勒索软件流行态势分析

2024 年 10 月

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。

2024 年 10 月，全球新增的双重勒索软件家族有 Sarcoma、Playboy、DragonRansom、Interlock、Hellcat。10 月新增的传统勒索软件家族 Weaxor 在国内的传播较为显著，目前监测其主要通过远程桌面登录手动投毒。

以下是本月值得关注的部分热点：

1. Fog 勒索软件以 SonicWall VPN 为目标来破坏公司网络
2. BianLian 勒索软件声称对波士顿儿童健康医生发起攻击
3. 卡西欧确认客户数据在勒索软件攻击中被盗

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：TargetCompany(Mallox)家族占比 43.50%居首位，第二的是 Makop 占比 17.51%的，RNTC 家族以 10.73%位居第三。

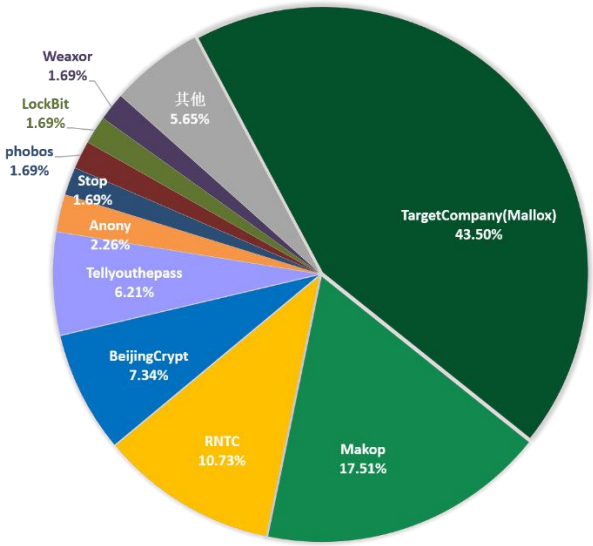

图 1. 2024 年 10 月勒索软件家族占比

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。

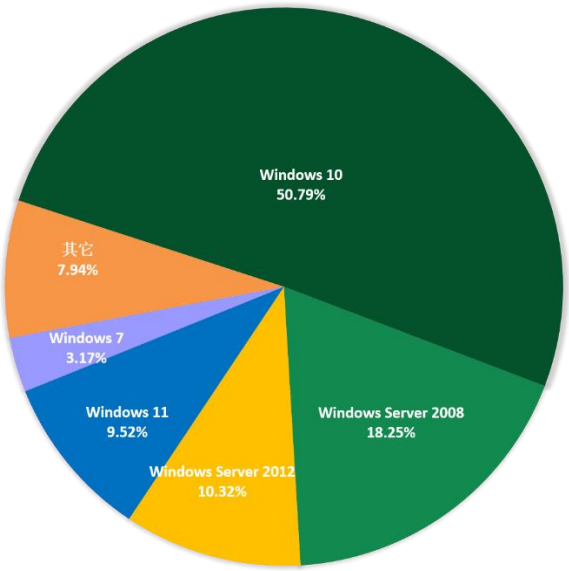

图 2. 2024 年 10 月勒索软件入侵操作系统占比

2024 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 PC 高于服务器平台。

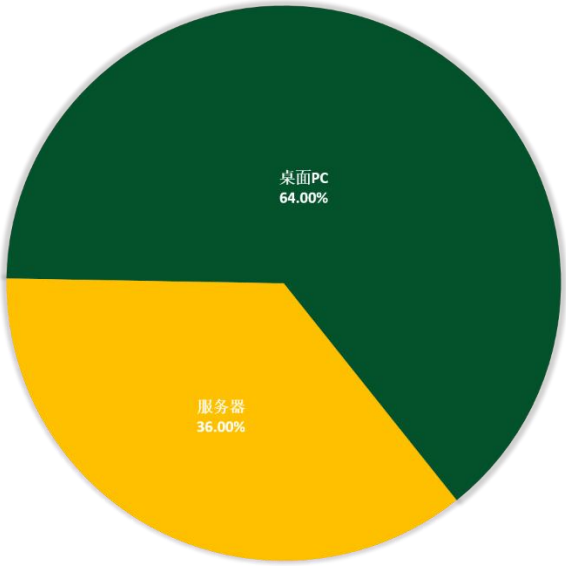

图 3. 2024 年 10 月勒索软件入侵操作系统类型占比

勒索软件热点事件

Fog 勒索软件以 SonicWall VPN 为目标来破坏公司网络

Fog 和 Akira 勒索软件运营商越来越多地通过 SonicWall VPN 账户入侵企业网络，据信攻击者正在利用 CVE-2024-40766，这是一个严重的 SSL VPN 访问控制漏洞。

与此同时，安全研究人员报告说看到 Akira 勒索软件下属公司利用该漏洞获得对受害者网络的初始访问权限。安全研究人员的一份新报告警告说，Akira 和 Fog 勒索软件已经进行了至少 30 次入侵，这些入侵都是从通过 SonicWall VPN 账户远程访问网络开始的。在这些案例中，75%与 Akira 有关其余则归因于 Fog 勒索软件。

有趣的是，这两个威胁组织似乎共享基础设施，这表明两者之间非官方合作的继续。虽然研究人员并不能 100%肯定该漏洞在所有情况下都被使用，但所有被破坏的端点都容易受到它的攻击，运行的是较旧的、未修补的版本。在大多数情况下，从入侵到数据加密的时间很短，大约十小时，最快的甚至达到 1.5~2 小时。在许多此类攻击中，攻击者通过 VPN/VPS 访问客户端，混淆其真实 IP 地址。安全研究人员指出，除了运

行未修补的客户端外，受感染的组织似乎没有在受感染的 SSL VPN 账户上启用多因素身份验证，也没有在默认端口 4433 上运行其服务。

从被破坏的系统窃取数据涉及文档和专有软件，但攻击者不会理会超过 6 个月的文件或者超过 30 个月的敏感文件。

BianLian 勒索软件声称对波士顿儿童健康医生发起攻击

BianLian 勒索软件组织声称对波士顿儿童健康医师（BCHP）进行了网络攻击，并威胁称如不支付赎金则会泄露被盗文件。BHCP 是一个由 300 多名儿科医生和专家组成的网络，在纽约哈德逊谷和康涅狄格州的 60 多个地点运营，在波士顿儿童医院附属的诊所、社区医院和保健中心提供患者护理。

根据 BHCP 在其网站上发布的公告称，其信息技术供应商在 9 月 6 日遭到了一次网络攻击，几天后 BHCP 也在其网络上检测到未经授权的活动。随后在第三方法医专家的帮助下进行的调查证实，攻击者未经授权进入了 BHCP 系统并窃取了文件。

此次泄露影响到了现任和前任员工、患者和担保人。根据客户提供给 BHCP 的信息，泄露的数据包括以下内容：

- 全名
- 社会安全号码
- 地址
- 出生日期
- 驾照号码
- 病历号
- 健康保险信息
- 账单信息
- 治疗信息（部分）

BHCP 进一步澄清说，因为托管在一个单独的网络上，此次网络攻击没有影响其电子病历系统。

目前，BianLian 还没有泄露任何东西，也没有泄露被盗信息的最后期限，这表明他们仍然希望与 BHCP 谈判。

卡西欧确认客户数据在勒索软件攻击中被盗

卡西欧目前证实，本月早些时候它遭受了勒索软件攻击，警告说员工、求职者和一些客户的个人和机密数据也被盗。

此次攻击于 7 日被披露，当时卡西欧警告称，由于周末未经授权访问其网络，该公司正面临系统中断和服务中断。9 日，Underground 勒索软件组织声称对此次攻击负责，并泄露了据称从日本科技巨头系统中窃取的各种文件。10 日，在数据泄露后，卡西欧发表了一份新声明，承认敏感数据在其网络受到攻击期间被盗。

至于目前正在进行的调查结果，卡西欧表示，以下信息已被证实可能被泄露：

- 卡西欧及其关联公司的长期和临时/合同员工的个人数据。
- 与卡西欧和某些关联公司的业务合作伙伴相关的个人详细信息。
- 过去在卡西欧面试过的个人信息。
- 使用卡西欧及其关联公司提供的服务的客户的个人信息。
- 与当前和过去业务合作伙伴的合同相关的详细信息。
- 有关发票和销售交易的财务数据。
- 包括来自卡西欧及其关联公司的法律、财务、人力资源规划、审计、销售和技术信息的文件。

具体关于客户数据，卡西欧指定公开的集合不包括信用卡信息，因为支付数据不存储在其系统上。

此外，这家日本公司表示，像卡西欧 ID 和 ClassPad.net 这样的服务系统没有受到该事件的影响，因为它们没有托管在被破坏的服务器基础设施上。

随着调查的继续，影响的范围可能会扩大，建议那些认为自己可能受到影响的人对未经请求的电子邮件保持警惕。卡西欧还要求互联网用户避免在线分享任何泄露的信息，因为这只会使受数据泄露影响的人的情况恶化。“请不要通过社交媒体等传播这些信息，因为这可能会增加本案信息泄露造成的损害，侵犯受影响者的隐私，对他们的生活和业务产生严重影响，并鼓励犯罪，”卡西欧最新声明说。警方和日本个人信息保护委员会从本周早些时候就已经获悉了这一情况，因此当局参与了调查和整治工作。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

ecrypter.files@gmx.com	iwillhelpyou99@zohomail.eu	defarmx@tutamail.com
lerchsilas125@gmail.com	LabsDecode@gmail.com	immortalsupport@cock.li
wehavesolution@onionmail.org	itservicerec@zohomail.eu	support@p-security.li
solution247days@outlook.com	mammoncomltd@gmail.com	file@p-security.li
wewillrestoreyou@onionmail.org	petrus34@p-security.li	bitblack@onionmail.org
wewillrestoreyou@cyberfear.com	systempc1@keemail.me	pomocit15@kanzensei.top
hermesaa@tutamail.com	systempc18x@protonmail.com	pomocit15@surakshaguardian.com
linger11@cock.li	hashby@yandex.com	support1@cocerid.com
mkprun@onionmail.org	ashbyh@yandex.com	support2@adigad.com
solutionhere@mailum.com	helen.a@inarne.com	proof3200@proton.me
solutionhere@keemail.me	x3m-pro@protonmail.com	adm.helproot@gmail.com
somran@cyberfear.com	x3m@usa.com	finamtox@zohomail.eu
v7991215@gmail.com	your_last_chance_help@protonmail.com	cris_nickson@zohomail.eu
bisonshadoloo@proton.me	your_last_chance_help@elude.in	cris1997nickson@libertymail.net
francess2221@protonmail.com	yourlastchancehelp@cock.li	kkeessnnkkaa@cock.li
frances2@tutamail.com	nemesis-decryptor@india.com	hhaaxxhhaaxx@tuta.io
yestimt@yandex.ru	webmafia@asia.com	sdwyusvsv@outlook.com
help@wizrac.com	Blacklagoon@aolonline.top	sdwyusvsv@meta.ua
returnthefile@cock.li	pizdoglaz@asia.com	helldown@onionmail.org
jimyjoy140@cyberfear.com	ransomed@india.com	help24dec@cyberfear.com
jimyjoy140@tutamail.com	mk.nightwolf@aol.com	help24dec@aol.com
watchdogs20@tuta.io	mk.Nighwolf@inbox.lv	cryzipper@firemail.cc
watchdogs20@cock.li	nemesis_decryptor@aol.com	cryzip11@dnmx.su
password1@tutamail.com	paradise@all-ransomware.info	protonis@skiff.com
king_ransom1@mailfence.com	help@badfail.info	hedaransom@gmail.com
stormouss@onionmail.org		

表 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）。

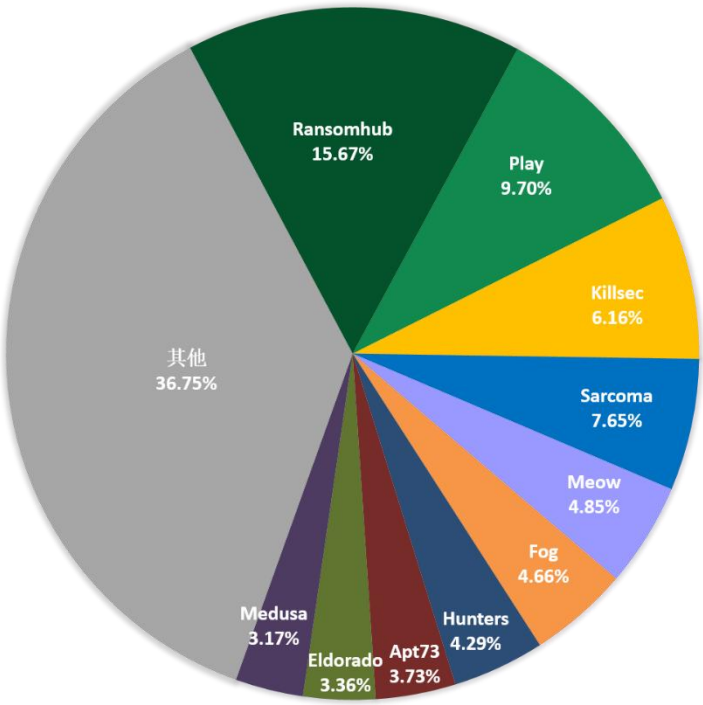

图 4. 2024 年 10 月通过数据泄露获利的勒索软件家族占比

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 536 个组织/企业遭遇勒索攻击，其中包含中国 3 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 10 个组织/企业未被标明，因此不在以下表格中。

HoustonHousingAuthority	ClearConnection	RobbJack&Crystallume
freedomhomecare.net	Aerotecnic	UniversalCompanies
www.mabeglobal.com	PrecisionSteelServices	argofinance.org
AsklingCar	tkg.com	transfoodbeverage.com
anuenterprise.com.au	lpahorticole.faylbillot.educagri.fr	SOFPO
inhometexas.com	bwdtechnology.com	SCHUMAGAKTIENGESELLSCHAFT
caillau.com.br	davisbrothersinc.com	WildAppleGraphics
sandray.com	polypane.be	Evlox
mpspromotions.com	dennissupply.com	HauschildInstallationen
BULLONERIEGALVIT	specpro-inc.com	ErgoFloor

hacla.org	semna.fr	IslandGrill
TDMTechnicalServices	1doc.sg	Volkswagengroup
CASSoftware	Automha	GroupeBayard
Brancaia	AmericanMechanical,inc	Kerkstoel
granjazul.com	AmericanMedicalBilling	Futureguard
illumin8global.com	mauguio-carnon.com	DaldossElevetronic
PaulWhiteCompany	donbosco-landser.net	StoneFutureinc
MavalIndustries	boloforms.com	CANEAONE
UnlimitedLawnCare	onedayevent.com	ICSNett
PureflowAirdog	autodukan.com	Ferrer&Ojeda
iFocusConsulting	temple-inc.com	AHISupply
Pelsue	milleredge.com	ImportadoraMonterreySRL
SunriseExpress	gkcorp.com	NationalEdging
Jillamy	ssbwc.com	Nexus-Shinozaki
IMCannabis	lewa.com	Structure-flex
SmartSource	fordcountrymotors.mx	CicloCairu
nagucoop.com	LaTazzaD'oro	Nora-Lindefrakt
tlie.org	TeddySpA	RioMarine
Scaff'Holding	www.stivo.com	InCareTechnologies
SpiritLakeCommunitySchoolDistrict	SchweigerTransport	AntenneReunionRadio
www.baymark.com	PhiladelphiaMacaroni	GmgMiningSupplies
Astac	MercuryTheatre	SmartMediaGroupBulgaria
DanaSafetySupply	SanglierLimited	TheRobertsFamilyLawFirm
DirksenScrewProducts	yorozu-corp.co.jp	Gedco
noblehouse.com.ph	TrimarcFinancial	EARTHWORKSGroup
hcfinc.com	ArangoBillboard	PerfectionFresh
www.ztexconstruction.com	TransakInc.	AdvancedAccounting&BusinessAdvisory
daserv.com	qs-group.com	RoadDistributionServices
celo.com	Interbel	LácteosLorán
CLASInformationServices	PetropolisPetResort	CurtidosBarbero
rosenlegal.com	SuperiorQualityInsuranceAgency	EasyPay
weberpackaging.com	Vasesa	JumboElectronicsQatar
SurfnetCommunications	CountryClubElBosque	Navarra&Marzano
anhf.org.auh	AtendeSoftware's	CostaDelSolHotels
www.trinitesolutions.com	apollohospitals.com	ThePlasticBag
www.scopeset.de	mh-mech.com	ElevatorOne
sokkakreatif.com	sizeloveconstruction.com	MarchElevator
www.legilog.fr	rcschools.net	SuntrustProperties
projektalp.ch	mopsohio.com	tankstar.com
JordanPublicSchools	KansasCityHospice	victrongroup.com
SageAutomotiveInterior	MichaelJGurfinkel	FULTON.COM
nathcompanies.com	KMCControls	OrbitSoftware,Inc.

BerridgeManufacturingCo.	starhealth.in	UniversiteParisSud
MasterySchools	SPECTRUMCHEMICAL.COM	avans.com
AccuracyInternational	clinicia.com	EagleRecoveryAssociates
K&STool&MfgCo.	paciente.sempremedico.com.br	AnVaIndustries
BasilioAdvogados	T-Space	Smoker'sChoice
CHRISTODOULOSG.VASSILIADES&CO.LLC	PheimUnitTrustsBerhad	SaratogaLiquor
Fortis	ZierickManufacturingCorporation	AccountingResourceGroup
phxcmp.com	OpenRangeFieldServices	pingan.com
barranquitas.pr.gov	McCody	AmbassadorofIsraelinGermanyEmails
www.keizers.ca	ask.vet	AarenScientific
mmpunion.com	CountryInn&SuitesbyRadisson	TrinityWholesaleDistributorsInc
GermanChamberofCommerce	Wilkinson	blalockcompanies.com
flueid.com	MidStateElectric	okcabstract.com
EvergreenSD50	TheStrainriteCompanies	AIUT
guymontigers.com	AbsoluteMachineTools	AdvantageCDC
harrispersonalinjury.com	INDIBAGroup	Sit&Sleep
ConCash	Astolabs.com	Maxdream
AGAS	NeighborsCreditUnion	BlainSupply
LakesightTechnologiesInformation	Fromm(FrommBeauty.com)	DavisPickrenSeydelandSneedLLP
IslandCoastalServicesLtd	UltraTune(ultratune.com.au)	matki.co.uk
Mixfame	Alqaryahauction.com	corporatejobbank.com
payxpress.co.il	www.qal.com	AccurateRailroadConstructionLtd
TexasTechUniversityHealthSciencesCenter	DubinGroup	MaxShop
melangesystems.com	RDCControlLtd	autodoc.pro
mkarrari.com.br	CreaGenInc	trulysmall.com
Edmov	RacingForensicsInc	nspproteins.com
TVGuideMagazine	LuxwoodSoftwareTools	healthyuturn.in
PositiveBusinessSolutions	tripxoxo.com	premierpackaging.com
C&CIndustries	www.proflex.ro	htetech.com
PTTransportasiGasIndonesia	www.icp.pr.gov	goughconstruction.com
TheEyeClinicSurgicenter	Valu-TracInvestmentManagementLtd.	fleetequipment.com
WestwoodCountryClub	PropakCorp.	auto-recyclers.com
BlissWorldwide	MRIRadiologyNetwork,P.A./UniversityMRI	atd-american.com
wescan-services.com	DaikinIndustries(Thailand)Ltd.	allianceind.com
LegacyTreatmentServices	AikenElectricCooperative,Inc.	avioesforza.it
PremierWorkSupport	oklahomasleepinstitute.com	totalelectronics.com
www.olanocorp.com	www.chiltonisd.org	Istrail
Doctor24x7	www.kersey.net	AlbanyCollegeofPharmacy
Delcaper	www.aristoiclassical.org	ArelanceGroup
GovernmentofBrazil	www.camelotservices.com	PearlCohen

NoBroker	HiCare.net	TheSuperiorCourtofCalifornia
SWReclaim	Bigpharmacy.com.my	BrowardRealtyCorp
WilsonTarquin	AuxitS.r.l	yassir.com
OttawaValleyHandrailingCompanyLtd	volohealth.in	tpgagedcare.com.au
EvergreenPublicSchools	FractalID	lyra.officegroup.it
hcsgcorp.com	Welker(welker.com)	AOSense/NASA
DeRoseLawyers	CordoganClarkandAssociates	CreativeConsumerConcepts
MatoukBassiouny	powiatjedrzejow.pl	PowerTorqueServices
CucamongaValleyWaterDistrict	transport-system.com	seoulpi.io
EvergreenLocalSchoolDistrict	DoctorsToYou.com	canstarrestorations.com
AmbicaSteels	Horsesportireland.ie	www.ravencm.com
NikoResourcesLtd.	FoodSciencesCorporation	Ibermutuamur
ValueMaxGroup	synertrade.com	betterhalf.ai
PrecisionElectricalSystems	G-plans.com	HARTSON-KENNEDY.COM
Denkali	Fpapak.org	omniboxx.nl
SRS-StahlGmbH	CETRULO	BNBuilders
MESHWORKS	Nor-Well	winwinza.com
TheKnesset-Israel	KuhnandAssociates	Storck-BaugesellschaftmbH
HUBBARDHALL.COM	moi.gov.ly	C&LWard
deschampsimp.com	CorporateJobBank	WilmingtonConventionCenter
omara-ag.com	LeinLawOffices	Guerriere&Halnon
nrcs.net	BostonChildren'sHealthPhysicians	MarkdomPlasticProducts
Groupseco.com	HenryCountySchools	Pete'sRoadService
zyloware.com	CentralPennsylvaniaFoodBank	releese.io
unitedsprinkler.com	PromiseTechnology,Inc.	kleberandassociates.com
PacificPulmonaryMedicalGroup	basarsoft.com.tr	RileyGearCorporation
CentrillionTechnologies	UltimateRemoval	TANYACreations
AspenHealthcare	Ideker	mullenwylie.com
SpinebyVillamilMD	InnerCityEducationFoundation	GenProInc.
DigitalEngineering	SystemPavers	CopySmartLLC
www.resourceinternational.com	McMunn&YatesBuildingSuppliesorp	NorthAmericanBreaker
McElroy,Quirk&Burch,APC	Microworks	AmplitudeLaser
bulloch.solutions	ParnellDefense	FursanTravel
www.kciconst.com	AarenScientific	GWMechanical
www.oma.aero	ByerlyAviation	Dreyfuss+BlackfordArchitecture
DrugandAlcoholTreatmentService	NoraBiscuits	TranstecSAS
tuggleduggins.com	RescarCompanies	McGaughey&KeaneyCPAs
ValueCityNJ	Concord	DPCDATA
TheGetzGroup	OzarksGo	enterpriseoutsourcing.com
pkaufmann.com	CourtneyConstruction	LyomarkPharma
modplan.co.uk	rudrakshahospitals.com	ConductiveContainers,Inc
hpecds.com	HennemanEngineering	bbgc.gov.bd
carolinaarthritis.com	MisioneroVegetables	CobelPlast

Smeg	SteelArtSigns	ShinBet
ApacheMills,Inc.	Astero	Barnes&Cohen
thompsoncreek.com	gfm-uk.com	TRCWorldwideEngineering
www.northernsafety.com	caseparts.com	RobLevine&Associates
mgfsourcing.com	compra-aruba.com	CaleyWray
appen.com	DurhamRegion	RedBarrels
filmai.in	medicato.com	LIFTING.COM
drizly.com	FUN-LAB	Emerson
robinhood.com	CathexisHoldingsLP	GoldenAgeNursingHome
thebeautyclick.co.uk	AsciresBiomedicalGroup	mccartycompany.com
trans-logik.com	RockyMountainGastroenterology	bypeterandpauls.com
www.talonsolutions.co.uk	WorldVisionPerú	domainindustries.com
SandroForteFinancialSupport	ConstructionSystemsinc	ironmetals.com
SusanFischgrund	Timber	rollxvans.com
nanolive.ch	saizeriya.co.jp	ETCCompanies
picsolve.com	confidencegroup.com.bd	BranhavenChryslerDodgeJeepRam
bcllegal.com	OSGTool	ForsheyProstokLLP
EagleIndustries	ModiinEzrachi	Holmes&Brakel
ActionHeating&Cooling	NextStage.AI	IsraelPrimeMinisterEmails
GlucksteinPersonalInjuryLawyers	VoltaRiverAuthority	FoccoERP
ThePovmanLawFirm	ProtectiveIndustrialProducts	QuantumHealthcare
LifeMine	TherabelLucienPharmaSAS	asobostudio
IronWorldManufacturing	RumpkeConsolidatedCompanies	AcuityAdvisor
MainelliMechanicalContractors	ØsteråsBygg	UnitedAnimalHealth
TUParks	UnitaTurism	CascadeColumbiaDistribution
IvanhoeClub	ElmoreGoldsmith	Akromold
PrincePipes	practicesuite.us	LabibFunkAssociates
P+BTeamAircargo	peorialawyers.com	ResearchElectronicsInternational
passivecomponent.com	extramarks.com	ShoreMaster
ByDesignLLC	DoctorsRegionalCancerCenter	marthamedeiros.com.br
WayneCounty	AxisHealthSystem	aberdeenwa.gov
YoungsTimberBuildersMerchants	TheLawOfficeofOmarOVargas	CSGConsultants
GoshenCentralSchoolDistrict	StructuralandSteelProducts	Corantioquia
Mar-Bal	medexhco.com	performance-therapies
elnamagnetics.com	AtlanticCoastConsultingInc	www.galab.com
KEEProcess	LaFutura	telehealthcenter.in
Easterseals	BarnesCohenandSullivan	howardcpas.com
TriconEnergy	Glacier	bshsoft.com
shipkar.co.in	CasioComputerCo.,Ltd	credihealth.com
IdeaLab	Doscast	FortyEightyArchitecture
LincolnUniversity		

表 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 10。

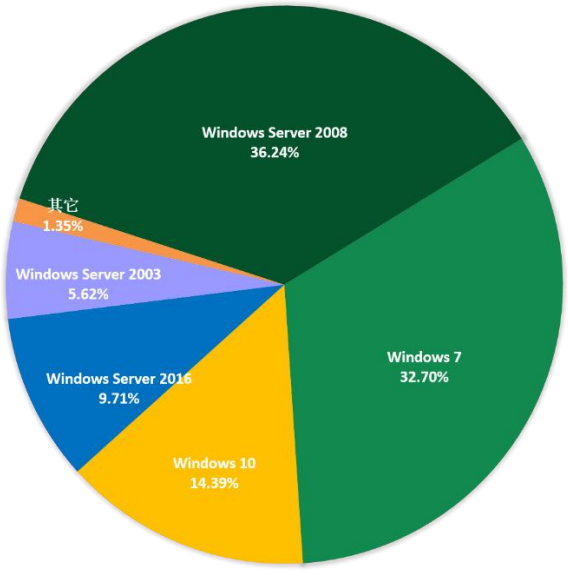

图 5. 2024 年 10 月受攻击系统占比

对 2024 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。

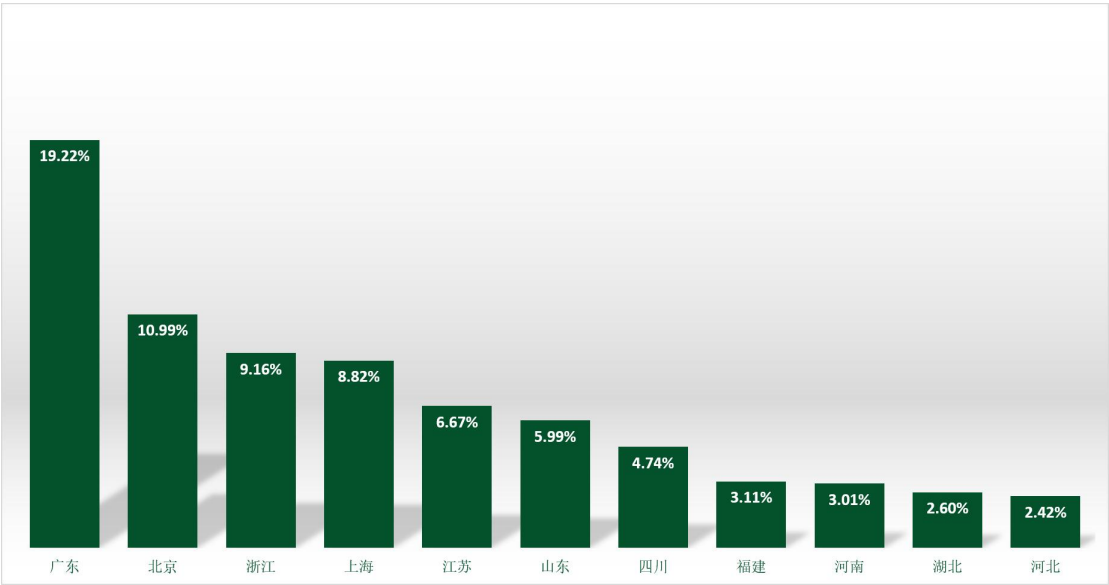

图 6. 2024 年 10 月国内受攻击地区占比排名

通过观察 2024 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。

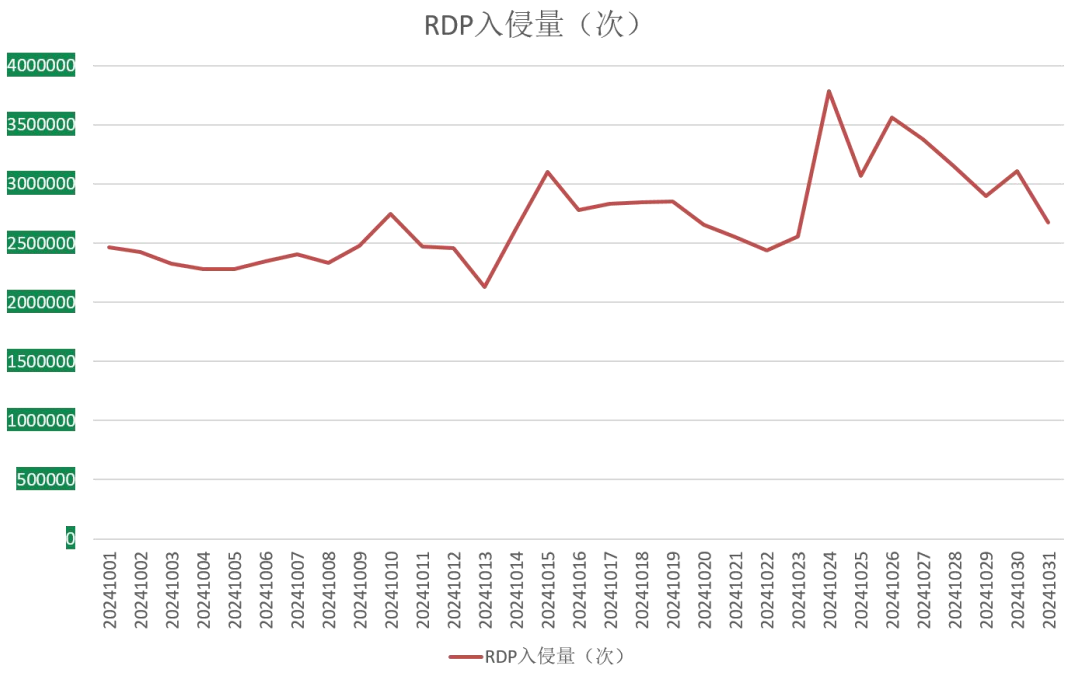

图 7. 2024 年 10 月监控到的 RDP 入侵量

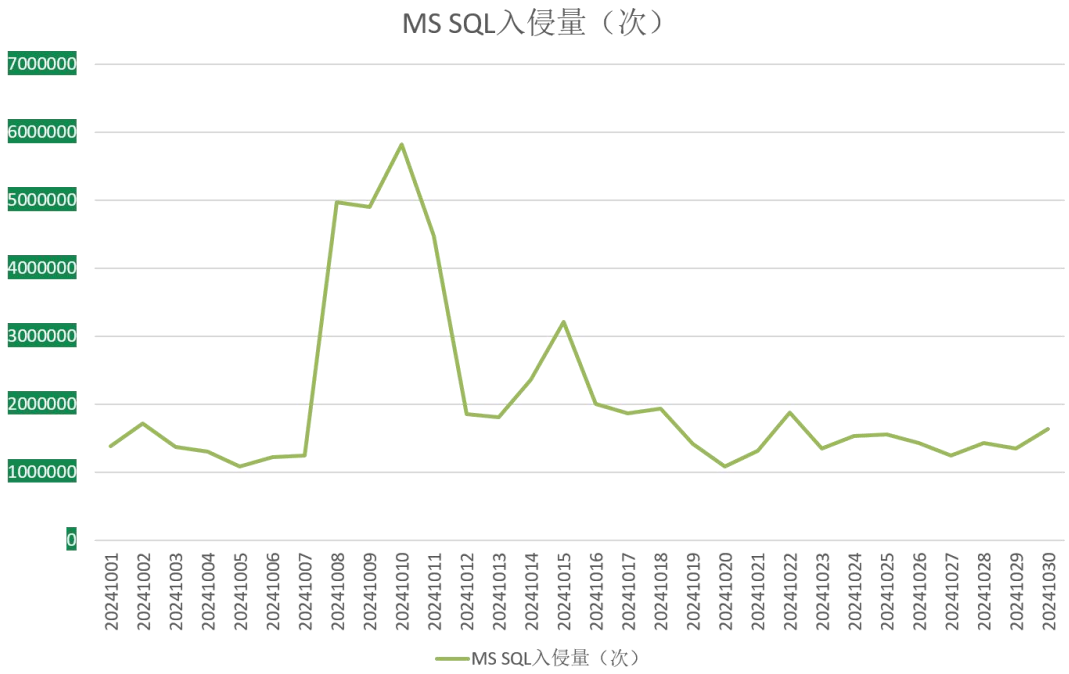

图 8. 2024 年 10 月监控到的 MS SQL 入侵量

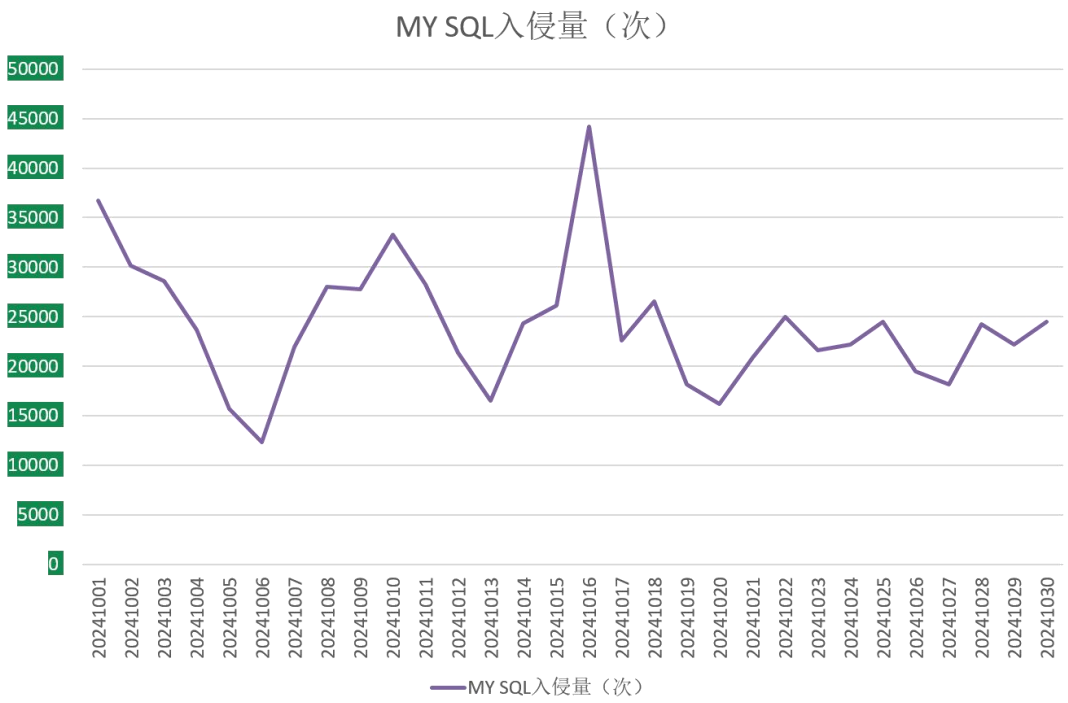

图 9. 2024 年 10 月监控到的 MYSQL 入侵量

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。

- rmallox：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，今年起增加了漏洞利用的传播方式。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。
- wstop： RNTC 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，同时通过 smb 共享方式加密其他设备。
- 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。
- bixi：属于 BeijngCrypt 勒索软件家族，由于被加密文件后缀会被修改为 beijing 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与数据库弱口令成功后手动投毒。
- 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。

- src：同 mkp。
- mallox：同 rmallox。
- wormhole：属于 Wormhole 勒索软件家族，由于被加密文件后缀会被修改为 Wormhole 而成为关键词。该家族主要的传播方式为：通过瑞友天翼软件漏洞发起攻击。
- 888：属于 Nemesis2024 家族，以勒索信中的 Nemesis 家族字段命名。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。
- baxia：同 bixi。

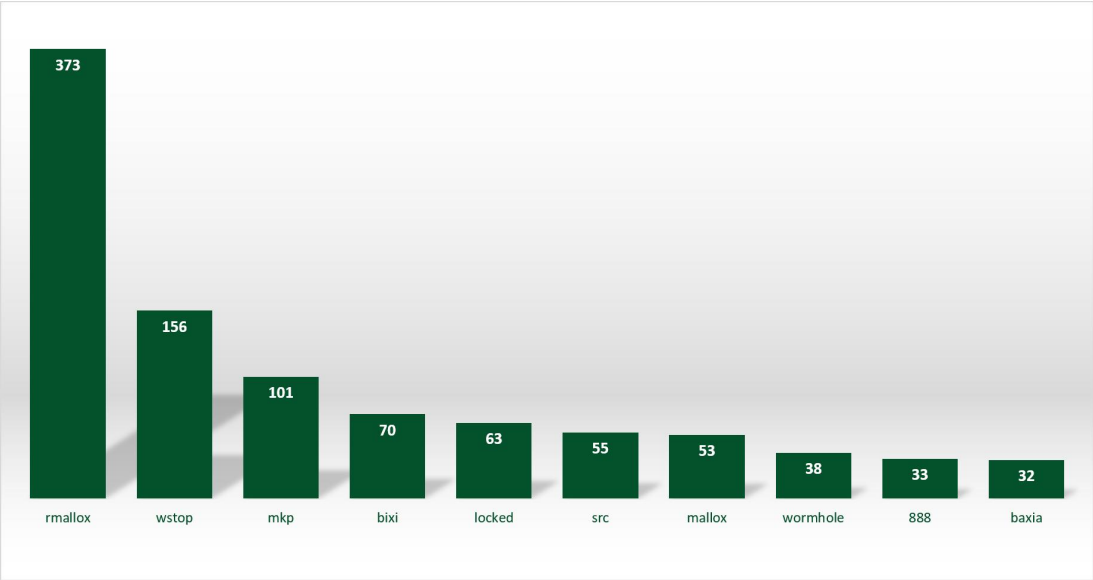

图 10. 2024 年 10 月反病毒搜索引擎关键词搜索排名

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 OpenMeV2。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。

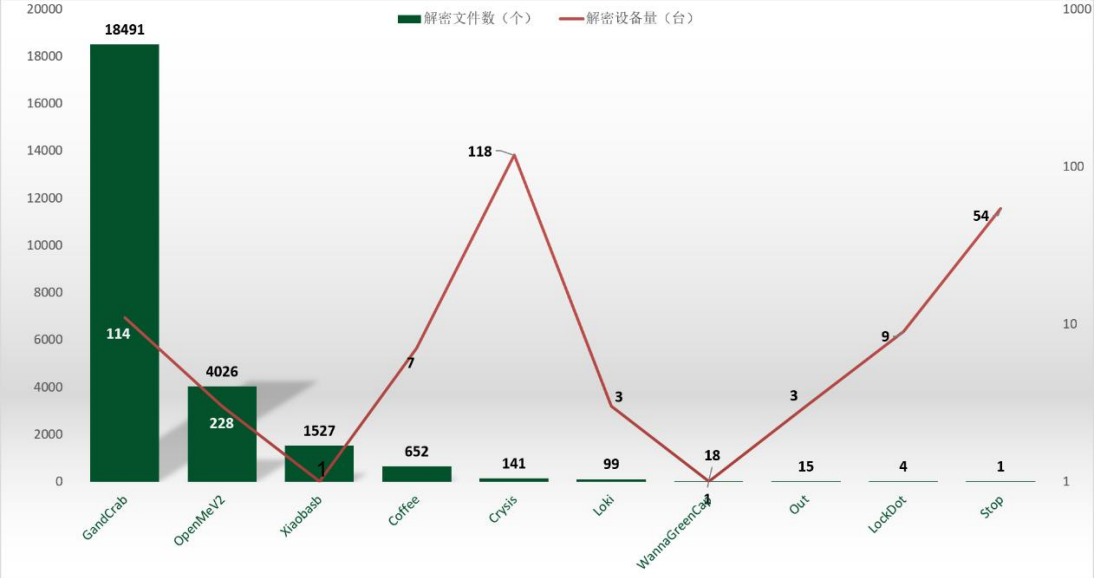

图 11. 2024 年 10 月解密大师解密文件数及设备数排名


360数字安全
数 字 安 全 的 领 导 者
360安全大脑