勒索软件流行态势分析

2024 年 4 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 4 月，全球新增的双重勒索软件家族有 EMBARGO、Space Bears、Qiulong、DarkVault、dAn0n、Dispossessor、APT73、HelloGookie。国内的新增的勒索软件家族有 Wormhole 与 wuibei。前者在国内通过第三方软件漏洞进行广泛传播，后者则通过钓鱼邮件利用人们的猎奇心理进行传播。

本月老牌勒索软件 TargetCompany（Mallox）家族后缀为 rmallox 的变种，在攻击方式上增加了对国内各主流第三方软件 web 漏洞的利用。

以下是本月值得关注的部分热点：

1. Web 漏洞利用攻击逐渐成为国内勒索软件主流攻击方式

2. 托管公司的 VMware ESXi 服务器遭新型 SEXi 勒索软件攻击

3. 芯片制造商安世在遭勒索软件公布数据后确认数据泄露

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 22.83%居首位，第二的是 TargetCompany(Mallox)占比 20.55%，phobos 家族以 19.18%位居第三。

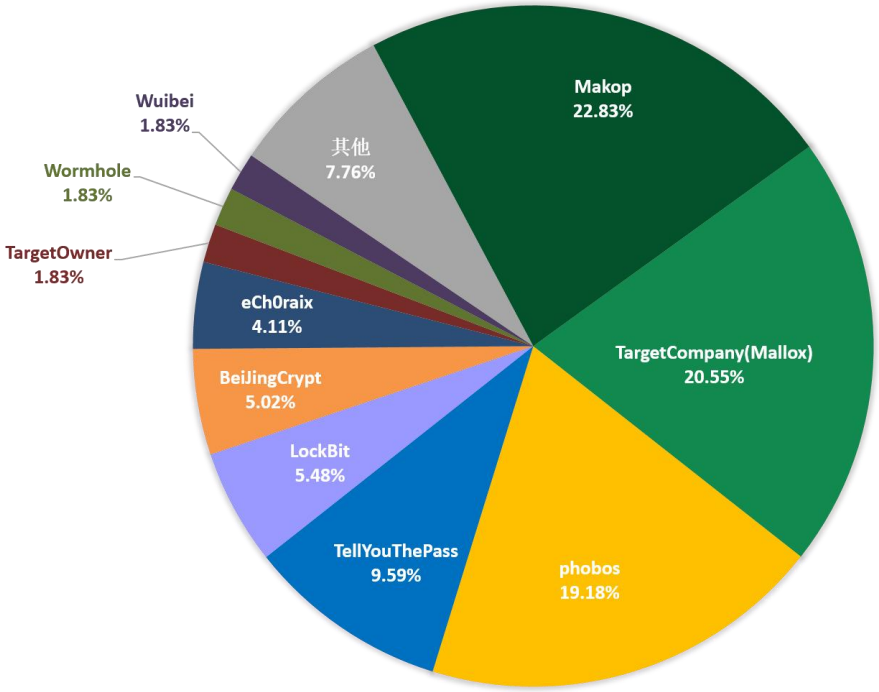

图 1. 2024 年 4 月勒索软件家族占比

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 2012 以及 Windows Server 2008。

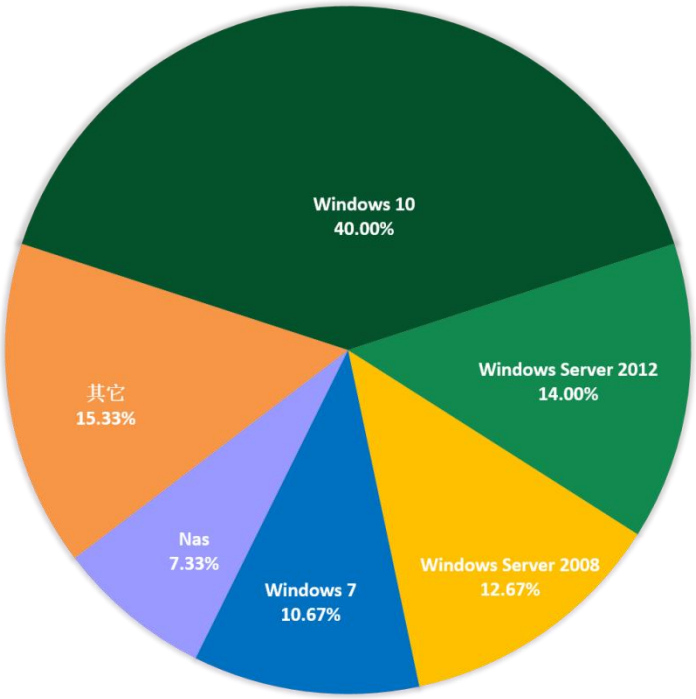

图 2. 2024 年 4 月勒索软件感染操作系统占比

2024 年 4 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 平台持续有勒索软件攻击检出。

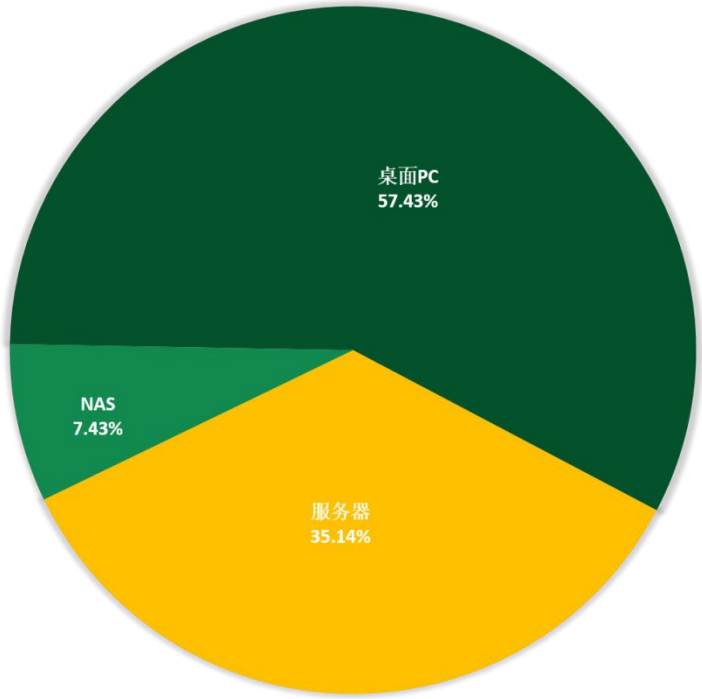

图 3. 2024 年 4 月勒索软件感染操作系统类型占比

勒索软件热点事件

Web 漏洞利用攻击逐渐成为国内勒索软件主流攻击方式

本月老牌勒索软件 TargetCompany（Mallox）家族以及国内新增的 Wormhole 勒索软件家族均开始采用 Web 漏洞利用方式进行传播。此前该方式长期曾被 TellYouThePass 家族频繁采用，预示着自 4 月起国内不同的勒索团伙间也开始在相同的攻击渠道入口“卷”起来了。

以下是 360 安全大脑监控到的 Wormhole 家族利用 Web 漏洞入侵攻击现场命令行快照

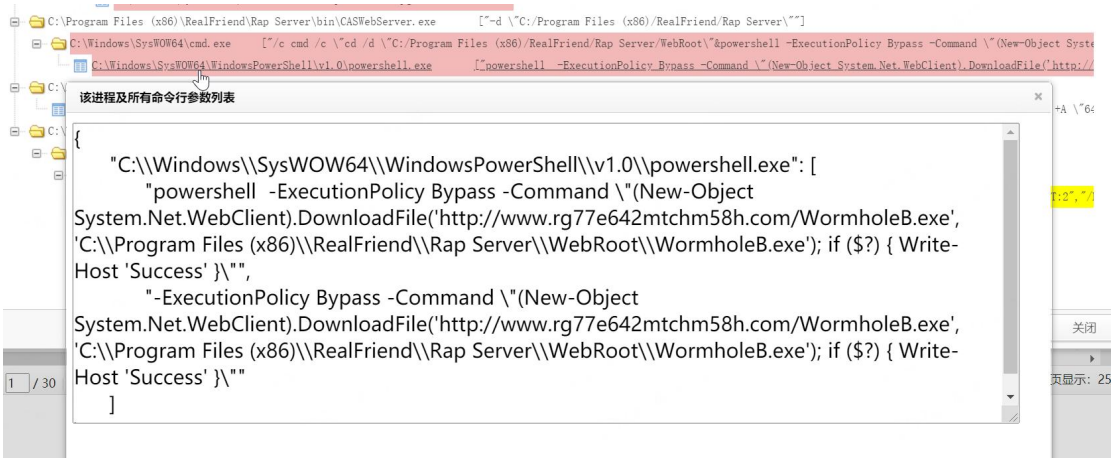

图 4. Wormhole 勒索软件入侵现场快照

漏洞利用类勒索病毒异常活跃，典型攻击目标包括：瑞友天翼、恩软 EnterCRM、亿赛通电子文档管理系统、金蝶 K3Cloud、金蝶星空云、海康威视 IVMS、用友时空 KSOA、用友 U8、用友时空 CCERP、用友时空 CDM、速达天耀、泛微 OA、致远 OA、通达 OA、泛微 E-Office、畅捷通 T+、IBM WebSphere，攻击方法均为 Web 应用服务漏洞。建议使用上述产品的用户尽快更新产品补丁至最新版。

托管公司的 VMware ESXi 服务器遭新型 SEXi 勒索软件攻击

4 月 1 日，PowerHost 的智利分公司 IxMetro 警告客户，该公司在周六早上遭遇了勒索软件攻击，该公司的一些 VMware ESXi 服务器被加密，这些服务器用于为客户托管虚拟专用服务器。由于该公司试图从备份中恢复数以 TB 的数据，在这些服务器上托管网站或服务的客户目前处于关闭状态。而由于备份也被加密，所以这些服务器中的数据可能无法恢复。

发动此次攻击的勒索软件团伙要求每个受害者支付 2BTC，而 PowerHost 的首席执行官表示，按照遭攻击的设备估算这相当于 1.4 亿美元。

根据第三方安全研究员的说法， PowerHost 是遭到了一款新型勒索软件的攻击。该勒索软件给被加密文件添加了.SEXi 扩展名，并释放名为 SEXi.txt 的勒索信息文件。到目前为止，已知该攻击者发起的攻击只针对 VMWare ESXi 服务器，因此勒索软件选择了“SEXi”这个名字。而勒索软件本身的功能则较为常规：加密文件及备份，并通知受害者索要赎金。

虽然目前尚未找到 SEXi 勒索软件的样本，但据分析人员推断该变种可能使用了 Babuk 勒索软件泄露出的源代码，许多勒索软件团伙都使用了该源代码来创建 ESXi 加密器。此外，目前也不清楚攻击者是否会通过数据泄露网站窃取数据来勒索公司进行双重勒索攻击。

芯片制造商安世在遭勒索软件公布数据后确认数据泄露

荷兰芯片制造商 Nexperia 是中国公司闻泰科技的子公司。在 4 月 12 日的新闻声明中，该公司披露了其在 3 月份因遭到勒索攻击而迫使其关闭了 IT 系统并启动调查以确定影响范围。目前勒索软件团伙已泄露了涉嫌被盗数据的样本。Nexperia 方面表示已向荷兰警方和数据保护机构报告了这一事件，并与 FoxIT 签约以寻求调查方面的协助。

4 月 10 日，勒索网站 Dunghill Leak 宣布入侵了 Nexperia，并声称窃取了 1TB 的机密数据，同时也发布了据称是被盗文件的样本作为证据。攻击者发布了电子元件、员工护照、保密协议和各种其他样本的扫描图像，但这些样本的真实性尚未得到 Nexperia 方面的证实。

Dunghill 声称，若不支付赎金，他们计划泄露以下数据：

- **371GB 的设计和产品数据。**包括：QC、NDAs、商业秘密、技术规格、机密原理图和生产说明；
- **246GB 的工程数据。**包括：内部研究和制造技术；
- **96GB 的商业和营销数据。**包括：定价和营销分析；
- **41.5GB 的公司数据。**包括：HR、员工个人详细信息、护照、保密协议等；
- **109GB 的客户和用户数据。**包括：SpaceX、IBM、Apple 和华为等品牌；
- **121.1 GB 的各种文件和杂项数据。**包括：电子邮件存储文件。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

coronavirus@qq.com	masonhoyt@onionmail.org	luebegg8024@onionmail.org
yourdatahelp@seznam.cz	merry.lane@mailfence.com	luiscorreiasantos@onionmail.org
mds.svt.mir2@protonmail.com	Jamesy.kettlewell@protonmail.com	lukasuperr@protonmail.com
mirror-broken@tuta.io	platt.lucais@protonmail.com	marcusalorenzen@protonmail.com
mirrorbroken@cock.li	jarret.wharram@protonmail.com	maryulrich@onionmail.org
youcanchangethatall@skiff.com	hewitt_rogers@protonmail.com	mayakinggw3732@onionmail.org
Hunter-X@tuta.io	thorvald_beattie@protonmail.com	minginskilian@protonmail.com
service@cyberkiller.xyz	warden_riddoch@protonmail.com	natanschultz67@protonmail.com
teilightomemaucd@gmx.com	cowland_lothaire@protonmail.com	nicoleescobedo@onionmail.org

gyeceeidia7y@gmx.com	Nickola_men@protonmail.com	robertgunther@onionmail.org
RestorationGuarantee@gmx.com	veronabello@onionmail.org	schofield_niko@protonmail.com
callan@airmail.cc	giuliacabello@onionmail.org	scotthamiton@protonmail.com
backupmail@cock.li	avitacabrera@protonmail.com	shamnaska@protonmail.com
datahelper@onionmail.org	domenikuvoker@protonmail.com	sharonsimmons@onionmail.org
versacee@tuta.io	mespinoza980@protonmail.com	verastroving@protonmail.com
nevorah775@dacgu.com	ellershaw.kiley@protonmail.com	waltercollins77@onionmail.org
ijtg5gr@keemail.me	jonivaeng@protonmail.com	willi999ejohnsonhh@onionmail.org
ag55htr@keemail.me	alanson_street8@protonmail.com	gareth.mckie31@protonmail.com
socks777@airmail.cc	raingemaximo@protonmail.com	admin@admin.com
datacanbeback@skiff.com	mcpherson.artair@protonmail.com	lmoen@goyette.info
charity_ussr_01@proton.me	lambchristoffer@protonmail.com	vonrueden.antonietta@gmail.com
charity_ussr_02@proton.me	gareth.mckie3l@protonmail.com	leanne.roob@hotmail.com
charity_ussr_03@proton.me	rohrbacherlucho@protonmail.com	wilderman.belle@gibson.com
gmritmirivo@tutanota.com	aireyeric@protonmail.com	lesch.stephany@abshire.org
vrestlmabilo@outlook.com	noblecocking@protonmail.com	plockman@medhurst.com
gemysonzidov@tutanota.com	presleybarry63@protonmail.com	jerrod19@yahoo.com
robertkirvin@outlook.com	duncan_cautherey@protonmail.com	collins.ike@corwin.com
faustdata@onionmail.org	shdujdsh@protonmail.com	bosco.hipolito@wilkinson.com
faustdata@cock.li	ihdtwesfs@portonmail.com	hayden.rempel@kunde.com
kil4tx@secmail.pro	williamjohnson1963@protonmail.com	cobson@hwabag.us
removed@rexsdata.pro	casualstroons@portonmail.com	suntorydots@tutanota.com
coca2024cola@libertymail.net	izak.pollington@protonmail.com	suntorydots@outlook.com
ransom.data@gmail.com	t_trstram@protonmail.com	balloon@onionmail.org
ced_cririele93@protonmail.com	willmottlem01@protonmail.com	m@airmail.cc
irvingalfie@protonmail.com	BettyRacine@protonmail.com	skiffdecrypt@mail2tor.com
gustaf.wixon@protonmail.com	Ohsgsuywb@protonmail.com	skiffdecrypt@onionmail.com
ralfgriffin@protonmail.com	Lojdgseywu@protonmail.copm	alldatacanbeback@skiff.com
korgy.torky@protonmail.com	Johnbeamvv@protonmail.com	senatorrans@gmail.com
astion11@protonmail.com	rewhgsch@protonmail.com	Senatorrans@outlook.com
Bfgkwethnsb@protonmail.com	lhdbeysdq@protonmail.com	winhooder@keemail.me
Logan_A_Gray@protonmail.com	mario1@mailfence.com	winhooder@CyberFear.com
rafaeldari@onionmail.org	adrianiagua@protonmail.com	x-decrypt@worker.com
Abelzackary@onionmail.org	Aireyeric@protonmail.com	x-decrypt@hackermail.com
Elliotstaarss1@protonmail.com	alisonrobles@onionmail.org	boris_qq@tuta.io
TimWestbrook@onionmail.org	andrianiabel@onionmail.org	Decodemdr@outlook.com
PaulDade@onionmail.org	andrianosabarca@onionmail.org	whosdumb_stackz@proton.me
CarmenWashingtonGton@portonmail.com	deborahtrask@onionmail.org	parig47317@iliken.com
cozmo.storton@protonmail.com	galetrendall@protonmail.com	contact@pandoraxyz.xyz
karim.abson@protonmail.com	jameswoolley23@protonmail.com	balloon@onionmail.com
chettle.willem@protonmail.com	jeanettecook@onionmail.org	balloon_onion@proton.me
dalliss.prout96@protonmail.com	jeffery_hammonds@protonmail.com	DwayneLinette@protonmail.com

karkeck.arch@protonmail.com	jonathanhhall@ onionmail.org	bughunt@keemail.me
keefe.mcmeckan@protonmail.com	lauriabornhat7722@protonmail.com	bughunt@airmail.cc
keepupchell@protonmail.com	lillysellwood@onionmail.org	info-hunt.txt
gabriel8970@protonmail.com	lpyotr.barclay@protonmail.com	pa.encrypted@onionmail.org
databack77@tuta.io	somos.malas.podemos.ser.peores@protonmail.com	sari9890@onionmail.org
databack77@cock.li	blackproton@zohomail.com	phantom.encryption@onionmail.org
WangTeam@skiff.com	Hiit9890@cyberfear.com	

表格 1. 2024 年 4 月用于勒索的黑客邮箱

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）。

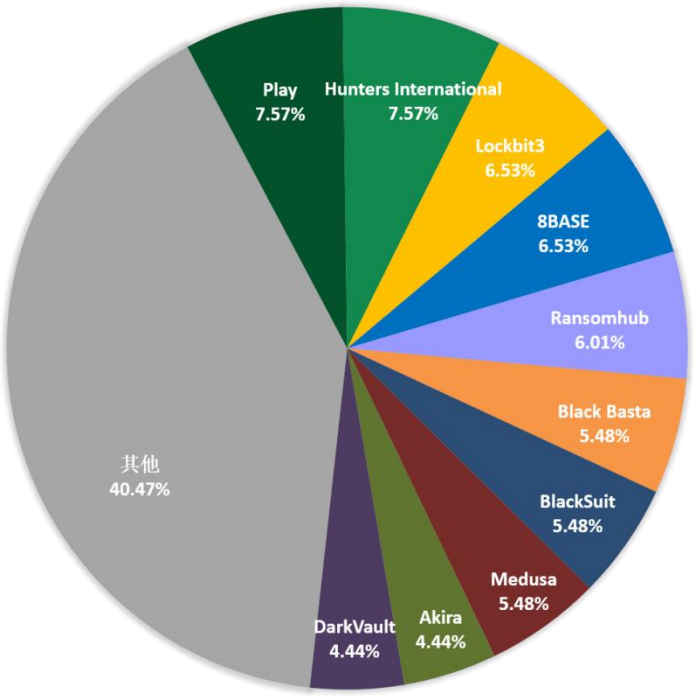

图 5. 2024 年 4 月双/多重勒索软件家族占比

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 383 个组织/企业遭遇勒索攻击，其中包含中国 1 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 9 个组织/企业未被标明，因此不在以下表格中。

Advanced Business Networks	call4health.com	Robertson Cheatham Farmers

firstmac.com.au	Hey cisco!	specialoilfield.com
GCH Hotel Group	CD Projekt!	theharriscenter.org
tudio Libeskind	Mid-South Health Systems	wencor.com
sbsofbak.com	SIS Automatisering	processsolutions.com
Mellitah Oil & Gas / Enigas Ly (Eni Electricity, Oil & Gas)	Pennsylvania Convention Center	numotion.com
ottlite.com	Engineered Automation of Maine	siemensmfg.com
bdcm.com	Alltruck Bodies	Parklane Group
ch-cannes.fr	sierraconstruction.ca	sermo.com
Drogaria Preco Bom	JE Owens	schlesingerlaw.com
Sunlux Group	Mercatino S.r.l. https://www.mercatinousato.com/	robar.com
Algen Healthcare	etateam.be	atlascontainer.com
Bitz Softwares	JE Owens and Company PA.	patersoncooke.com
The Line Up, Inc	Myers Automotive Group	arch-con.com
Thinkadam	Western Saw Inc.	Consilux (Brazil)
Medizinische Grosshandlung GmbH	sagaciousresearch.com	New Production Concept
Lumina Americas	ablinc.com	columbiapipe.com
CORTEX Chiropractic & Clinical Neuroscience	ht-hospitaltechnik.de	T A Khoury
todoagro	https://geodis.com	Kadushisoft
Mr Bean	FábricaInfo	Saint Cecilia's Church of England School
SM EMBALLAGE	doyon.com | doyondrilling.com	Swansea & South Wales
Surewerx USA	Delano Joint Union High School District	MajuHome Concept
Fifisystems	Serfilco, RP Adams, Baron Blakeslee, Pacer, Service Filtration of Canada, Polymar.	Team Locum
Fliesenstudio am Rhein	Asteco	Rigcon
Magicolor	craigwire.com	Vstblekinge Miljo
hospitalescultural.com.br	tristatetruckandequip.com	JM Heaford
melting-mind.de	Lee University	Eagle Hydraulic Components
sandipuniversity.edu.in	TrueNet Communications Corp	MULTI-FILL
Herron Todd White	drmarbys.com	Central Carolina Insurance Agency Inc.
Human Technology Inc.	rehab.ie	Panacea Healthcare Services
Yale Mortgage	D&V Electronics	Baca County Feedyard, Inc
Toolmarts	Len Dubois Trucking	Brewer & Company of WV
Precision Fluid Controls	Pioneer Oil Company, Inc.	Olea Kiosks
Anders Group	Empresa de energía del Bajo Putumayo	Hudson Supplies
Ce***.com	Lopesan Hotels	Homeocan

Original Herkimer Cheese	UPC Technology Corporation	Macuz
New Hudson Facades	Wright Brothers Construction	speditionlangen.de
polaris-SOLUCIONES TECNOLÓGICAS PARA EMPRESAS -- polaris.es	Medequip Assistive Technology	maccarinelli.it
sesenergy.org	Lotz Trucking	Skyway Coach Lines and Shuttle Services -- skywaycoach.ca
Madata	Studio LAMBDA	John R. Wood Properties
iddink.nl	hbmolding.com	Paulmann Licht
Legislative Bill Drafting Commission	City of St. Cloud, Florida	PGF Technology Group
Axip Energy Services	Grupo Cuevas	REV Drill Sales & Rentals
SSS Australia	Thermodyn Corporation	PHARMACY ETTORE FLORIO SNC - Online Pharmacy Italy
thelawrencegroup.com_privat	UnivationTechnologies	Paducah Dermatology
Rocky Mountain Sales	Autoglass	Domestic Violence Project, Inc
Erler & Kalinowski	charlesparsons	Rairdon Automotive Group
Hong Kong College of Technology	Po****sa	Integration International
Precision Time Systems	Cembell Industries	Tarrant Appraisal District
Jutebag	Heritage Cooperative	Speditionweise.de
Protected: HIDE NAME SELL DATA SOON	Druckman Law Group	Mahoney Foundry, Inc.
atriline.by	Pulaski academy	Z Development Services, LLC
Pedsurology	Chicony Electronics	Inno-soft Info Systems Pte Ltd
The Blake Law Firm	Fullington Trailways	DUNN, PITTMAN, SKINNER and CUSHMAN, PLLC
United Equitable Group	bigtoe.yoga	Change HealthCare - OPTUM Group - United HealthCare Group
Allen Blasting and Coating	regulatormarine.com	PalauGov
Semilab	The Royal Family of Great Britain	Ellsworth Cooperative Creamery
O'Connell Mahon Architects	Deacon Jones	SERVICES INFORMATIQUES POUR PROFESSIONNELS(SIP)
RSH legal	Biggs Cardosa Associates	Malaysian Industrial Development Finance
Les Miroirs St-Antoine Inc	The Post and Courier	easchangesystems
CDSHotels	Best Reward Federal Credit Union	Carrozzeria Aretusa srl
www.trifecta.com	LYON TERMINAL	HCI Systems, Inc.
Design Intoto	R.B. Woodcraft, Inc.	Madero
Beloinlaw	GPI Corporate	On Q Financial, LLC
Peter Condakes	SOA Architecture	Better Accounting Solutions
bzrastreador.com.br	ASMFC: Atlantic States Marine Fisheries Commission	TermoPlastic S.R.L
hominemclinic.com.br	The Souza Agency Inc.	truehomes.com
Central Power Systems and Services	LEMODOR	casio india
STERCH - INTERNATIONAL s.r.o.	Council for Relationships	Aussizz Group

Mainwein	jeyesfluid.co.uk	emalon.co.il
true.co.uk	compagniedephalsbourg.com	Doctorim
The Council of Fashion Designers of America	ndpaper.com	Agencia Host
Principle Cleaning Services	qint.com.br	Commerce Dental Group
Army Welfare Trust	Jack Doheny Company	Sit
EUROPEANPROF - Expertos en Seguridad y Altura -	Traverse City Area Public Schools	Guy's Floor Service
https://goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)	Omni Hotels & Resorts (US)	Everbrite
CORIENT	countryvillahealth.com	Orientrose Contracts
CYNC SOLUTIONS - The unexpected target.	disb.dc.gov	Sutton Dental Arts
Hirsh Industries	Solano County Library	Inspection Services
www.drwilliansegalin.com.br	Alliance Mercantile	Radiant Canada
xdconnects.com$50.5MNetherlands1TB 100% DISCLOSED	Novus International	Constelacion Savings and Credit Society
Octapharma Plasma	Toyota Brazil	Remitano - Cryptocurrency Exchange
Ministerio de Desarrollo Local	Kablutronik SRL	mcalvain.com
defi SOLUTIONS.	Caxton and CTP Publishers and Printers	Wacks Law Group
ghimli.com	NanoLumens	BeneCare Dental Insurance
Bank Pembangunan Daerah Banten Tbk PT	Integrated Control	Interface
rangam.com	Frederick Wildman and Sons	DataBank
draandrearechia.com.br	oraclecms.com	Beaver Run Resort
Wasserkraft Volk AG	thsp.co.uk	Olimpias Group S.R.L. (Benetton Group)
The Tech Interactive	tommyclub.co.uk	Citi Trends
jean-nouvel	Notions Marketing	Intersport
Optometric Physicians of Middle Tennessee	Jordano's Inc.	West Idaho Orthopedics
HARMAN - CYNC SOLUTIONS client	Bojangles' International	Norman Urology Associates
saglobal.com	Snchez-Betances Sifre & Muñoz-Noya	Phillip Townsend Associates
concordegroup.ca	Feldstein & Stewart	San Pasqual Band of Mission Indians
ebir.com	Agate Construction	East Baton Rouge Sheriff's Office
coastalcargogroup.com	Robeson County Sheriff's Office	Leicester City Council
Texas Retina Associates	MCP GROUP Commercial Contractor Topeka	Samhwa Paint Ind. Ltd
Speedy France	Hernando County	Tamura Corporation
United Carton Industries Company	baheyabeauty.com	Ringhoffer Verzahnungstechnik GmbH and Co. KG

Ruwac Industrial Vacuums	Gimex	Pim
Diagnostica Stago	Victor Fauconnier	Apex Business Advisory
Bombardier Recreational Products	MoldTech	Innomotive Systems Hainichen GmbH
Consorci Sanitari Integral	Theatrixx Technologies	Seven Seas Technology
D'amico & Pettinicchi, LLC	New England Wooden Ware	delhipolice.gov.in
FEB31st	The MBTW Group	regencyfurniture.com
Bieler + Lang GmbH	LS Networks	casajove.com
www.rosalvoautomoveis.com.br	Community Alliance	KICO GROUP
www.drlincoln.com.br	Henningson & Snoxell, Ltd.	Precision Pulley & Idler
Ted Brown Music	hawkremote.com	W.P.J. McCarthy and Company
mulfordconstruction.com	hirebus.com	Gaia Herbs
taylorlaw.net	ezeldsolutions.com	Sterling Plumbing Inc
NORTHEAST OHIO NEIGHBORHOOD HEALTH SERVICES (NEON)	zanebenefits.com	C&C Casa e Construção Ltda
Continuing Healthcare Solutions	taskhound.com	TUBEX Aluminium Tubes
Lutheran Social Services of Indiana	lankacom.net	Wyoming Machinery
kjf-augsburg.de	adachikan.com	Roberson & Sons Insurance Services
eurosko.com	agribazaar.com	Partridge Venture Engineering
tascoplumbing.com	wexer.com	pdq-airspares.co.uk
The law firm Dr. Fingerle Rechtsanwälte	Missouri Electric Cooperatives	anwaltskanzlei-kaufbeuren.de
fluenthome.com	Access Intelligence	aerodynamicinc.com
macphie.com	Optima Manufacturing	besttrans.com
cavotec.com	Oki Golf	Blueline Associates
hymer-alu.de	Inszone Insurance Services	Sisu Healthcare
azdel.com	Nexperia	Xenwerx Initiatives, LLC
Targus.com	Samart	

表 2. 2024 年 4 月统计受害组织/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。

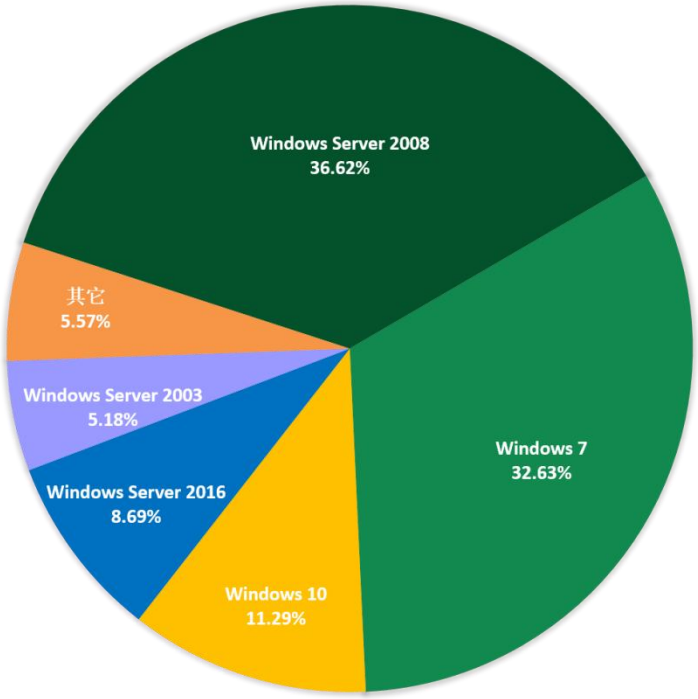

图 6. 2024 年 4 月受到入侵的各系统占比

对 2024 年 4 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。

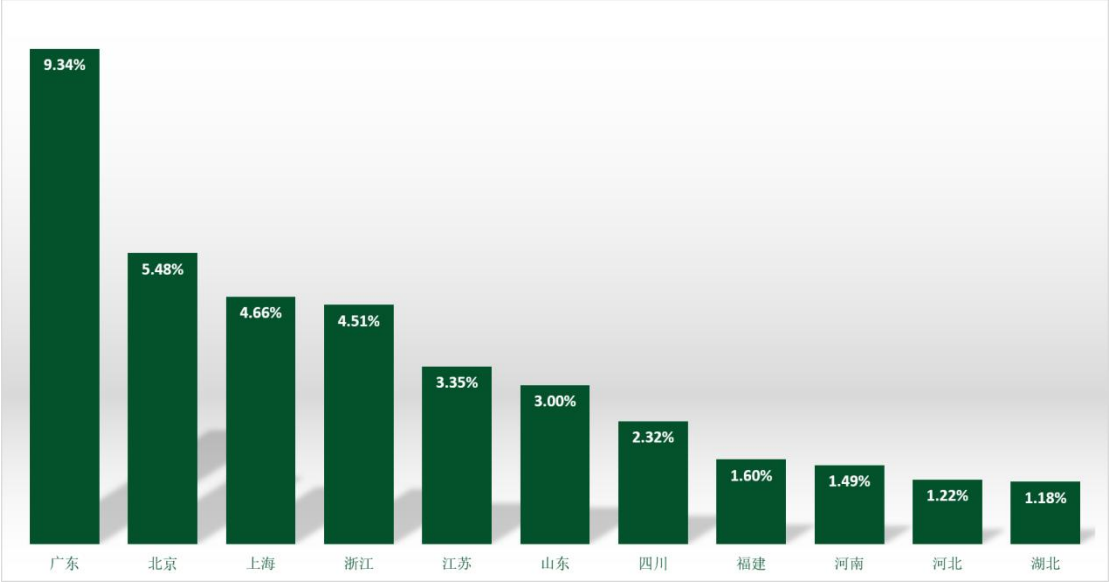

图 7. 2024 年 4 月受到入侵的地区占比

通过观察 2024 年 4 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。

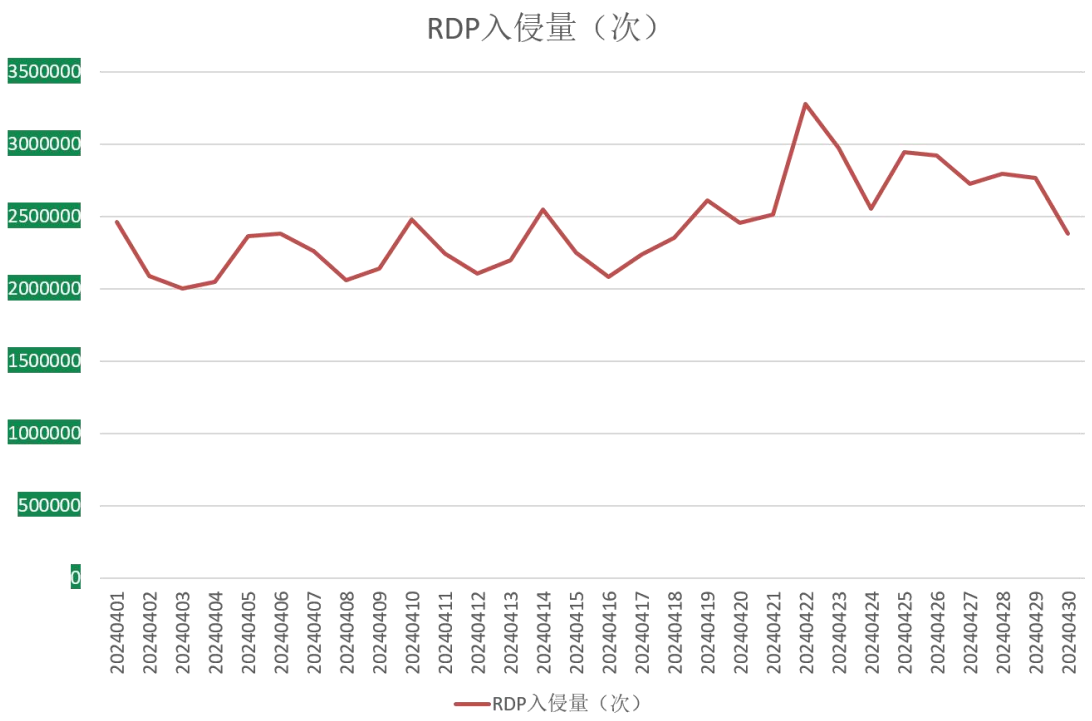

图 8. 2024 年 4 月 RDP 入侵量

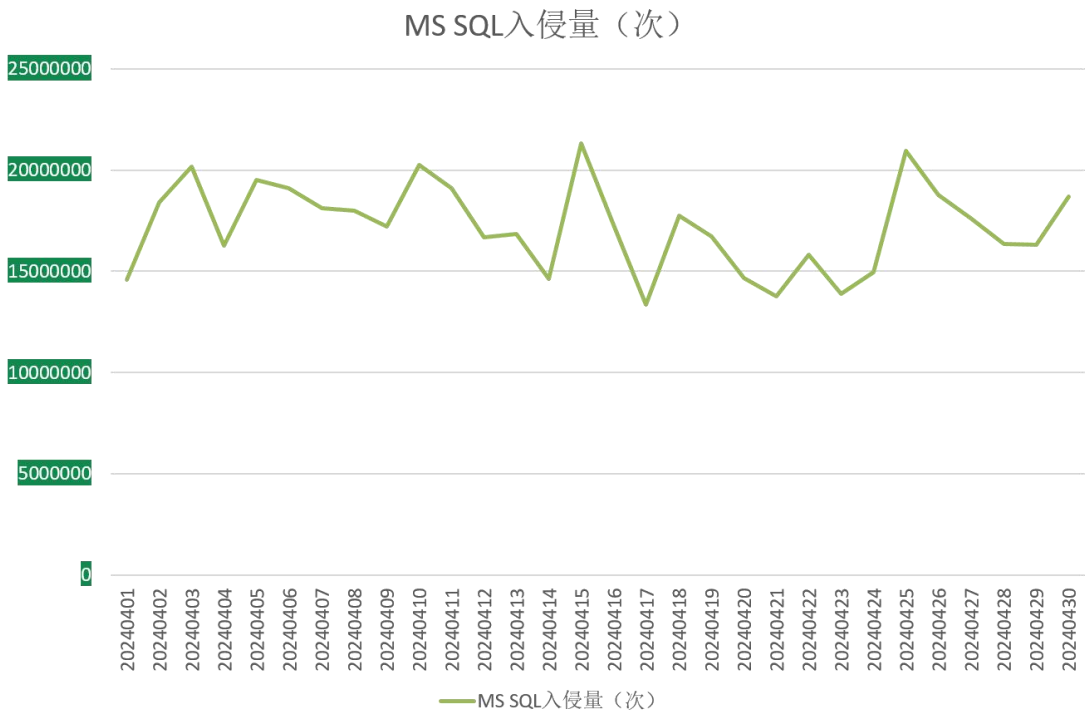

图 9. 2024 年 4 月 MS SQL 入侵量

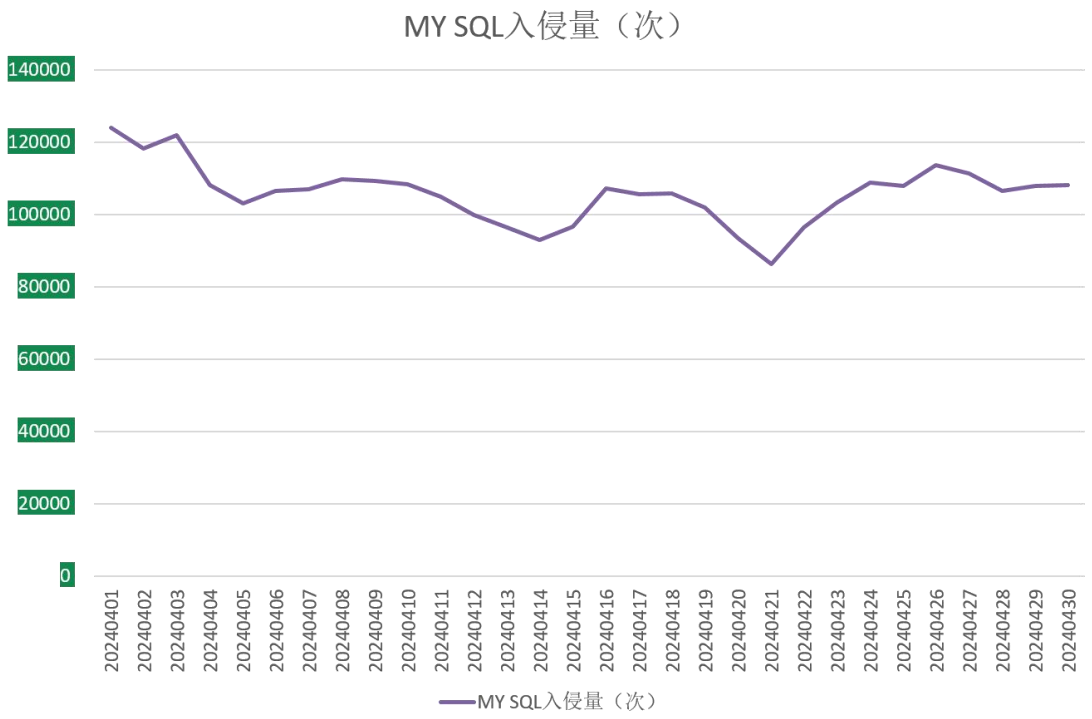

图 10. 2024 年 4 月 MYSQL 入侵量

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，本月起增加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。

- 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。

- 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。

- mkp：同 svh。

- 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。

- halo：同 360。

- mallox：同 rmallox。

- devos 同 faust。

- eblie：同 faust。

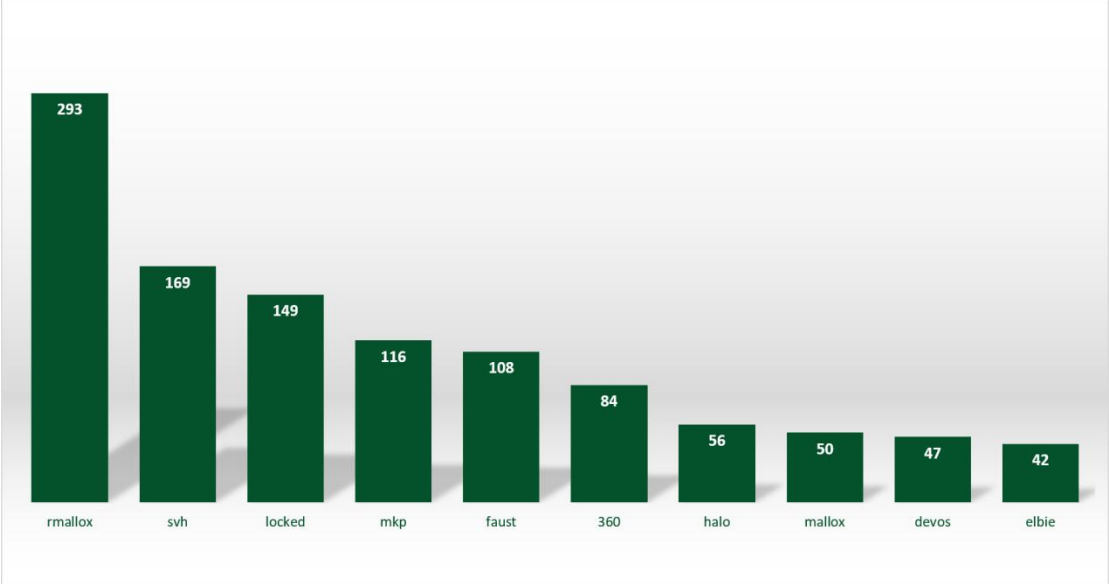

图 11. 2024 年 4 月勒索软件搜索引擎搜索量 Top10

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 Stop 家族加密的设备。

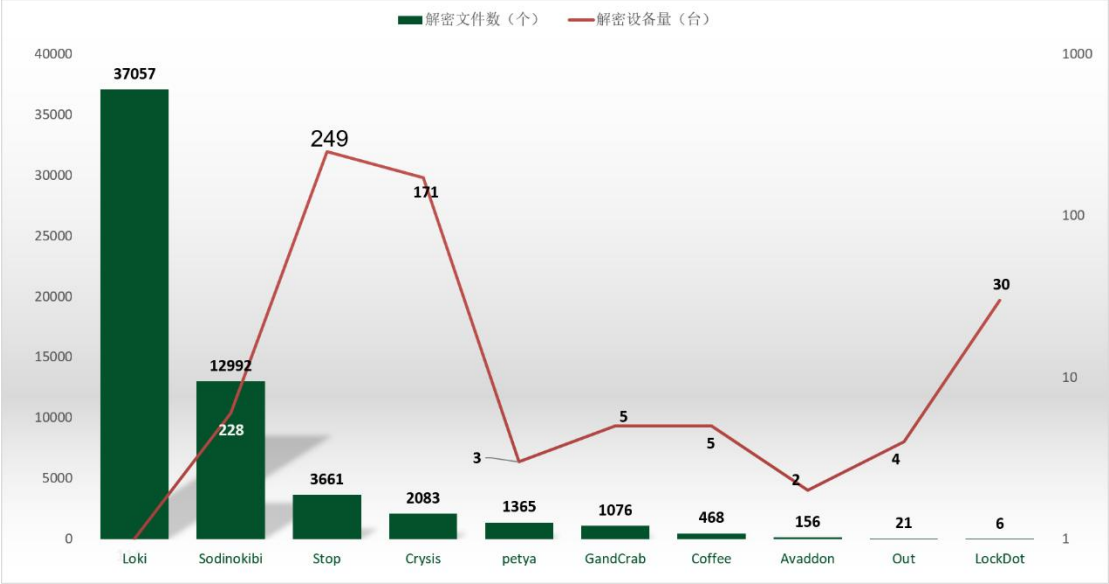

图 12. 2024 年 4 月解密大师解密量


360数字安全
数 字 安 全 的 领 导 者
360安全大脑