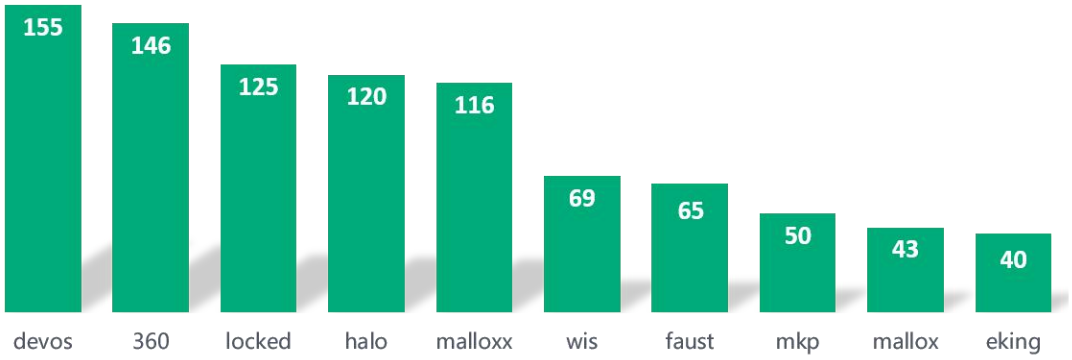
- wis：属于 Makop 勒索软件家族，由于被加密文件后缀会被修改为 mkp 而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。

- faust：同 devos。

- mkp：同 wis。

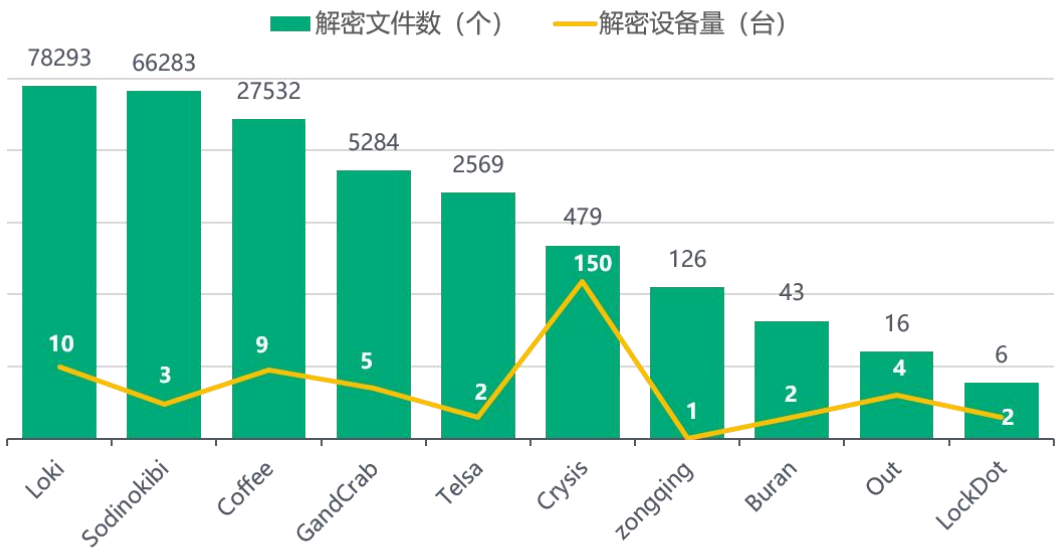
- mallox：同 malloxx。

- eking：同 devos。



解密大师

从解密大师本月解密数据看，解密量最大的是 Loki，其次是 Sodinokibi。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