勒索软件流行态势分析

2023 年 10 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 10 月，全球新增的活跃勒索软件家族有 Hunters International、Electronic 等家族。其中 Hunters International 为多重勒索家族,基于 Hive 勒索病毒家族代码修改演化而来。

以下是本月值得关注的部分热点：

1. 勒索软件攻击正针对未修补漏洞的 WS_FTP 服务器

2. 亲巴勒斯坦黑客组织声称使用 Crucio 勒索软件发动攻击

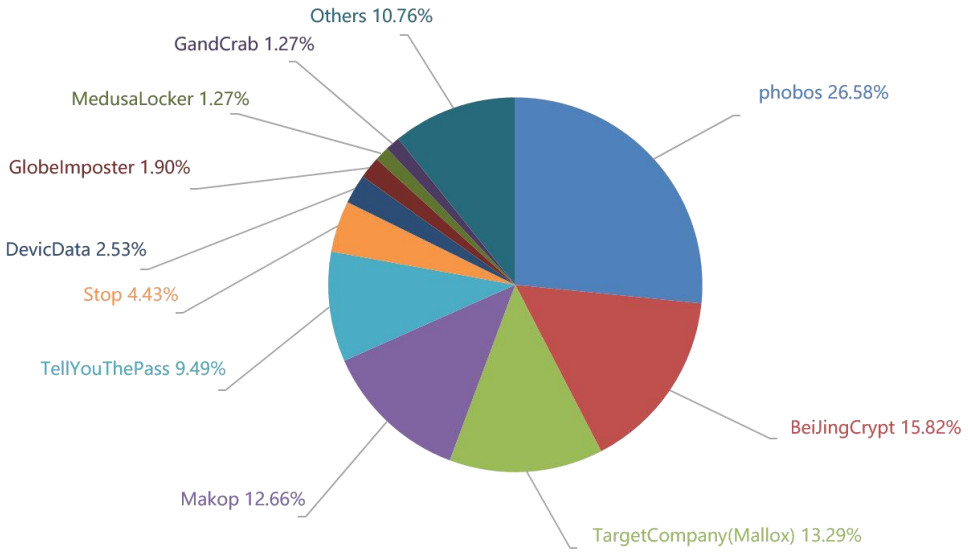
3. Ragnar Locker 勒索软件的设备及相关人员被警方查获

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。

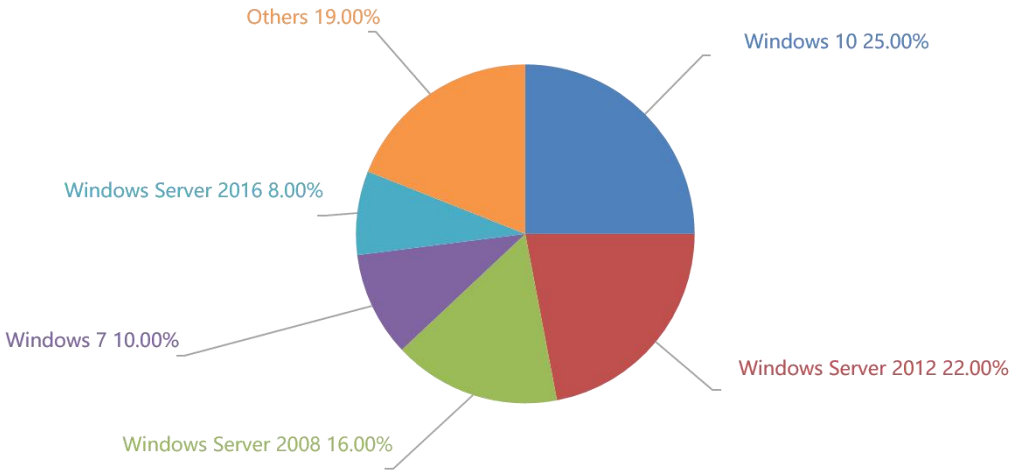
感染数据分析

对本月勒索软件受害者设备所中的病毒家族进行统计：Phobos 家族占比 26.58%居首位，第二的是占比 15.82%的 BeiJingCrypt，TargetCompany(Mallox)家族以 13.29%位居第三。

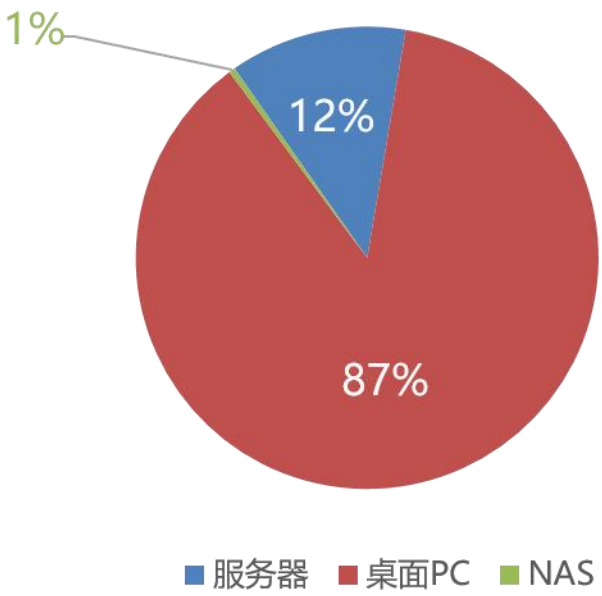
其中位居第三的 TargetCompany(Mallox)，本月新增了以 Mallab 后缀结尾的新变种。



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。



2023 年 10 月，被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型桌面系统占比远高于服务器，偶有 NAS 平台感染。



勒索软件热点事件

勒索软件攻击正针对未修补漏洞的 WS_FTP 服务器

安全研究人员最近发现，自称为 Reichsadler 的网络犯罪组织试图利用 2022 年 9 月被泄露的 LockBit 3.0 生成器来部署勒索软件，但未成功。研究人员表示：“勒索软件攻击者利用了最近公开的 WS_FTP 服务器软件中的漏洞。”尽管 Progress Software 于 2023 年 9 月就发布了针对此漏洞的修复程序，但并非所有服务器都已对其进行修补。

此次监控到的攻击者尝试使用开源的 GodPotato 工具进行提权操作，该工具允许跨 Windows 客户端（Windows 8 到 Windows 11）和服务器（Windows Server 2012 到 Windows Server 2022）平台提权至“NT AUTHORITY\SYSTEM”账户。幸运的是，从此次攻击的受害系统上看，部署的勒索软件执行失败导致攻击者未能成功加密目标数据。但尽管如此，攻击者仍然要求支付 500 美元的赎金……

此次攻击所利用的 WS_FTP Server 漏洞编号为 CVE-2023-40044，是由 Ad Hoc Transfer Module 中的.NET 反序列化漏洞引起的。其可以使未经身份验证的攻击者通过 HTTP 请求远程在服务器系统中执行命令。而研究人员通过对 WS_FTP 的分析，发现当前互联网中约有 2900 台主机正在运行 WS_FTP。而这些在线资产大多数属于大型企业、政企单位以及教育机构。

亲巴勒斯坦黑客组织声称使用 Crucio 勒索软件发动攻击

据安全分析人员透露：一个新兴的名为“所罗门士兵”的亲巴勒斯坦黑客组织近期出现，声称对破坏内瓦蒂姆军事区内 50 多个服务器、安全摄像头和智能城市管理系统的攻击事件负责。该组织表示，他们使

用了一款名为“Crucio”的勒索软件——该软件可能使用了勒索软件即服务（RaaS）功能生成。除此之外，该组织还声称其已从攻击中获取到了高达 25TB 的数据。

此前，“所罗门士兵”通过电子邮件将此信息发送给几家威胁情报公司，同时为了证明其消息的可信度，该组织还提供了来自受感染的闭路电视系统中的一些视频截图，并通过更改被入侵系统的桌面壁纸来显示他们的存在。

Ragnar Locker 勒索软件的设备及相关人员被警方查获

Ragnar Locker 勒索软件在 Tor 网络上的“勒索及数据泄露网站”，于 10 月 19 日上午被查获。此次行动是由美国、欧洲、德国、法国、意大利、日本、西班牙、荷兰、捷克共和国和拉脱维亚等多个国际执法机构共同参与的一次联合执法行动。欧洲刑警组织发言人已确认：作为针对 Ragnar Locker 勒索软件团伙持续行动的一部分，此次扣押了 Ragnar Locker 组织的服务器设备。

此外，在本次行动中，执法机构还逮捕了一名与勒索软件团伙有关联的恶意软件开发人员。欧洲刑警组织在 10 月 20 日表示：“这一恶意勒索软件的‘主要参与者’于 10 月 16 日在法国巴黎被捕，行动同时搜查了他在捷克的家。随后几天，共五名嫌疑人在西班牙和拉脱维亚也接受了讯问。”……“目前，涉案的开发者主犯已被带到巴黎司法法院预审法官处等待进一步审理。”

与此同时，乌克兰警方还突袭了基辅另一名犯罪嫌疑人的住所，没收了其笔记本电脑、手机和电子设备。

黑客信息披露

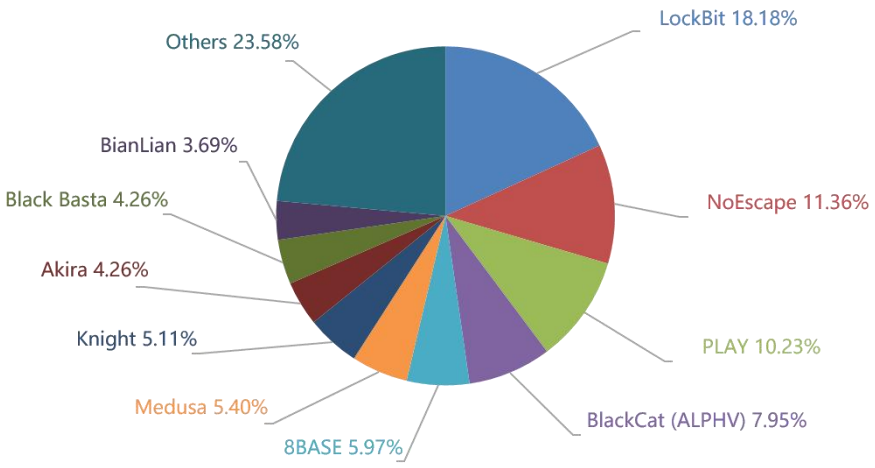
以下是本月收集到的黑客邮箱信息：

ai.sarah@techmail.info	Encryptedd@mailfence.com	pipikaki@onionmail.org
ai_sarah@keemail.me	ghzsr@onionmail.org	Plessys@proton.me
aisara@cock.lu	ghzsr@onionmail.org	pmmx@techmail.info
aisara@confidential.life	goldenapple120pere@gmail.com	ragnarok@cyberfear.com
Blackdream01@skiff.com	Goodmorningfriends@messagesafe.co	receivertes@cock.li
Blackdream01@zohomail.eu	Goodmorningfriends@onionmail.org	receivertes@tutanota.com
brazil-sulin@tutanota.com	Goodmorningfriends@thesecure.biz	reopenran2023@firemail.de
bricesupp@onionmail.org	help.file@zohomail.eu	restaurera@rbox.co
bruttinezubrise2@gmx.de	help.web@gmx.com	rxyyno@gmail.com
c2y@startmail.com	ithelp08@securitymy.name	servicehelp@onionmail.org
chaosdepartment@tutanota.com	ithelp08@yousheltered.com	sir.luke.stevens@gmail.com
contactme@msgden.net	itlab@cyberfear.com	spicy@onionmail.com
crypt_group@outlook.com	itsecurity@cyberfear.com	spicy01@onionmail.com
datahelp23@msgsafe.io	itsevilcorp90@hotmail.com	SULINFORMATICA@proton.me
datasecurity@cock.li	itweb@techmail.info	Supp@firemail.de
Decipher@mailfence.com	Jarjets18@onionmail.org	support1@ranfas.com
decoderdata@onionmail.org	Jarjets18@skiff.com	support2@contonta.com
desm4578@rambler.ru	keybranch@mailfence.com	support890@onionmail.org
DeXret@proton.me	keychain@onionmail.org	support8951@onionmail.org

digitalbro@msgsafe.io	malluma@beeble.com	Targetchamin@gmail.com
drhelper4@gmail.com	Merlin@cyberfear.com	Tta450043@gmail.com
e093d75c25d0637a86589c1b3c4fca35	Merlin@onionmail.org	uncrypthelp@yahoo.com
earthgrass1@protonmail.com	Merlin@outlookpro.net	wholekey@mailfence.com
enc0@dr.com	midostuff@protonmail.com	zinok19899@cock.li
enc1@usa.com	msy85689@rambler.ru	zinok19899@tuta.io
Encrypted@proxy.tg	paymoney@onionmail.org	zxcvb@onionmail.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，该数据仅涉及未能第一时间缴纳赎金或拒缴纳赎金的情况（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 351 个组织/企业遭遇勒索攻击，其中有 6 个中国组织/企业在本月遭遇了双重勒索/多重勒索。另有 2 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

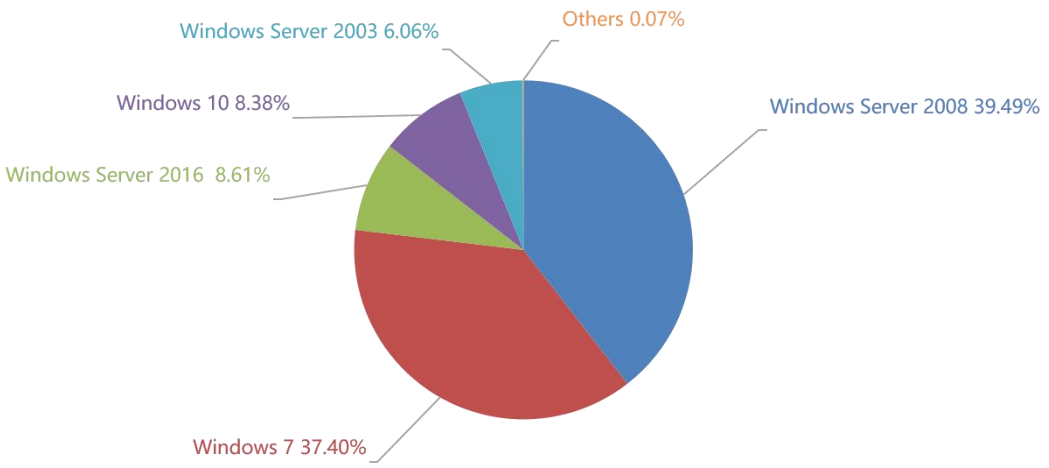
Northwave s.r.l.	St Margaret's Prep	Prestige Care
Barco Uniforms	SMWLLC.COM	Nordic Security Services
Balcan	Steelforce	Woody Anderson Ford
Swipe.bg	wdgroup.com.my	BestPack Packaging
Balmit Bulgaria	pvbfabs.com	Istituto Prosperius
Knight Barry Title	intechims.com	Network Pacific Real Estate - Leak
cdwg.com	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	onyx-fire.com
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	CEFCO
meroso.be	Gossler, Gobert & Wolters Group.	Glassline
nobleweb.com	Peacock Bros	SydganCorp
gormanusa.com	Hacketts printing services	

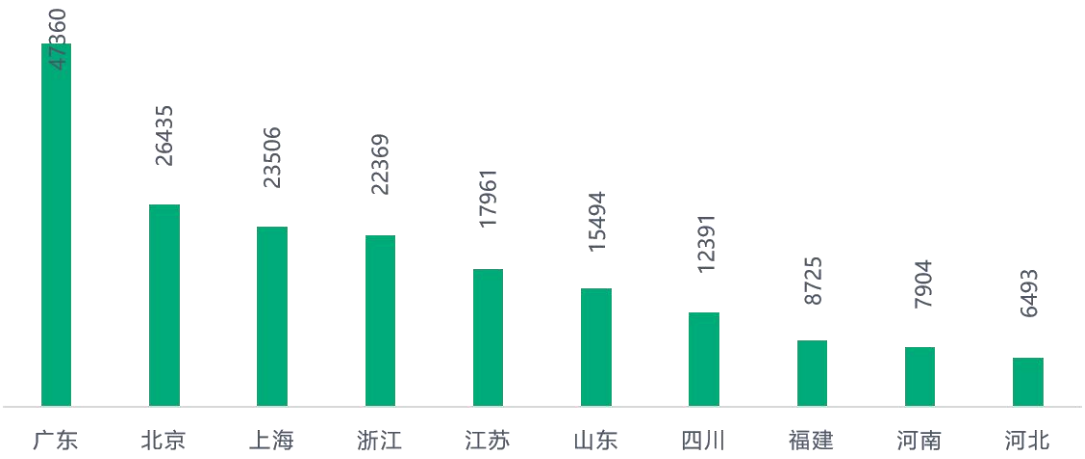
表格 2. 受害组织/企业

系统安全防护数据分析

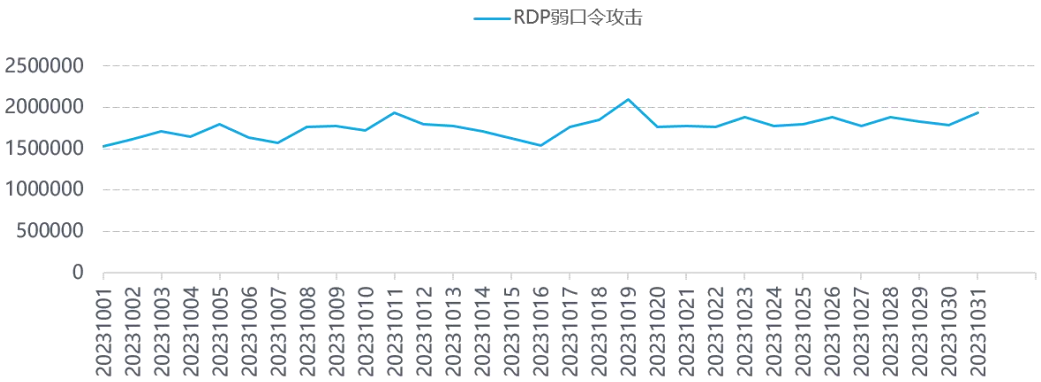
360 系统安全产品，目前已加入黑客入侵防护功能。在本月被攻击的系统版本中，排行前三的依次为 Windows Server 2008、Windows 7 以及 Windows Server 2016。

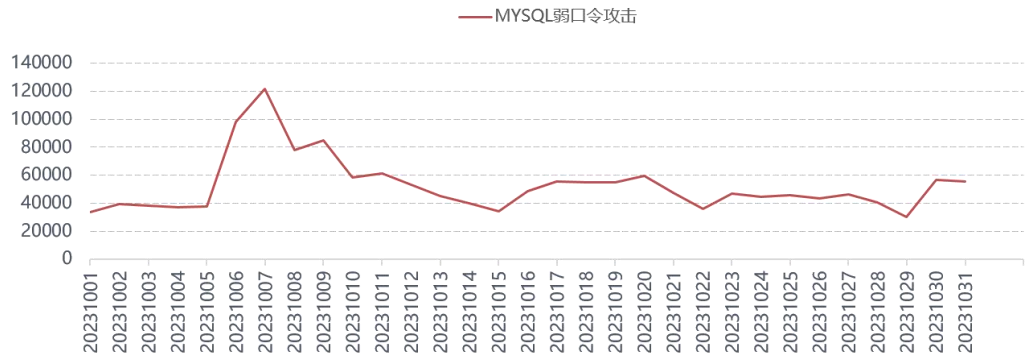


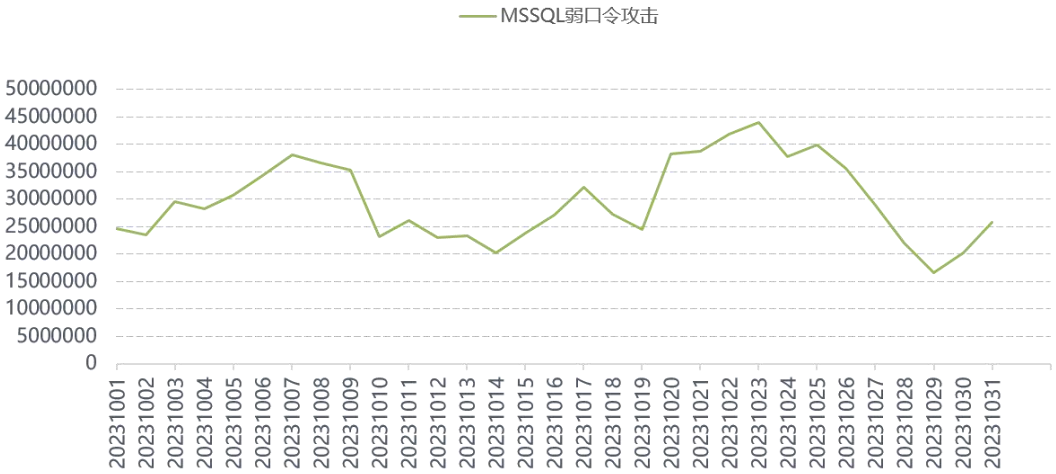
对 2023 年 10 月被攻击系统所属地域统计发现，与之前几个月采集到的数据进行对比，地区排名和占比变化均不大。数字经济发达地区仍是攻击的主要对象。



通过观察 2023 年 10 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。

- mallab：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，本后缀为 10 月新增变种。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曾通过匿影僵尸网络进行传播。

- 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。

- 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。

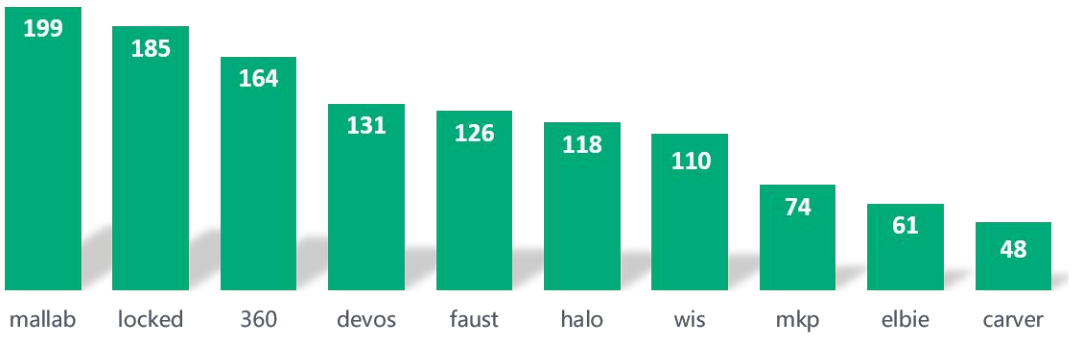
- faust：同 devos。

- halo：同 360。

- faust：同 devos。

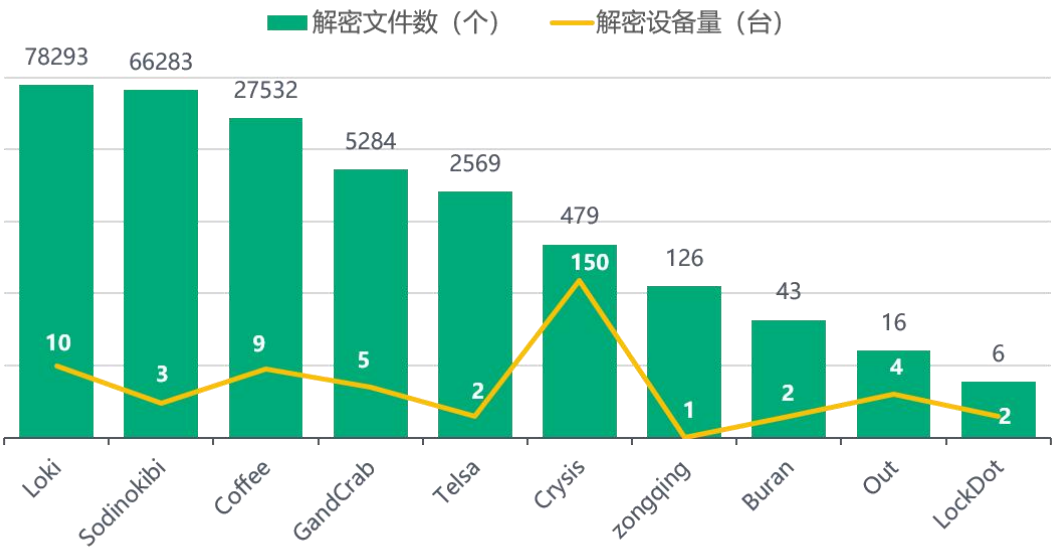
- wis：属于 Makop 勒索软件家族，由于被加密文件后缀会被修改为 mkp 而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。

- elbie：同 devos。
- carver：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