勒索软件流行态势分析

2024 年 3 月

360数字安全
数 字 安 全 的 领 导 者
360安全大脑

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 3 月，全球新增的活跃勒索软件家族有 RA World、Red Ransomware、Kill Security 等，均为双重勒索病毒。

本月针对国内主流云服务器进行的勒索攻击比例大幅提高，从大量的云服务器用户反馈的案例看，相关系统均未安装 360 终端安全产品进行勒索防护，被攻击的直接原因主要是 Web 服务漏洞、数据库弱口令登录、远程桌面弱口令登录。

以下是本月值得关注的部分热点：

1. TellYouThePass 再度活跃
2. 瑞士表示 Play 勒索软件泄露了 65000 份政府文件
3. 法国失业机构数据泄露影响 4300 万人

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 17.98%居首位，第二的是占比 16.67%的 Makop，phobos 家族以 15.35%位居第三。

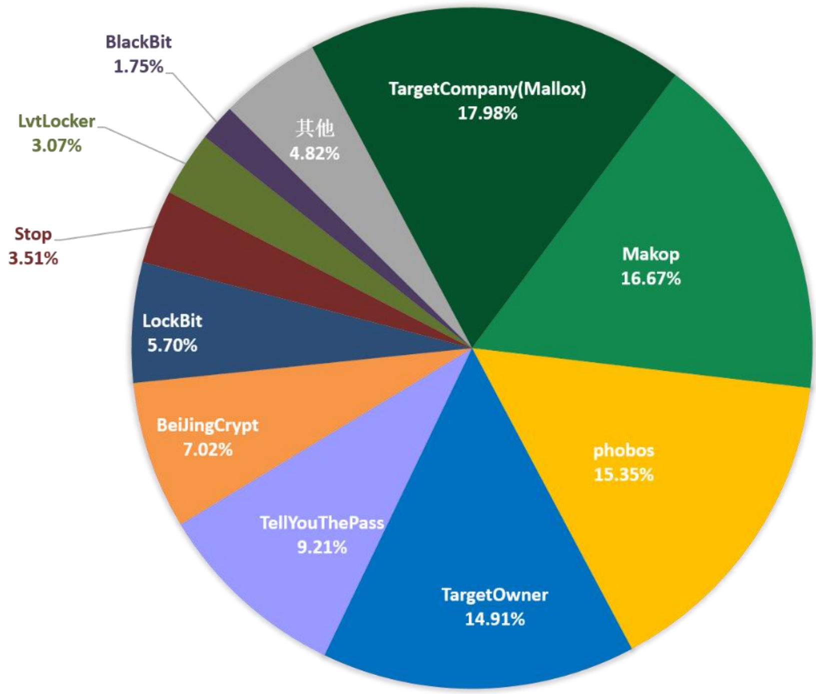

图 1. 2024 年 3 月勒索软件家族占比

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。

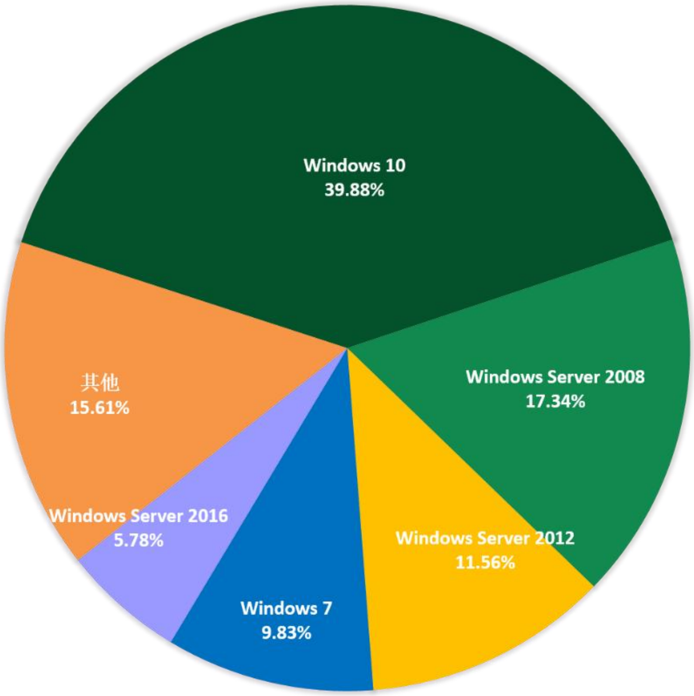

图 2. 2024 年 3 月勒索软件感染操作系统占比

2024 年 3 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 与服务器为主流平台，Nas 平台受 LvtLocker 勒索家族的持续影响，占比依然居高不下。

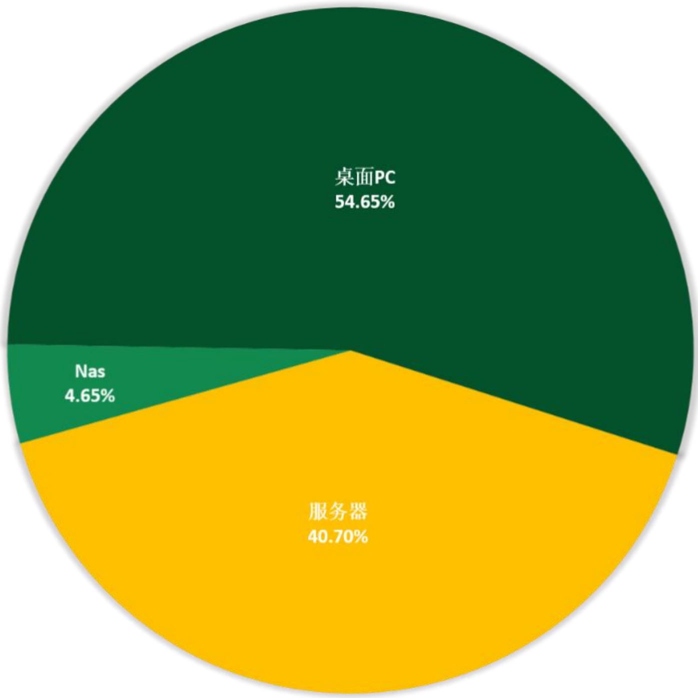

图 3. 2024 年 3 月勒索软件感染操作系统类型占比

勒索软件热点事件

TellYouThePass 再度活跃

3 月中旬与 3 月末 360 反勒索服务接到大量受害者反馈其设备中被植入了勒索软件。

而本月 TellYouThePass 勒索攻击的受害者都有着两个显著的共同特征：

1. 中招设备未安装 360 安全产品，且云服务器占比很高；

2. 中招设备均为运行财务管理服务的计算机。

经 360 安全智脑的分析研判，成功锁定了这一波攻击的来源为 TellYouThePass 勒索家族——一家擅长利用服务器漏洞进行规模化攻击的老牌勒索软件家族。

该家族仅在 2023 年就发动了 3 轮较大规模的攻击，而在 2024 年初又开始继续作恶。

而 360 云端智脑也为我们展示了其最近半年的攻击趋势，可以看到最近一段时间，其活跃程度显著增加：

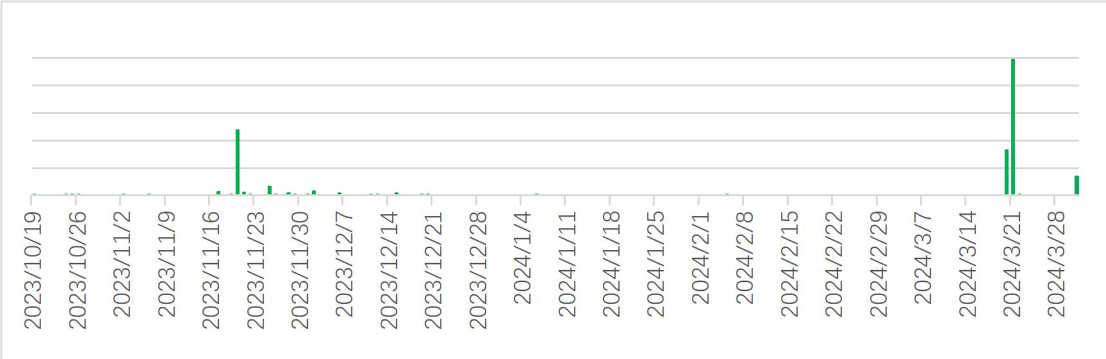

图 4. TellYouThePass 近期传播量

本轮集中爆发是该家族在龙年后的首度回归,仅在 3 月 20 日一天我们就监测到了数千台财务电脑遭其攻击。

瑞士表示 Play 勒索软件泄露了 65000 份政府文件

瑞士国家网络安全中心(NCSC)发布了一份报告，分析了 Xplain 遭受勒索软件攻击后的数据泄露情况，披露该事件影响了数千份敏感的联邦政府文件。Xplain 是一家瑞士技术和软件解决方案提供商，为各种政府部门、行政单位，甚至该国的军事力量提供服务。

当时，攻击者声称盗取了包含机密信息的文件，而其也确实在之后的 2023 年 6 月初兑现了该威胁，并在其暗网门户上发布了被盗数据。这之后，瑞士政府开始调查泄露的文件，并立即承认泄露的数据可能包含属于瑞士联邦管理局的文件。

2024 年 3 月 7 日，瑞士政府发布了一份关于此事的声明，称有 65000 份政府文件遭到泄露：

- 这些文件中的大部分(95%)影响了联邦司法和警察部(FDJP)的行政单位：联邦司法办公室、联邦警察办公室、国家移民秘书处和内部 IT 服务中心 ISC-FDJP。
- 联邦国防部、民防和体育部(DDPS)受到的影响较小，占该数据的 3%多一点。
- 大约 5000 份文件包含敏感信息，包括个人数据(姓名、电子邮件地址、电话号码和地址)、技术细节、机密信息和账户密码。
- 一个由几百个文件组成的小集合，包含 IT 系统文档、软件或架构数据和密码。

公告称调查将于本月底完成，并将与联邦委员会分享全部结果和网络安全建议。

法国失业机构数据泄露影响 4300 万人

2024 年 3 月 13 日，法国就业部披露黑客在 2 月 6 日至 3 月 5 日期间对其发动了网络攻击，窃取了过去 20 年在该机构注册的求职者详细信息，导致这些求职者个人数据遭到泄露。法国就业部已经通知了该国的数据保护机构——法国国家信息和自由委员会(CNIL)。而该机构表示，多达 4300 万人可能会受到影响。

此次攻击所泄露的数据类型包括:

- 全名
- 出生日期
- 出生地点
- 社会安全号码(NIR)
- 法国劳工身份识别码
- 电子邮件地址
- 邮寄地址
- 电话号码

这些数据增加了个人身份被盗和网络钓鱼的风险，因此该机构建议潜在的受影响人群对他们收到的电子邮件、电话和短信要特别警惕。法国劳工局澄清说，数据泄露事件不会影响人们的银行信息或账户密码。但法国国家信息保护委员会警告说，网络罪犯可能会利用这些信息与其他泄露事件中的被盗数据关联起来。

黑客信息披露

以下是本月收集到的黑客邮箱信息:

jimyjoy139@proton.me	secdatltd@gmx.com	payransom1@gmail.com
freaqzer@proton.me	fredmoneco@tutanota.com	MogilevichSupport@mail2tor.com
deblackbithelp@gmail.com	skymix@tuta.io	databack129@tuta.io
AlbetPattisson1981@protonmail.com	getdata@gmx.com	databack129@cock.li
henryk@onionmail.org	sory@countermail.com	reload2024@outlook.com
atomicday@tuta.io	greenbookBTC@gmx.com	oct@sent.com
info@fobos.one	spacegroup@tuta.io	sourcehack@nigge.rs
axdus@tuta.io	greenbookBTC@protonmail.com	decr.nem@tuta.io
it.issues.solving@outlook.com	stafordpalin@protonmail.com	imhere.ru77@gmail.com
barenuckles@tutanota.com	helperfiles@gmx.com	meowcorp2022@aol.com
JohnWilliams1887@gmx.com	starcomp@keemail.me	meowcorp2022@proton.me
Bernard.bunyan@aol.com	helpermail@onionmail.org	meowcorp@msgsafe.io
jonson_eight@gmx.us	xdone@tutamail.com	meowcorp@onionmail.org
bill.g@gmx.com	helpfiles@onionmail.org	4926564818284@tutanota.com
joshuabernandead@gmx.com	xgen@tuta.io	nice2meetyou@mail2tor.com
bill.g@msgsafe.io	helpfiles102030@inboxhub.net	nicetomeetyou@exploit.im
LettoIntago@onionmail.com	xspacegroup@protonmail.com	harry_whitest@zohomail.ca
bill.g@onionmail.org	helpforyou@gmx.com	harry.whitest@onionmail.org
Luiza.li@tutanota.com	zgen@tuta.io	data199@mailum.com
bill.gTeam@gmx.com	helpforyou@onionmail.org	poop69news@gmail.com
MatheusCosta0194@gmx.com	zodiacx@tuta.io	cmbi.pentesting@keemail.me
blair_lockyer@aol.com	companyadvanc@tutanota.com	hellomydata@onionmail.org
mccreight.ellery@tutanota.com	companyadvanc@onionmail.org	cedillos@cyberfear.com
CarlJohnson1948@gmx.com	flapalinta1950@protonmail.com	gratefulcode@gmail.com
megaport@tuta.io	xersami@protonmail.com	donexsupport@onionmail.org
cashonlycash@gmx.com	MarcusFeldmann1988@gmx.com	decryption@cock.lu
miadowson@tuta.io	web.assistant@onionmail.org	helpdata@zohomail.eu
chocolate_muffin@tutanota.com	imhere.ru@protonmail.com	email.recovery24@onionmail.org
MichaelWayne1973@tutanota.com	woxoto@tuta.io	pbdgja7el1@tutanota.com
claredrinkall@aol.com	assistant01@backup.capital	Er60t1@proton.me
normanbaker1929@gmx.com	assistant01@decodezone.net	h3lp2022@proton.me
clausmeyer070@cock.li	HG57iQqPL@gmail.com	h3lp2022@tuta.io
nud_satanakia@keemail.me	backmydata@skiff.com	websalm@tutanota.com
colexpro@keemail.me	stenlicyber@onionmail.com	jayy@tuta.com
please@countermail.com	stenlicyber@tutanota.com	hpssupfast@mailfence.com
cox.barthel@aol.com	qqtiq@tuta.io	info@fobos.one,axdus@tuta.io
precorpman@onionmail.org	miltonqq@tuta.io	ea7rt3nu0k@onionmail.org
recovery2021@inboxhub.net	antich154@privatemail.com	nicetomeetyou@onionmail.org
everymoment@tuta.io	rikyrank113@protonmail.com	dorradocry@outlook.com
recovery2021@onionmail.org	zinok19998@tuta.io	decryption@msgden.com
expertbox@tuta.io	santafun@email.tg	RestorationGuarantee@gmx.co
SamuelWhite1821@tutanota.com	decrypt2024@skiff.com	bkpdoclaso@proton.me
fastway@tuta.io	decrypt2024@onionmail.com	cc7ddos@airmail.cc

SaraConor@gmx.com	tramoryp@proton.me	fquatela@techie.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）。

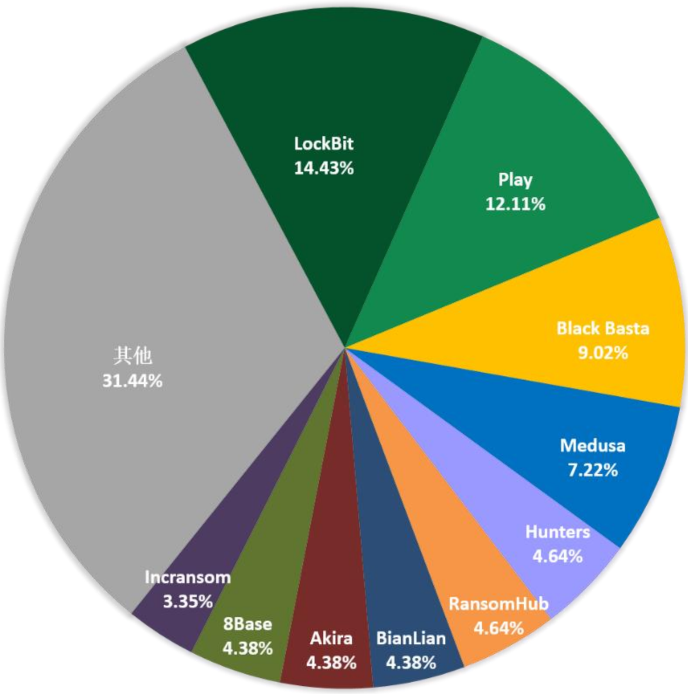

图 5. 2024 年 3 月通过数据泄露获利的勒索软件家族占比

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 388 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 4 个组织/企业未被标明，因此不在以下表格中。

rjcorp.in	go4kora	politiaromana.ro
A&A Wireless	gpaa.gov.za	polycab.com
Accipiter Capital Management, LLC	Grassmid Transport	Ponoka.ca
Acculabs Inc	Graypen Ltd	Power Generation Engineering and Services Company (PGESCo) - pgesco.com

ACE Air Cargo	Greenline Service	PowerRail Distribution
ACS	Group Health Cooperative - Rev 500kk	Powill Manufacturing & Engineering
activeconceptsllc.com	grupatopex.com	Premier Technology
aerospace.com	H + G EDV Vertriebs	prodrive.com
Affiliated Dermatologists and Dermatologic Surgeons	Haivision MCS	Prompt Financial Solutions
AGL	Hallesche Kraftverkehrs & Speditions GmbH	PSEC Church
agribank.com.na	Hartz	pstrans.com
airbogo	hawita-gruppe	PT Bank Pembangunan Daerah Banten Tbk
Alber Law Group	HC Querétaro	ptsmi.co.id
Aluminumtrailer.com	hdstrading.com	QEO Group
America Chung Nam orACN	Hedlunds	QI Group
American Nuts	Henry County, Illinois	qosina.com
American Renal Associates	highfashion.com.hk	Quality Enclosures
amerlux.com	Hozzify	rabitbd.com
ammega.com	HSI	Rafum Group
anovahealth.com	consorzioinnova.it	Ramdev Chemical Industries
ATL Leasing	HUDSONBUSSALES.COM	rameywine.com
ATMCo	iamdesign.com	Ranzijn
automotionshade.com	iemsc.com	Red River Title
Autorità di Sistema Portuale del Mar Tirreno Settentrionale It	igf-inc.com	redwoodcoastrc.org
Avant IT Norway	Image Pointe	Reeves-Wiedeman
Barrie and Community Family Health Team	Impac Mortgage Holdings	regencymedia.com.au
Baystate.edu	imperialtrading.com	Regina Dental Group
Bechtold	In****GmbH	Rekamy
Bendallmednick	Indoarsip	renypicot.es
bergmeister.eu	Industrial de Alimentos EYL SA	Retirement Line
Big Issue Group	Influence Communication	rmhfranchise.com
Biomedical Research Institute	Infosoft	roehr-stolberg.de
Bira 91	interluxury.com	Romark Laboratories
BiTec	ipmaltamira	rrib.com
Boingo Graphics	isophon glas GmbH	RSHP
Brewer Davidson	Jasper-Dubois County Public Library	Ruda Auto
Bridger Insurance	JM Thompson	rushenergyservices.com
brightwires.com.sa	journeyfreight.com	Saglobal.com
Brooks Tropicals	jovani.com	Santa Cruz Seaside
bulwarkpestcontrol.com	Judge Rotenberg Center	SBM & Co
Burnham Wood Charter Schools	JVCKENWOOD	SBM & Co
Butler, Lavanceau & Sober	K2systems.ca	sbmandco.com

Bwizer	Kaplan	Scadea Solutions
Calida	Keboda Technology Co., Ltd.	Schokinag
Canada Revenue Agency	kelson.on.ca	schuett-grundei.de
carolinafoodsinc.com	Kenneth Young Center	SchwarzGrantz
Casa Santiveri	keralapolice.gov.in	Seven Seas Group
Centennial Law Group LLP	keystonetech.com	Sfi-wfc.com
central.k12.or.us	kh.org	Shooting House
certifiedcollection.com	kmbdg.com	SHORTERM GROUP
Chambers Construction Co.	Kogok.com	SIEA
CHOCOTOPIA	Koi Design	sierralobo.com
CHRG	Kolbe Striping	SJCME.EDU
Chris Argiropoulos Professional	Kool-air	Skyland Grain
CLARK Material Handling Company	Kovra	smuldes.com
Claro	krueth.de	Solucionesls.com
cleshar.co.uk	Kudulis Reisinger Price	Sophiahemmet University
Coastal Car	Kumagai Gumi Group	South St Paul Public Schools
colefabrics.com	La Pastina	South Star Electronics
Comohotels.com	lagunitas.com	Southcoindustries.com
Compact Mould	Lakes Precision	SP Mundi
Computan	Lambda Energy Resources	Sprimoglass
Consolidated Benefits Resources	lavelle.com	Springfield Sign
contechs.co.uk	Law Offices of John V. Orrick, P.L.	SREE Hotels
contenderboats.com	Lawrence Semiconductor Research Laboratory	Stack Infrastructure
Continental Aerospace Technologies	lec-london.uk	starkpower.de
Control Technology	Lieberman LLP	Steiner (Austrian furniture makers)
CoreData	lifelinedatacenters.com	Sting AD
Cosmocolor	Lindos Group Of Companies	stockdevelopment.com
countryvillahealthservices.com	lindquistinsurance.com	Stoney Creek Furniture
cpacsystems.se	Lindsay Municipal Hospital	Suburban Surgical Care Specialists
creativeenvironments.com	linksunlimited.com	SummerFresh
Crimsgroup	Liquid Environmental Solutions	Summit Almonds
crinetics.com	Lodan Electronics Inc	Sun Holdings
Crystal Window & Door Systems	logistasolutions.com	sunholdings.net
Delta Pipeline	londonvisionclinic.com	sunwave.com.cn
Denninger's	lostlb	Sysmex
Desco Steel	MainVest	Tanis Brush
dgse.com	MarineMax	Tbr Kowalczyk
dhanisisd.net	Marketon	Tech-Quip Inc
dismogas	Martin's, Inc.	Tecnolite.com
DiVal Safety Equipment, Inc.	Mayer Antonellis Jachowicz & Haranas, LLP	Telecentro
dkpvlaw.com	McKim & Creed	Teton Orthopaedics

Dörr Group	mckimcreed.com	THAISUMMIT.US
Dr. Leeman ENT	Medical Billing Specialists	Therapeutic Health Services
Dunbier Boat Trailers	Mediplast AB	THESAFIRCHOICE.COM
duttonbrock.com	Merchant ID	theshootingwarehouse.com
dutyfreeamericas.com	Mermet	Thors-Data.dk
duvel.com | boulevard.com	Metzger Veterinary Services	Title Management Inc
DVT	Miki Travel	tmbs.ch
earnesthealth.com	Miki Travel Limited	tmt-mc.jp
Eastern Rio Blanco Metropolitan	Ministry of Defense of Peru	Tocci Building Corporation
eclinicalsol.com	mioa.gov	Topa Partners
Ejército del Per	mirel	Trans+Plus Systems
El Debate	mjcelco.com	triella.com
elezabypharmacy.com	moperry.com	UNDP
Elior UK	nampak.com	unitednotions.com
elmatic.de	neigc.com	Urban Strategies
elsapspa	NetVigour	US #1364 Federal Credit Union
en-act-architecture	Neurobehavioral Medicine Consultants	valoremreply.com
Encina Wastewater Authority	New Bedford Welding Supply	vdhelm
Enplast	New York Home Healthcare	Veeco
Equatorial Energia	newagesys.com	Vhs-vaterstetten.de
ero-etikett.com	newmans-online.co.uk	viadirectamarketing
esser-ps.de	NHS Scotland	vilis.com
European Centre for Compensation	northamericansigns.com	Vita IT
everplast	northerncasket.com	voidinteractive.net you are welcome in our chat
Ewig Usa	oceaneering.com	vsexshop.ru
excellifecoaching.com	organizedliving.com	WALKERSANDFORD
Exela Technologies	ÖSTENSSONS LIVS AB	Ward Transport & Logistics
Fashion UK	Otolaryngology Associates	Watsonclinic.com
FBi Construction	otrwheel.com	wblight.com
Federchimica	oyaksgs.com.tr	Weld Plus
Felda Global Ventures Holdings Berhad	P&B Capital Group	West Monroe
Festspielhaus Baden-Baden	paginesi	White Oak Partners
Filexis AG Treuhand und Immobilien	Palmer Construction Co., Inc	Williams County Abstract Company
Fincasrevuelta	Pantana CPA	Winona Pattern & Mold
Florida Memorial University	Panzeri Cattaneo	Withall
flynncompanies.com	Pascoe International	Woodsboro ISD
Forstinger Österreich GmbH	pathologie-bochum.de	worthenind.com
fpdcompany.com	Paul Davis Restoration	Wurzbacher
Frawner	Pavilion Construction	www.duvel.com
Future Generations Foundation	Pavilion Construction LLC	www.loghmanpharma.com
Gansevoort Hotel Group	pbgbank.com	xcelbrands.com
Gascontec.com	pcscivilinc.com	yarco.com

geruestbau.com	pctinternational.com	Zips Car Wash
gfad.de	Petrus Resources Ltd	plymouth.com
Gilmore Construction	PFLEET	Global Zone

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 10。

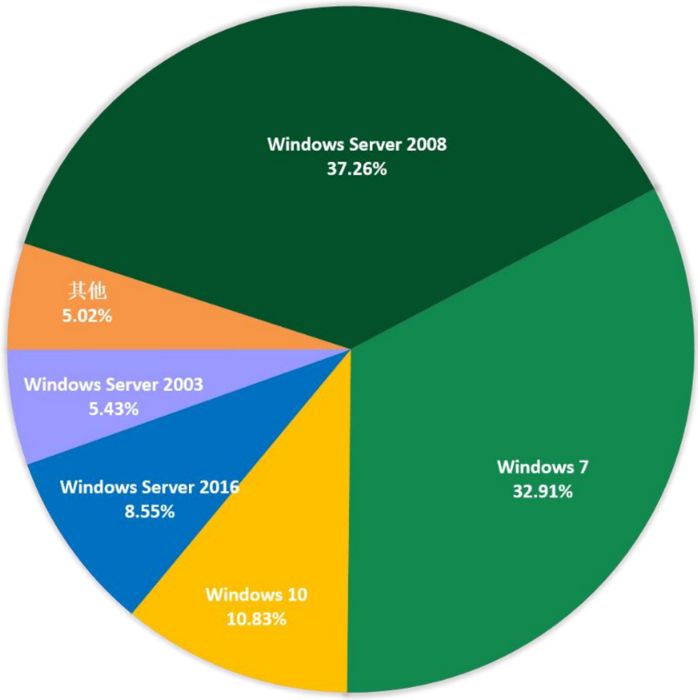

图 6. 2024 年 3 月黑客入侵各操作系统占比

对 2024 年 3 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。

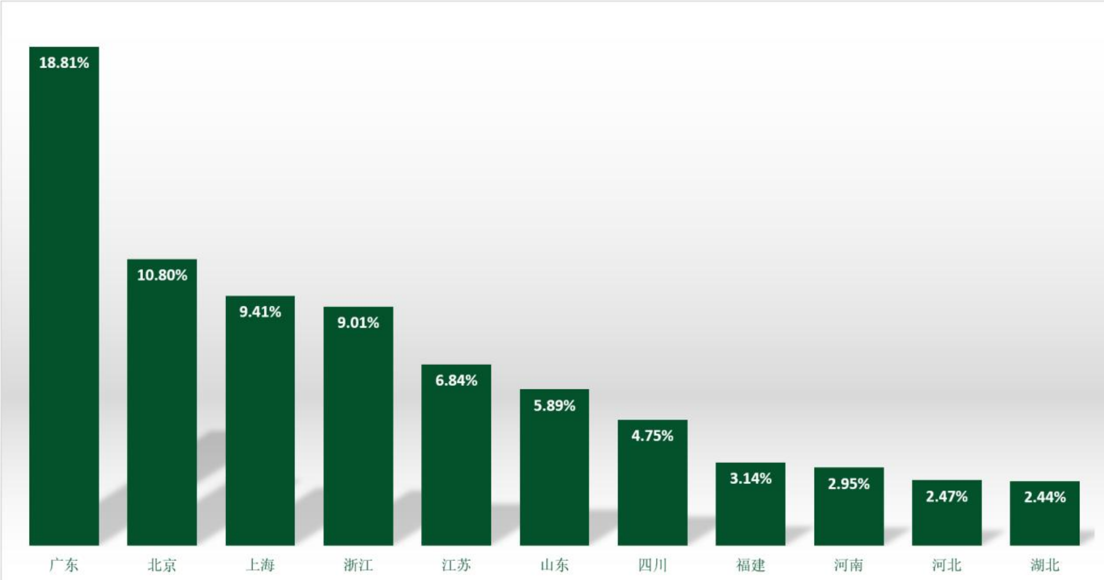

图 7. 2024 年 3 月国内受攻击地区占比

通过观察 2024 年 3 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。

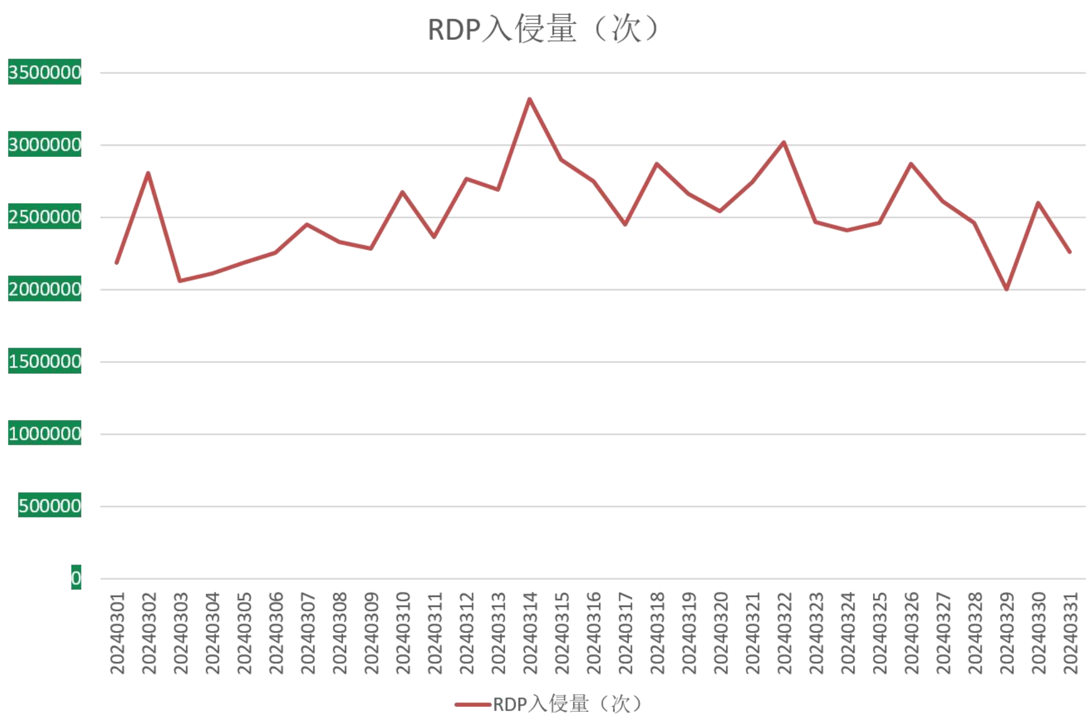

图 8. 2024 年 3 月 RDP 遭入侵量

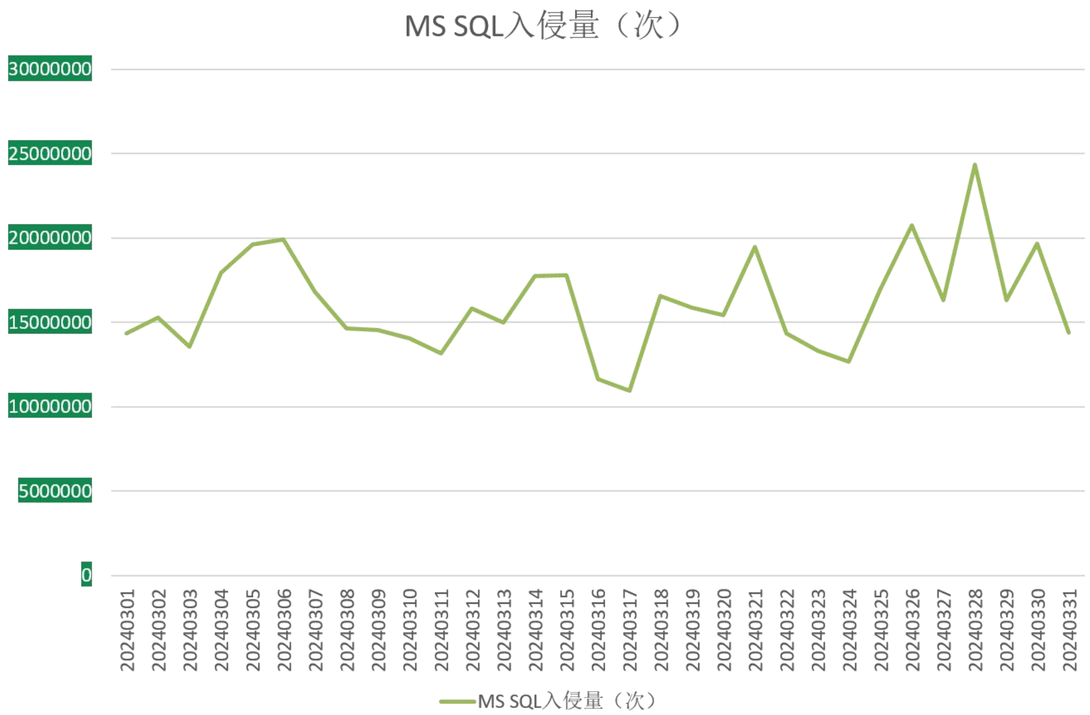

图 9. 2024 年 3 月 MSSQL 遭入侵量

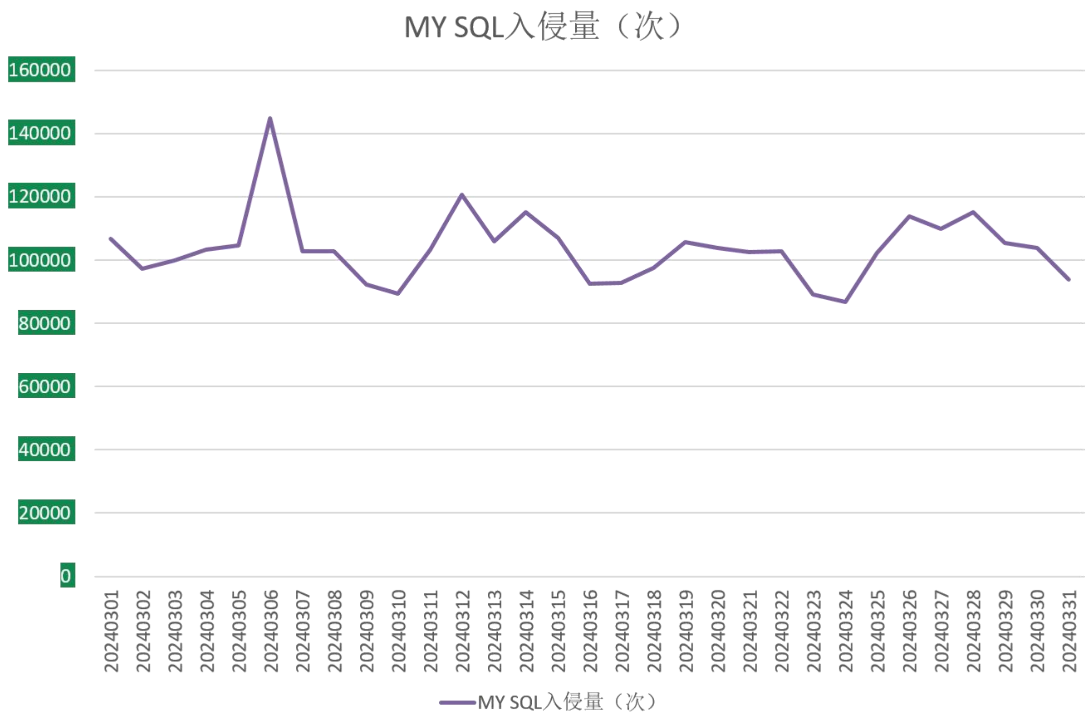

图 10. 2024 年 3 月 MYSQL 遭入侵量

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。

- 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。
- 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。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。
- helper：属于 TargetOwner 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： 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与数据库弱口令成功后手动投毒。
- mkp：同 wis。
- devos 同 faust。
- halo：同 360。

- mallox：同 rmallox。

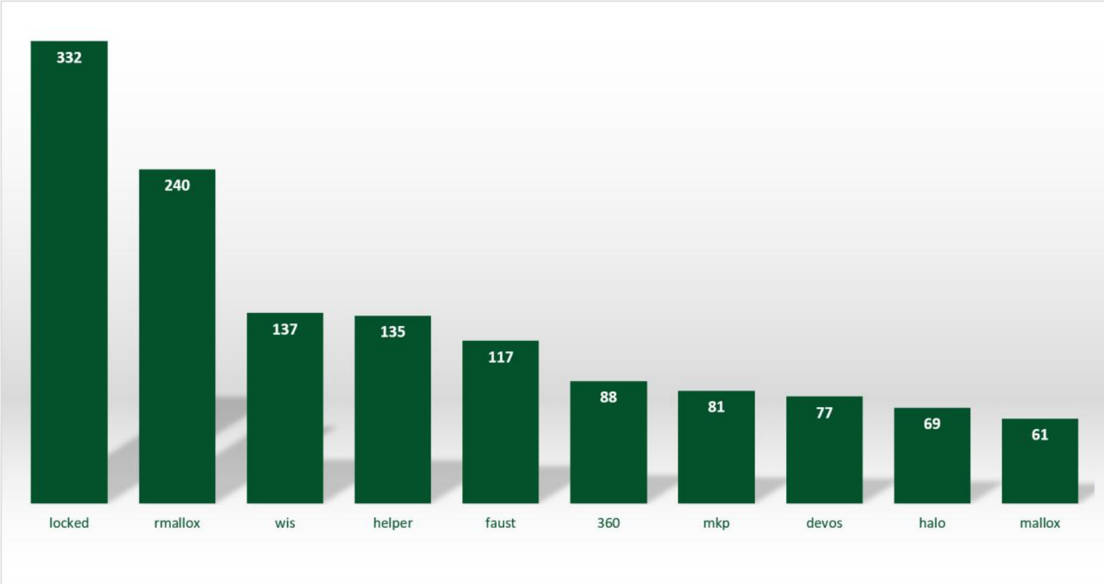

图 11. 2024 年 3 月勒索软件搜索量排行

解密大师

从解密大师本月解密数据看，解密量最大的是 Autoit，其次是 Crysis。使用解密大师解密文件的用户数量最高的是被 Stop 家族加密的设备。

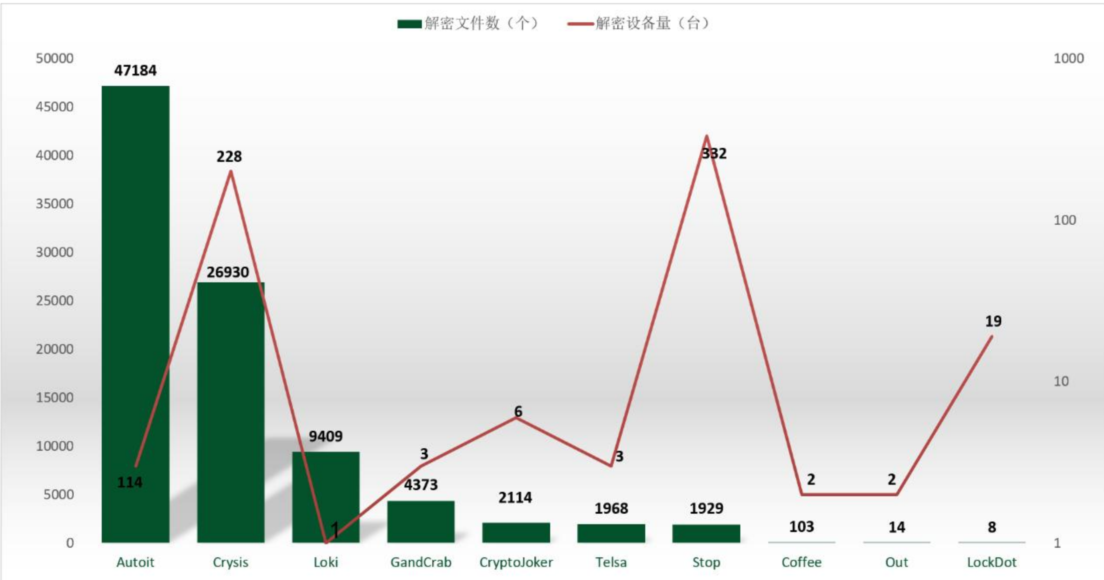

图 12. 2024 年 3 月解密大师解密量

360数字安全

数 字 安 全 的 领 导 者

360安全大脑