勒索软件流行态势分析

2024 年 5 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 5 月，全球新增的双重勒索软件家族有 FSOCIETY（flocker）、Arcus Media、Zero Tolerance。新增的传统勒索软件家族有 Phalcon、ShrinkLocker 、Moneyistime。其中 ShrinkLocker 利用操作系统的 Bitlocker 进行文件加密，Moneyistime 在国内广泛传播并开始出现变种。

以下是本月值得关注的部分热点：

1. 波音公司证实有勒索软件试图向其勒索 2 亿美元
2. 新版 BiBi 擦除器加入破坏硬盘分区表功能
3. 新型勒索软件 ShrinkLocker 会使用 BitLocker 加密文件

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：Makop 家族占比 21.39%居首位，第二的是 TargetCompany(Mallox)占比 20.32%，phobos 家族以 15.51%位居第三。

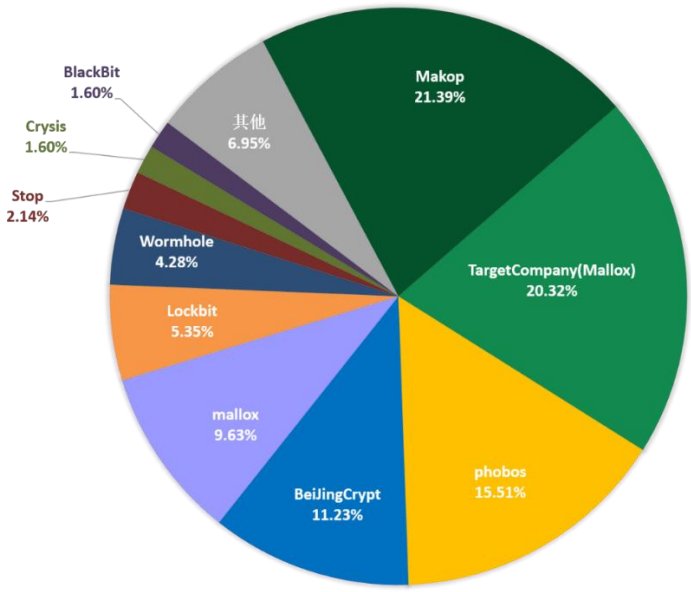

图 1.勒索软件 5 月各家族占比

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。

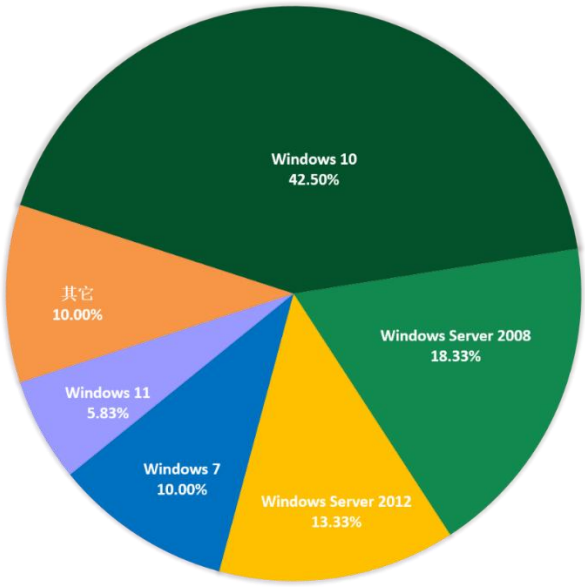

图 2. 勒索软件 5 月感染操作系统占比

2024 年 5 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 相比服务器平台的攻击比例略高。

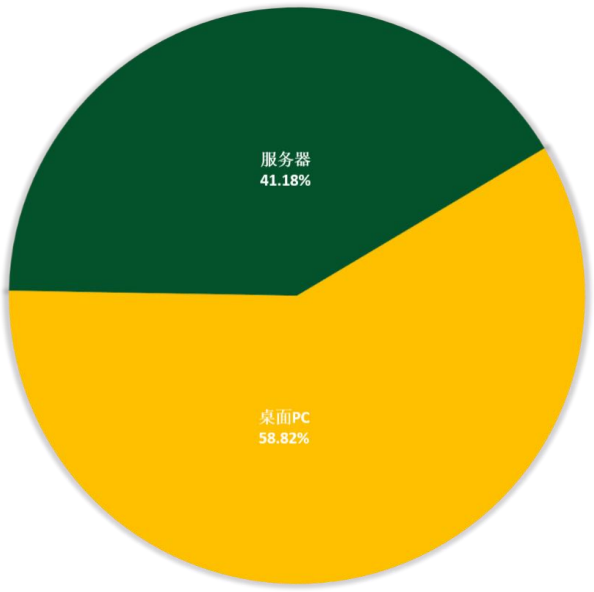

图 3. 勒索软件 5 月感染系统类型占比

勒索软件热点事件

波音公司证实有勒索软件试图向其勒索 2 亿美元

波音公司 5 月 8 日表示，该公司于 2023 年 10 月已向 LockBit 勒索软件平台的网络犯罪分子缴纳了其向该公司索要的 2 亿美元勒索赎金。波音公司证实，该公司就是美国司法部于 5 月 7 日公布的一份起诉书中所提到的一家未具名的跨国航空和国防公司。这份起诉书指控俄罗斯公民德米特里·尤里耶维奇·霍罗舍夫是 LockBit 勒索软件的主要管理员和开发者。

但除此以外，波音公司拒绝进一步置评，并表示已将问题转交给 FBI。而 FBI 方面则并未立即回应此次事件。去年 11 月初，LockBit 网站上曾公布了约 4.3GB 的波音公司数据，波音公司在当时曾表示并未向 LockBit 支付任何赎金。而在起诉书中提到的未具名公司是科罗谢夫及其同伙“索要巨额赎金”的一个例子，自 2019 年底或 2020 年初以来，他们已从受害者手中勒索了逾 5 亿美元赎金。

新版 BiBi 擦除器加入破坏硬盘分区表功能

一款名为 BiBi Wiper 的擦除器型勒索软件在其新版本中加入了删除硬盘分区表的功能，这一功能使数据恢复变得更加困难，从而延长了受害者的宕机时间。这款名为“BiBi Wiper”的擦除器型勒索软件主要在以色列及阿尔巴尼亚地区传播，据称该勒索软件是来自于一个名为“Void Manticore”的黑客组织，而部分研究机构认为该组织可能与伊朗有关，但目前尚无明确的关联证据。

BiBi Wiper 最早在 2023 年 10 月被安全研究员“Security Joes”发现，并因其攻击行为引发了以色列 CERT 在 2023 年 11 月的告警。该告警称有人利用 BiBi Wiper 对该国关键组织发动大规模的网络攻击。

根据安全研究机构的一份最新报告显示，BiBi Wiper 发布了其最新版本擦除器，同时发现与其同属一个黑客组织还使用了另外两种擦除器——Cl Wiper 和 Partition Wiper。该报告还表示，该擦除器背后的 Void Manticore 与另一个名为 Scarred Manticore 的组织可能存在运营上的重叠，这表明两者之间存在合作关系。并称 Void Manticore 可能隐藏在一个名为 Karma 的黑客组织背后。

目前，安全研究机构观察到较新版本的 BiBi Wiper 会用随机数据破坏非系统文件，并在文件后附加一个包含“BiBi”字符串的随机扩展名。与过去的版本相比，这些较新的变种仅针对地区标记在以色列操作系统，并且不再删除系统快照或禁用系统的错误恢复功能。但它们现在会从硬盘中删除分区表信息，这种专门针对系统分区表展开的攻击，因其会导致安全人员无法恢复硬盘布局而将数据恢复工作复杂化，并最大程度地

破坏数据。CI Wiper 则主要针对地区标记为阿尔巴尼亚的系统，它使用“EIRawDisk”驱动程序执行擦除操作并将预定义的缓冲区覆盖到物理驱动器的对应位置中。

新型勒索软件 ShrinkLocker 会使用 BitLocker 加密文件

一款名为 ShrinkLocker 的新勒索软件会在使用 Windows BitLocker 加密企业系统时创建一个新的启动分区。这款名为“ShrinkLocker”的勒索软件因其通过缩小可用的非引导分区来创建引导分区而得名，其目前已知曾对政府机构和疫苗及制造业公司发动过攻击。

ShrinkLocker 利用微软的 VBScript 脚本语言编写（该语言在即将推出的 Windows 11 系统的 24H2 更新中将变为可选组件而被逐步启用）。它的一个功能是通过使用 Windows 管理规范(WMI)和 Win32_OperatingSystem 类来检测目标机器上运行的特定 Windows 版本。如果满足特定的参数条件，攻击才会继续进行：例如当前域与目标域匹配，并且操作系统版本高于 Vista。否则，ShrinkLocker 会放弃攻击并删除自身。

而如果发现目标符合攻击要求，ShrinkLocker 便会使用 Windows 中的 diskpart 程序将每个非系统分区缩小 100MB，并将未分配的空间分割成同样大小的新主分区。研究人员表示在 Windows 2008 和 2012 系统中，该勒索软件首先会将启动文件与其他卷的索引一起保存下来。此外，ShrinkLocker 还会修改注册表项以禁用远程桌面连接或在没有可信平台模块（TPM）的主机上启用 BitLocker 加密。

通过分析，研究人员能够确认该勒索软件进行了以下注册表更改：

- fDenyTSConnections = 1:禁用 RDP 连接
- scforceoption = 1:强制智能卡身份验证
- UseAdvancedStartup = 1:需要在预启动时使用 BitLocker PIN 进行身份验证
- EnableBDEWithNoTPM = 1:允许在不兼容 TPM 芯片的情况下使用 BitLocker。
- UseTPM = 2:如果可用则允许使用 TPM
- UseTPMPIN = 2:如果存在 TPM，则允许使用启动 PIN
- UseTPMKey = 2:如果存在 TPM，则允许使用启动密钥
- UseTPMKeyPIN = 2:如果存在 TPM，则允许使用启动密钥和 PIN
- EnableNonTPM = 1:允许在不兼容 TPM 芯片的情况下使用 BitLocker，需要在 USB 闪存驱动器上输入密码或启动密钥。

- UsePartialEncryptionKey = 2:需要使用 TPM 启动密钥
- UsePIN = 2:需要在 TPM 上使用启动 PIN

ShrinkLocker 背后的攻击者不会给受害者留下赎金文件，而是将一个新的启动分区的标签设置为一个电子邮件地址。在加密驱动器之后，攻击者会删除 BitLocker 保护程序（例如 TPM、PIN、启动密钥、密码、恢复密码和恢复密钥）以阻止受害者恢复 BitLocker 的加密密钥，并将修改后的密钥其发送给攻击者。

用于加密文件的密钥是一个由随机乘法和替换变量为 0-9 数字、特殊字符以及“The quick brown fox jumps over the lazy dog.”（快速棕色狐狸跳过懒狗）的拉丁文组成的 64 位组合。在攻击的最后阶段，ShrinkLocker 还会强制系统关闭以使所有更改生效，并使受害者无法解锁驱动器且无法使用 BitLocker 恢复选项。

目前，研究人员发现 ShrinkLocker 有多个变种，并已被用于攻击墨西哥、印度尼西亚和约旦的政府机构以及钢铁和疫苗制造行业的组织。

黑客信息披露

以下是本月收集到的黑客邮箱信息:

devos-2686@zohomail.eu	room155@tuta.io	frankhans@tuta.io
21512232318132@proton.me	Email_Decryptor_Payment@scryptmail.com	zaton@tuta.io
321598789321@tutamail.com	blymer@xyzmailpro.com	ssget@protonmail.com
clarencezeedorf@onionmail.org	hack3dlikeapro@proton.me	zinton@tuta.io
fiileky2023@yahooweb.co	lockdata@onionmail.org	bufalo@boximail.com
fiileky2023@onionmail.com	chewbacca@cock.li	btcontact@protonmail.com
mrboot@privyinternet.com	diskstation@tutamail.com	supportforyou@msgsafe.io
ederdempsey@onionmail.org	synology@beeble.com	lohodf@mail.ru
eriosdataseller@onionmail.org	myds@mail2tor.com	xinoxix@tuta.io
virgilsnejder@keemail.me	alt.v2-4odknfr5@yopmail.com	zacapa@cock.li
decryptyourfileshereee1@cock.li	team.seven@zohomail.eu	zacapa2020@protonmail.com
helpadmin2@protonmail.com	infoadmin@mail.ee	zacapa@tuta.io
helpadmin2@cock.li	backupfile@cyberfear.com	gotis1@skiff.com
moneyistime@skiff.com	edyscm@skiff.com	banuda@tuta.i
imortalcrypt@morke.org	hongdou2011@skiff.com	antihacker2017@8ox.ru
imortalcrypt@mail2tor.com	opixware@gmail.com	JennyBrown3422@gmail.com
attackattack@tutamail.com	sp.problemsolver.sp@gmail.com	Jenny@gsd.com
attackattack@cock.li	ProblemSolver@onionmail.org	Decipher@waifu.club
garrantydecrypt@airmail.cc	Decrypt.lilium@gmail.com	RestoreBackup@cock.li
2189321765132@cock.li	Open_file@tutanota.com	mexicancartel523@gmail.com
bewool@keemail.me	imbeast@skiff.com	anonymous22109@proton.me
bewool1@outlook.com	fast_decrypt_and_protect@tutanota.com	trufflehogger@proton.me
amir206amiri2065sa@gmail.com	corporacaoxrat@mail2tor.com	AnyvAnyv@skiff.com
amir206amiri2065sa@tutamail.com	xRatTeam@mail2tor.com	keylan@techmail.info
qq.decrypt@gmail.com	xratteam@email.tg	gerb666@proton.me

qq.encrypt@gmail.com	corporacaoxrat@protonmail.com	venusdata@onionmail.org
Decrypt.rz@zohomail.com	repair_data@scryptmail.com	itpro2030@cyberfear.com
bakbak@cocaine.ninja	frozen_service_security@scryptmail.com	itpro2030@cock.li
admin@cuba-supp.com	gitersupp@protonmail.com	xmmh@tutanota.com
inbox@mail.supports24.net	giter@cock.li	xmmh@tutamail.com
ethan@fastmsg.info	zynoxion@protonmail.com	mail4decrypt@foxmail.com
Protonmail ad_default@protonmail.com	cryoteons@protonmail.com	v.li17@zohomail.eu
admansmit001@protonmail.com	mrnice@riseup.net	ebby.gales@tutanota.com
afts_agent@protonmail.com	h911x@yahoo.com	dechelper@dremno.com
helpadmin1@protonmail.com	1413201760@qq.com	dechelper@excic.com
helpallen@protonmail.com	lolyta_restore@protonmail.ch	helper@atacdi.com
mail_supportRG@protonmail.com	freelocker@riseup.net	helper@buildingwin.com
roselondon@protonmail.com	yakomoko@protonmail.com	conspiracyid9@protonmail.com
system_admC@protonmail.com	makalikozo@cock.li	onboardingbinder@proton.me
Protonmail.ch dark_sysadmin@protonmail.ch	makalikozo@protonmail.com	pyotrmaksim@gmail.com
iracomp1@protonmail.ch	hnx911@yahoo.com	wintzs@proton.me
iracomp3@protonmail[.[ch	virusjahid4209@cyberper.net	Barbara.li@gmx.com
LR_FWS_H2M_ET@protonmail.ch	viruszone4209@opentrash.com	emily.florez@zohomail.com
under_amur@protonmail.ch	zalton@tuta.io	getdataback@rambler.ru
Kkarrytech@skiff.com	mujkontakt@protonmail.com	amaya_payne2@aol.com
waterstatus@cock.li	niggapoopoo123@protonmail.com	nikki.lond2@aol.com
help@room155.online	imbun6@gmail.com	

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）。

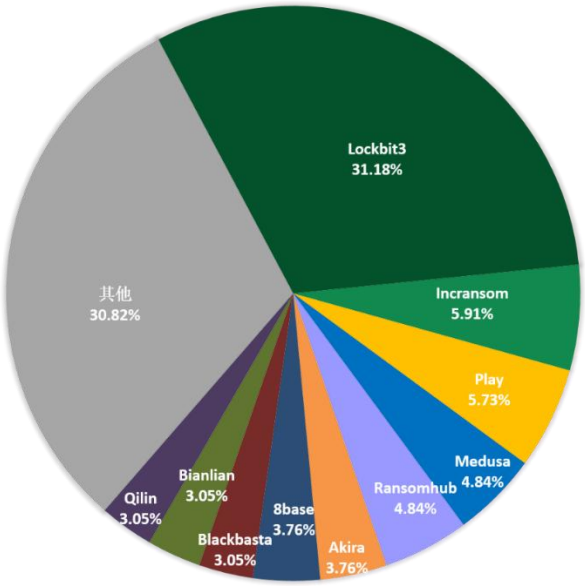

图 4. 双/多重勒索软件 5 月各家族占比

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 558 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。其中有 5 个组织/企业未被标明，因此不在以下表格中。

St. Helena	PRIMARYSYS.COM	Softura
New Hampshire PublicRadio	Formosa Plastics USA	Zuber Gardner CPAs
dollmar.com	Dean Lumber & Supply	Corr & Corr
familyguardian.com	WindCom	rexmoore.com
espackeuro.com	agranibank.org	Northeast Orthopedics and Sports Medicine
TriLiteral	laxmicapital.com.np	Glenwood Management
biremote.net	pricemodern.com	College Park Industries
keytronic.com	OKUANT - okuant.com	Holstein Association USA
Sems and Specials	valleyjoist.com	Unimed Vales do Taquari e Rio

		Pardo
strikeusa.com	fulcrum.pro	Electric Mirror Inc
aytosanlorenzo.es	Insurance Agency Marketing Services	Richelieu Foods
www.indigoent.ca	Baeckerei-raddatz.de	Trade-Mark Industrial
Rob's Whole Health Pharmacy	Colonial Surety Company	Dragon Tax and Management INC
Faultless Brands	kauffmanschool.org	Mewborn & DeSelms
DreamWall	ema-eda.com	Merritt Properties, LLC
Excel Security Corp.	twpunionschools.org	Autobell Car Wash, Inc
UNICRED.COM.AR	Chuo System Service Co.,Ltd	fortify.pro
MagicLand	East Shore Sound	Fribin
Wichita County Mounted Patrol	thermalsolutionsllc.com	consultingradiologists.com
Brownell Boat Stands & Equipment Company	escriba.com.br	Intuitae
Elmhurst Group	RIO TECHNOLOGY	williamsrdm.com
WALSER AUTOMOTIVE GROUP	Egyptian Sudanese	inforius
FPL Food	Consulting Radiologists	Kamo Jou Trading
Ntv	FIAB SpA	wichita.gov
Litigation Lawyers	Malone	City of Buckeye (buckeyeaz.gov)
Credit Central	Hardings Transport	Hibser Yamauchi Architects
Co, Chartered Accountants	Connelly Security Systems	Noritsu America Corp.
heras.co.uk	Motor Munich	Elbers GmbH & Co. KG
Western Dovetail	epsd.org	Jetson Specialty Marketing Services, Inc.
I.L.A. Local 1964	district70.org	Vega Reederei GmbH & Co. KG
mcmtelecom.com	keuka.edu	Max Wild GmbH
Aircod.com	allcare-med.com	woldae.com
Bjurholms kommun	Coplosa	Information Integration Experts
Manuchar	Surrey Place Healthcare & Rehabilitation	One Toyota of Oakland

Arrabawn Co-op	daubertchemical.com	Chemring Group
Avelina	BRAZIL GOV	lalengineering
OTR	Braz Assessoria Contábil	skanlog.com
Brett Slater Solicitors	Thibabem Atacadista	ctc-corp.net
PSG BANATSKI DVOR D.O.O. NOVI SAD (SERBIA)	FILSCAP	uslinen.com
Hohenadel	Cusat	tu-ilmenau.de
SIAED.it - HOSTER/DEV FOR ITALY BIGGEST BANKS	Frigrífico Boa Carne	thede-culpepper.com
Christies Auction House - christies.com	GOLD RH S.A.S	kimmelcleaners.com
S L B TRANSIT INC	Grupo SASMET	emainc.net
Information Technology	Neovia	southernspecialtysupply.com
Natsume Tax Accountant Corporation	City of Neodesha	lenmed.co.za
The Kelly Group	gravetye-manor	churchill-linen.com
Osaka Motorcycle Business Cooperative	Wealth Depot LLC	rollingfields.com
Matusima	morrisgroupint.com	srg-plc.com
Shirasaki	pierfoundry.com	gorrias-mercedes-benz.fr
Architecture LEJEUNE GIOVANELLI	GMJ & Co, Chartered Accountants	JFK Financial Inc.
Hytera US Inc	Fiskars Group	Central Florida Equipment
alliedtelesis.com	Bruno generators (Italian manufacturing)	High Performance Services
Datanet	Rocky Mountain Sales	Mauritzon
CNPC Sport	Talley Group	Somerville
Esc Pau Etudes-Conseils	acla.de	Donco Air
Aéroport de Pau	Watt Carmichael	Affordable Payroll & Bookkeeping Services

Israel Textile	500gb/www.confins.com.br/10kk/BR/Come to chat or we will attack you again.	Utica Mack
Israel Massad Quality	eucatex.com.br	KC Scout
Israel largest cyber security college	LPDB KUMKM LPDB.ID/LPDB.GO.ID	Sentry Data Management
Israel 99 Digital!	Accurate Lock and Hardware	NELLESFRERES
Israel Radars!	Monocon International Refractory	aletech.com.br
Kashin Distillery	Persyn	Young Consulting
High Group	Aero Tec Laboratories	Thaayakam LTD
Amigour Company	Altipal	The Weinstein Firm
Harmony Pharm	Municipalité La Guadeloupe	Nikolaus & Hohenadel
Ramat Gan Academic College	Eden Project Ltd	M2E Consulting Engineers
National Publisher Services LLC	Helapet Ltd	NRS Healthcare
Payne & Jones	oseranhahn.com	gammarenax.ch
Wind Composite Services Group, LLC	jmjcorporation.com	oraclinical.com
Assist Informatica	countyins.com	acsistemas.com
multigroup.info	utc-silverstone.co.uk	cpashin.com
pressurejet.com	hesperiausd.org	epr-groupe.fr
mgops.sedziszow-mlp.pl	Eden Project	isee.biz
kharafiglobal.com	Treasury of Cote d'Ivoire	cdev.gc.ca
sunpetro.com	scanda.com.mx	netspectrum.ca
cafesnovell.com	acfin.cl	qstartlabs.com
highwaystrust.com	New Boston Dental Care	syntax-architektur.at
sysroad.com	Service public de Wallonie	carespring.com
longviewoms.com	Cushman Contracting Corporation	grand-indonesia.com
Access Sports Medicine & Orthopaedics	Costa Edutainment SpA	remagroup.com
Crandall ISD (CISD.crandallisd.org)	Sigmund Espeland AS	telekom.com

S&F Concrete Contractors	Brovedani Group	aev-iledefrance.fr
bnsgroup.co.uk	Fic Expertise	elarabygroup.com
Ipsotek LTD	W.I.S. Sicherheit	thebiglifegroup.com
Vannguard Utility Partners	Brick Court Chambers	sonoco.com
workscapes.com	Seaman's Mechanical	ville-bouchemaine.fr
EMPIRECOMFORT.COM	Deeside Timberframe	Rafael Viñoly Architects
kns.com	McSweeney / Langevin	TRC Talent Solutions
Audubon Nature Institute (audubooninstitute.org)	NITEK International LLC	eskarabajo.mx
colfax.k12.wi.us - $150.000	National Metalwares, L.P	eviivo.com
Sichuan Dowell Science and Technology Company Inc	Romeo Pitaro Injury & Litigation Lawyers	kras.hr
hiawathahomes	Jackson County	tdt.aero
valleylandtitleco.com	21stcenturyvitamins.com	svenskakyrkan.se
brightwayconsultants.co.uk	Montgomery County Board of Developmental Disabilities Services	htcinc.com
Nutec Group	LiveHelpNow	irc.be
United Urology Group	NK Parts Industries	geotechenv.com
Hands TheFamilyHelpNetwork.ca	Badger Tag & Label	ishoppes.com
iseta.fr (institut des Sciences de l'Environnement et des Territoires d'Annecy)	Haumiller Engineering	parat-techology.com
ICC	Crescent Point Energy	getcloudapp.com
Royal Star & Garter	Barid soft	yucatan.gob.mx
Advance Press	Reading Electric	arcus.pl
IZOMAT Praha	Pella	Nestoil
GRANVILLE FOOD CARE LIMITED	Kuhn Rechtsanwlte GmbH	Patterson & Rothwell Ltd
J & N Stone	colonialsd.org	Boyden

Newman Ferrara	wisconsinindustrialcoatings.com	W.F. Whelan
Cressex Community School	amsoft.cl	Seneca Nation Health System
Hedbergs	cultivarnet.com.br	COMPEXLEGAL.COM
Richland City Hall	ecotruck.com.br	ikfhomefinance.com
Midwest Covenant Home	iaconnecticut.com	cmactrans.com
First Nations Health Authority (fnha.local)	incegroup.com	ids-michigan.com
Golden Acre	Banco central argentina	provencherroy.ca
Ryder Scott Co.	Administração do Porto de São Francisco do Sul (APSFS)	swisspro.ch
Tri-state General Contractors	lavalpoincon.com	olsonsteel.com
Starostwo Powiatowe w Świebodzinie	ufresources.com	teaspa.it
Aspire Tax	cloudminds.com	ayesa.com
The Louis G Freeman	calvia.com	synlab.com
Experis Technology Group	manusa.com	active-pcb.com
Anchorage Daily News	habeco.com.vn	gai-it.com
RDI-USA	rehub.ie	The Islamic Emirat of Afghanistan National Environmental Protection Agency
Ardenbrook	torrepacheco.es	Accounting Professionals LLC. Price, Breazeale & Chastang
Visa Lighting	ccofva.com	Macildowie Associates
Semicore Equipment	dagma.com.ar	Mainline Health Systems (MHS.local)
Levin Porter Associates	Edlong	Dr Charles A Evans
Critchfield & Johnston	dpkv.cz	Universidad Nacional Autónoma de México

shamrocktradingcorp.com	hetero.com	Bitfinex
londondrugs.com	vikrantsprings.com	SBC Global
schmittyandsons.com	doublehorse.in	Rutgers University
ThrottleUp	iitm.ac.in	Coinmoma
ramfoam.com	cttxpress.com	kc.co.kr
ALO diamonds	garage-cretot.fr	sharik
Brittany Horne	hotel-ostella.com	tdra
William S. Hein & Co.	vm3fincas.es	fanr.gov.ae
Aztec Services Group	thaiagri.com	Bayanat
International Modern Hospital	tegaindustries.com	kidx
Heras	kioti.com	MCS
mfgroup.it	taylorcrane.com	Tohlen Building Technology Group
grupocadarso.com	grc-c.co.il	Stainless Foundry & Engineering
atlasoil.com	mogaisrael.com	US-Saudi Arabian Business Council
trugreen.com	ultragasmexico.com	Ayoub & associates CPA Firm
levian.com	eif.org.na	www.servicepower.com
lactanet.ca	auburnpikapp.org	www.credio.eu
Matadero de Gijón - Biogas energy plant - mataderodegijon.es	acla-werke.com	Lopez Hnos
American Clinical Solutions(acslabtest.com)	college-stemarie-elven.org	GWF Frankenwein
ORIUX: Experts in Mobility	snk.sk	Reederei Jüngerhans
Jess-link Products	mutualclubunion.com.ar	extraco.ae
MAH Machine	rfca.com	watergate
Marigin	hpo.pe	Canatal Industries
GE Aerospace	spu.ac.th	Lewis Brothers Bakeries
Crooker	livia.in	S.A. Piazza & Associates
Embellir	cinealbeniz.com	MyoVision

LEMKEN	truehomesusa.com	Woodfords Family Services
Berge Bulk	uniter.net	Calumet Civil Contractors, Inc.
California Highway Patrol (SVEL237.org)	itss.com.tr	Imedi L
qualityplumbingassociates.com	elements-ing.com	SHAMASS.ORG
Regional Obstetrical Consultants	heartlandhealthcenter.org	Trylon Srl
Specialty Market Managers	dsglobaltech.com	Azteca Tax Systems
Sterling Transportation Services (sts.local)	alian.mx	Clinica de Salud del Valle de Salinas
schuettemetals.com	evw.k12.mn.us	Studio Libeskind
allied-mechanical-services-inc	mpeprevencion.com	bulldogbag.com
Patriot Machine, Updated data leak.	binder.de	frenckengroup.com
carcajou.fr	interfashion.it	synology.com
equinoxinc.org	vstar.in	tpa-group.sk
unisi.it	brfibra.com	Triathlon.group
Widdop & Co.	museu-goeldi.br	awwg.com
Colégio Nova Dimensão	doxim.com	KyungChang
catiglass.com $100.000	essinc.com	Y. Hata & Co., Ltd.
Bluebonnet Nutrition	sislocar.com	Skender Construction
Center for Digestive Health	depenning.com	Creative Business Interiors
drmsusa.com	asafoot.com	cochraneglobal.com
WEICON	frankmiller.com	hookerfurniture.com
County Connection	vitema.vi.gov	alimmigration.com
Elm Grove	snapethorpeprimary.co.uk	anatomage.com
Comwave	agencavisystems.com	bluegrasstechnologies.net
Mesopolys	salmonesaysen.cl	PINNACLEENGR.COM
Pittsburgh's Trusted Orthopaedic Surgeons	kowessex.co.uk	MCKINLEYPACKAGING.COM

Sullairargentina.com	totto.com	PILOTPEN.COM
www.belcherpharma.com	randi-group.com	colonial.edu
orga-soft.de	grupopm.com	cordish.com
Houston Waste Solutions	ondozabal.com	concorr.com
Shyang Shin Bao Ind. Co., Ltd. (hereinafter referred to as "SSB")	orsiniimballaggi.com	yupousa.com
Vision Mechanical	vinatiorganics.com	peaseinc.com
Gantan Beauty Industry	peninsulacrane.com	UK government
ABS-CBN Broadcasting	brockington.leics.sch.uk	MORTON WILLIAMS
Isaacs Odinocki	cargotrinidad.com	Pinnacle Orthopaedics
aharvey.nf.ca		

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 7、Windows 10 以及 Windows Server 2016。

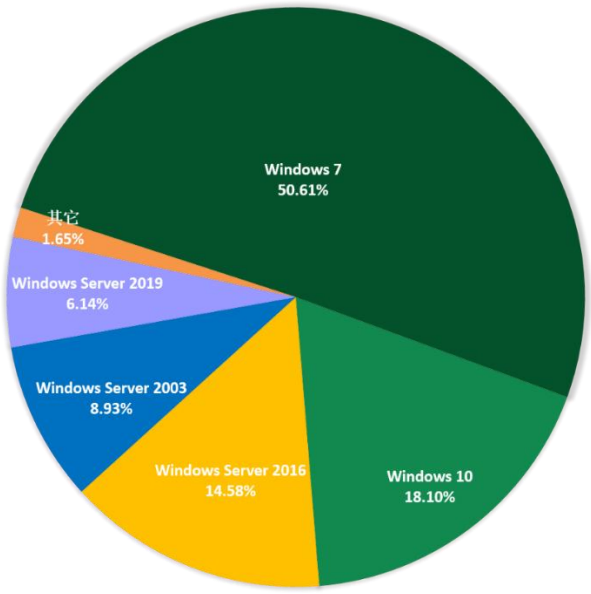

图 5. 黑客入侵防护 5 月各系统占比

对 2024 年 5 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。

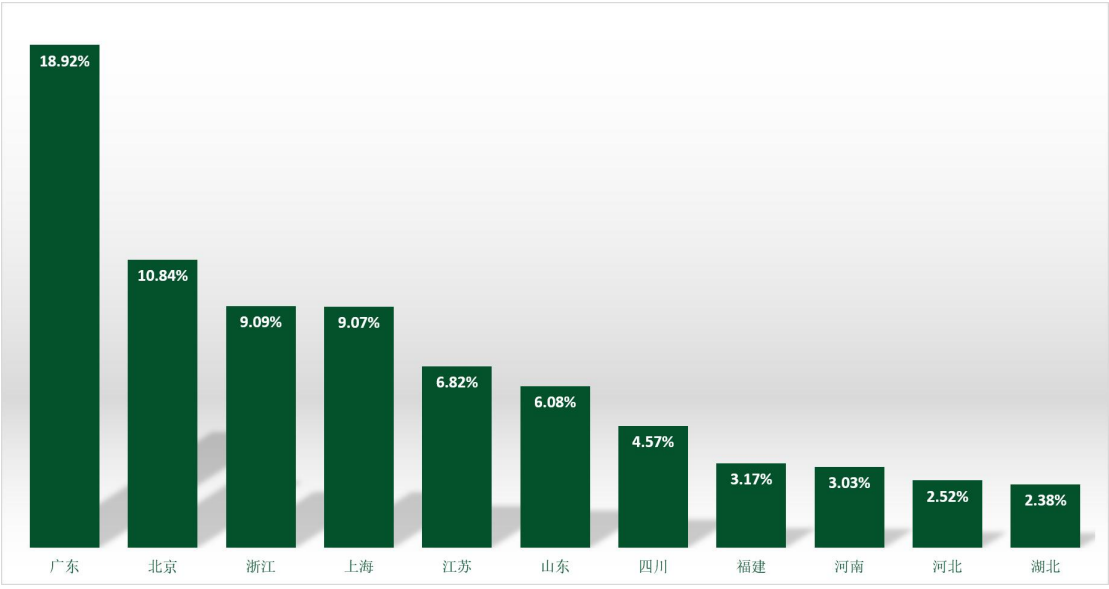

图 6. 黑客入侵防护 5 月各地区占比 Top

通过观察 2024 年 5 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。

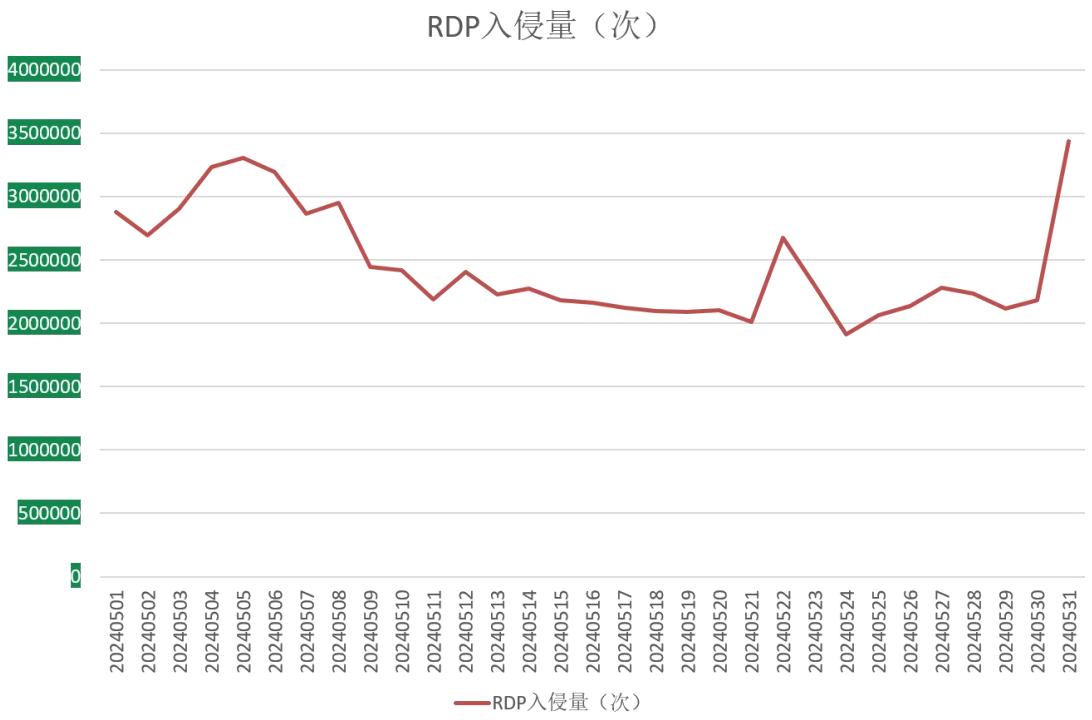

图 7. RDP 攻击在 5 月的入侵量

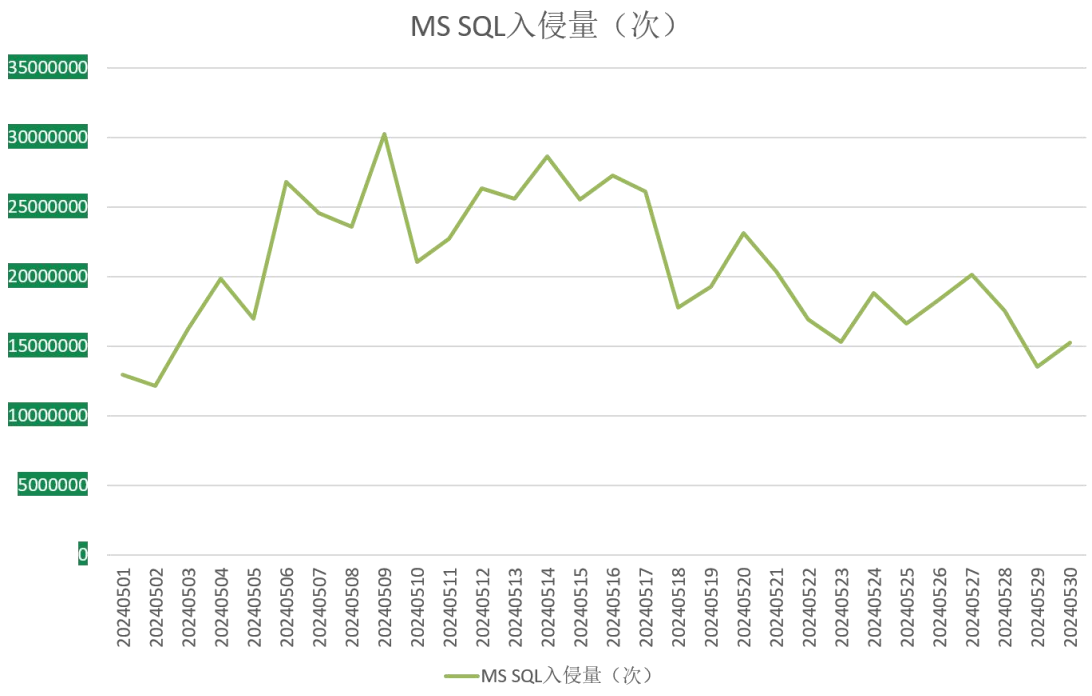

图 8. MS SQL 攻击在 5 月的入侵量

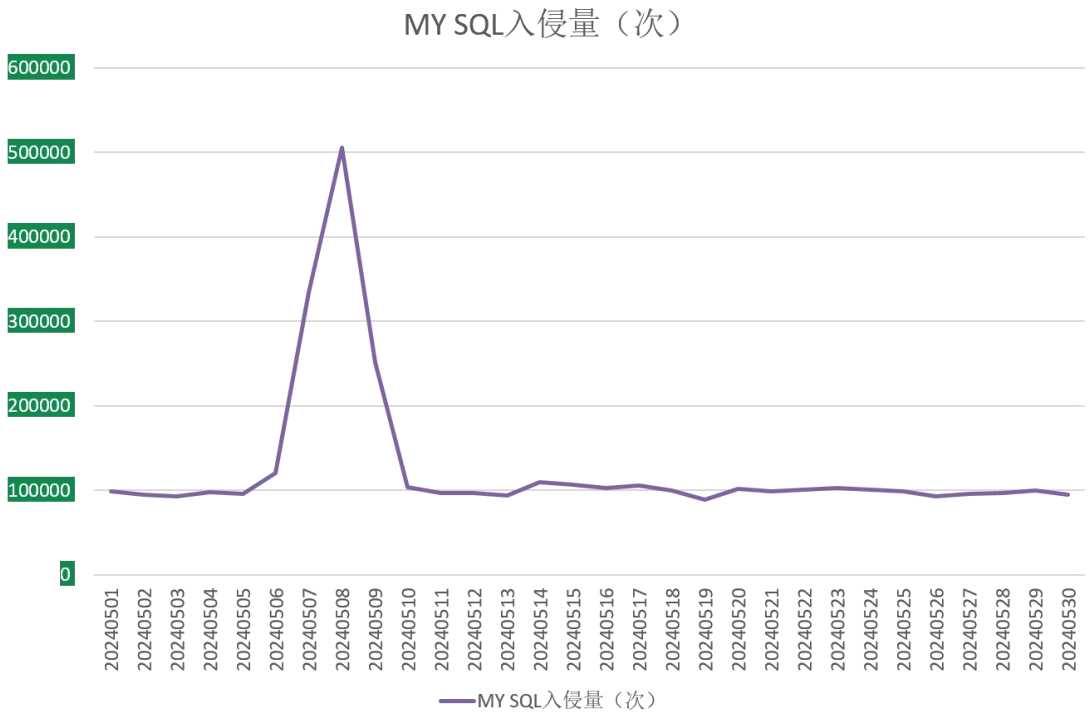

图 9. MY SQL 攻击在 5 月的入侵量

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。
- 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与数据库弱口令成功后手动投毒。
- svh：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。
- hmallox：同 rmallox。
- faust： 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。
- mkp：同 svh。
- blackbit 基于 Loki 勒索软件家族的修改版本，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：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 Web 应用漏洞利用进行传播。

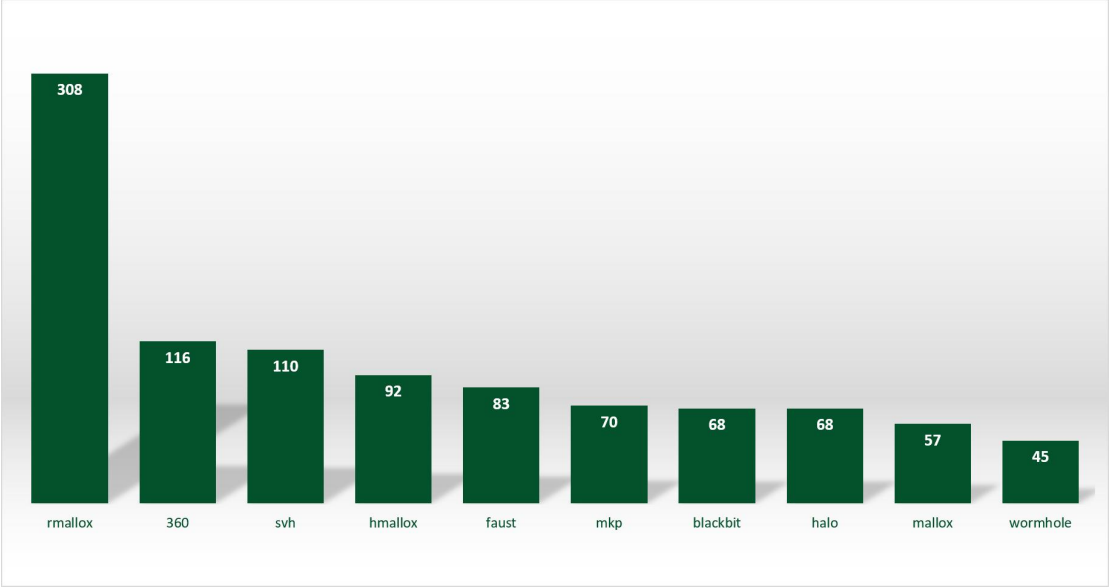

图 10. 勒索软件搜索引擎 5 月搜索关键词 Top10

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 Telsa。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。

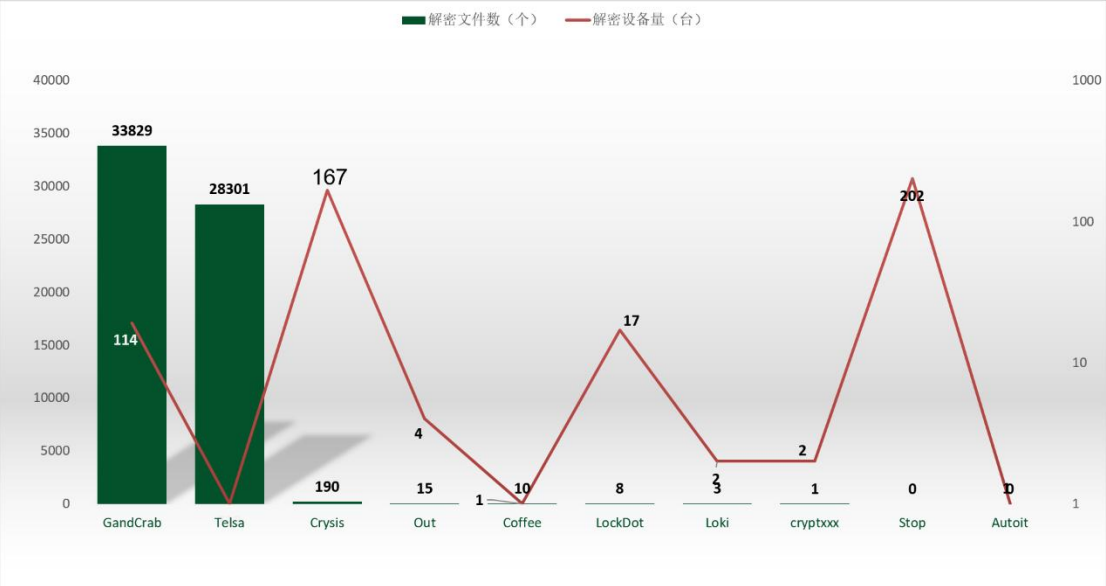

图 11. 解密大师 5 月解密受各家族感染的设备及文件数量 Top10


360数字安全
数 字 安 全 的 领 导 者
360安全大脑