勒索软件流行态势分析

2024 年 2 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 2 月，全球新增的活跃勒索软件家族有 Mirror、LVTLocker、Bl00dy 等。其中，LVTLocker 家族主要攻击 Nas 平台，Bl00dy 家族则利用 ScreenConnect 身份验证绕过漏洞（CVE-2024-1709）进行攻击。此漏洞已被广泛用于网络攻击，已知使用该漏洞的勒索软件家族还有 ALPHV/Blackcat。

以下是本月值得关注的部分热点：

1. LockBit 勒索软件在被警方查封后恢复服务器并卷土重来

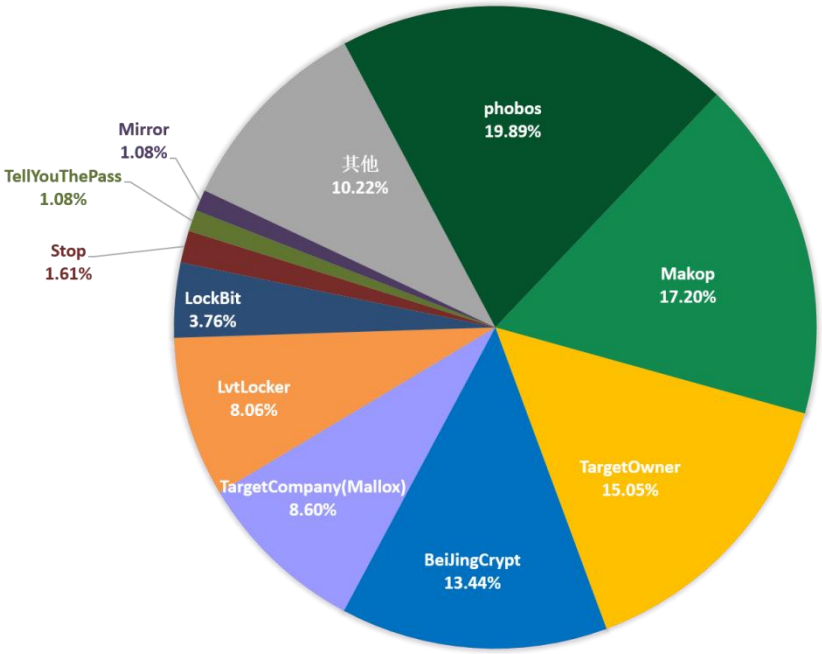
2. Rhysida 勒索软件索要 360 万美元赎买被盗的儿童数据

3. 国内知名品牌 NAS 系统遭 LvtLocker 勒索软件攻击

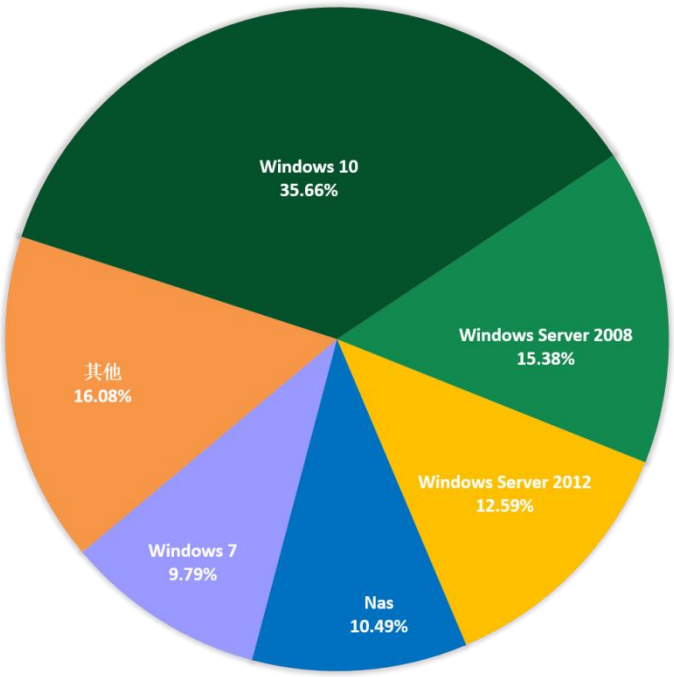
基于对 360 反勒索服务数据的分析研判，360 数字安全集团高级威胁研究分析中心（CCTGA 勒索软件防范应对工作组成员）发布本报告。

感染数据分析

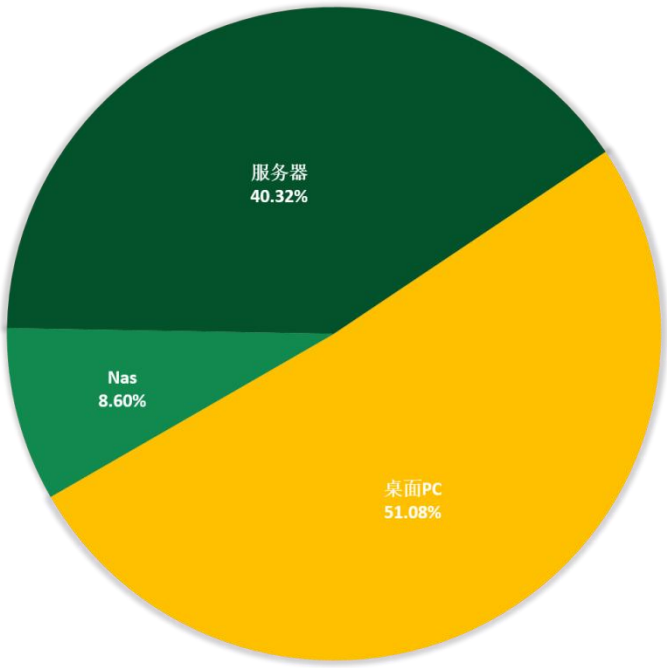
针对本月勒索软件受害者设备所中病毒家族进行统计：Phobos 家族占比 19.89%居首位，第二的是占比 17.20%的 Makop，TargetOwner 家族以 15.05%位居第三。



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。



2024 年 2 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 家族春节期间集中爆发的影响首次出现较高占比。

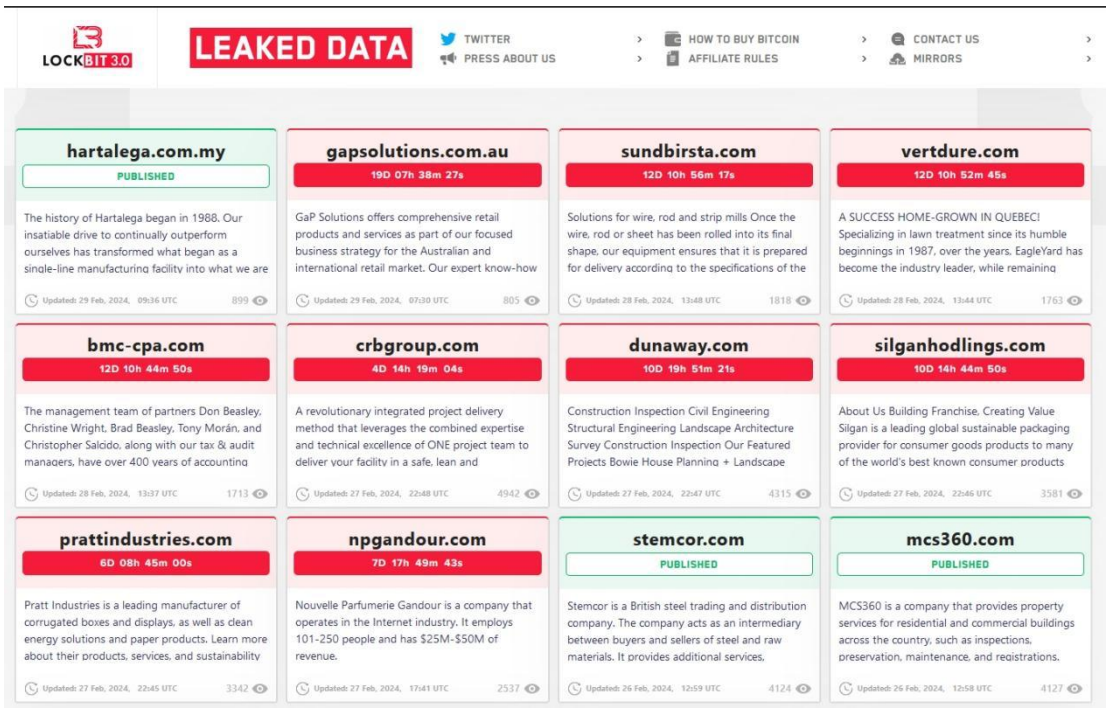


勒索软件热点事件

LockBit 勒索软件在被警方查封后恢复服务器并卷土重来

就在执法部门发动攻击拿下服务器不到一周后，LockBit 团伙便已开始在新的服务器上重新启动其在线服务，并威胁将更多的攻击集中到政府部门上。

下图便是 LockBit3.0 重新上线后的主页。

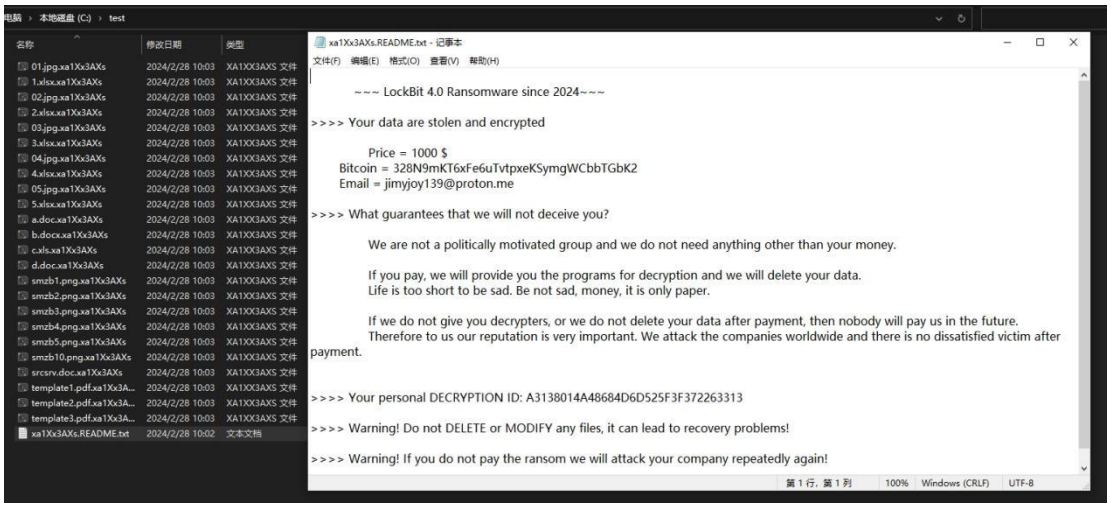


2 月 24 日，LockBit 宣布将恢复勒索软件业务并对近期遭到执法部门打击的情况做了“复盘”。LockBit 表示执法部门（他们将所有执法部门统称为 FBI）入侵了其两个主要服务器——“原因是在过去的 5 年里我沉迷于金钱而变得非常懒惰”……“由于我的个人疏忽和不负责任，我松懈了，没有及时更新 PHP”。团伙组织者表示：受害者的管理和聊天面板服务器以及博客服务器均运行在 PHP 8.1.2 环境中，而执法部门很可能是使用了 CVE-2023-3824 漏洞对其进行的攻击。据此，LockBit 表示他们已经更新了服务器所使用的 PHP 版本，并宣布将奖励任何在最新版本中发现漏洞的人。

此外，该团伙猜测此次“FBI”的入侵行动是由于其在今年一月份对富尔顿县的一次勒索攻击所致。在那次攻击中，他们掌握了“许多可能影响即将到来的美国大选的有趣事情以及唐纳德·特朗普相关的案件信息”

目前，LockBit 方面则表示执法部门所查获的数据、代码及密钥等数据仅为一小部分，并称以后会更加频繁地攻击各类政府部门以迫使“FBI”展示其是否有能力对自己展开更进一步的攻击。

360 安全大脑目前已监测到 LockBit4.0 的活动迹象。

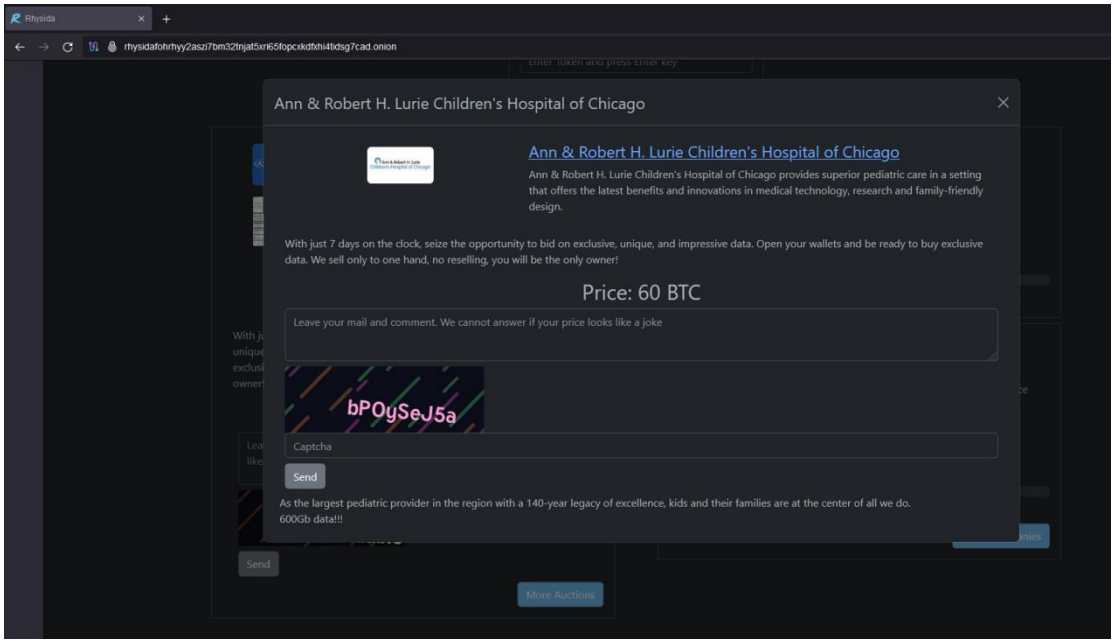


Rhysida 勒索软件索要 360 万美元赎买被盗的儿童数据

Rhysida 勒索软件团伙声称对本月初芝加哥 Lurie 儿童医院遭到的网络攻击负责。此次网络攻击迫使医疗保健提供商关闭其 IT 系统，并在某些情况下推迟医疗服务。此外，电子邮件、电话、MyChart 访问以及本地互联网都受到了影响，并且超声波和 CT 扫描结果也无法正常获取，而医生则被迫改用纸笔开具处方。

2 月 28 日，Rhysida 勒索软件团伙将 Lurie 儿童医院列入了其在暗网的勒索门户网站中，并声称从该医院窃取了 600GB 的数据。Rhysida 现在以 60 比特币（当前约合 370 万美元）的价格向单一买家出售被盗数据。此次售卖的时限为七天，超过时限后这些数据要么以较低的价格出售给多个攻击者，要么则在 Rhysida 的平台上免费公布。

而 Lurie 儿童医院方面则于 2 月 22 日更新了最新状态，表示 IT 系统的恢复工作仍在进行中，目前系统服务中断仍会影响某些部门的运营。



国内知名品牌 NAS 系统遭 LvtLocker 勒索软件攻击

春节期间，360 安全智脑监测并收到了一大波勒索攻击的集中反馈。经分析这波勒索攻击大多为一款名为 LvtLocker 的勒索软件所为，而该勒索软件的攻击目标主要是国内某知名的 NAS 设备系统。

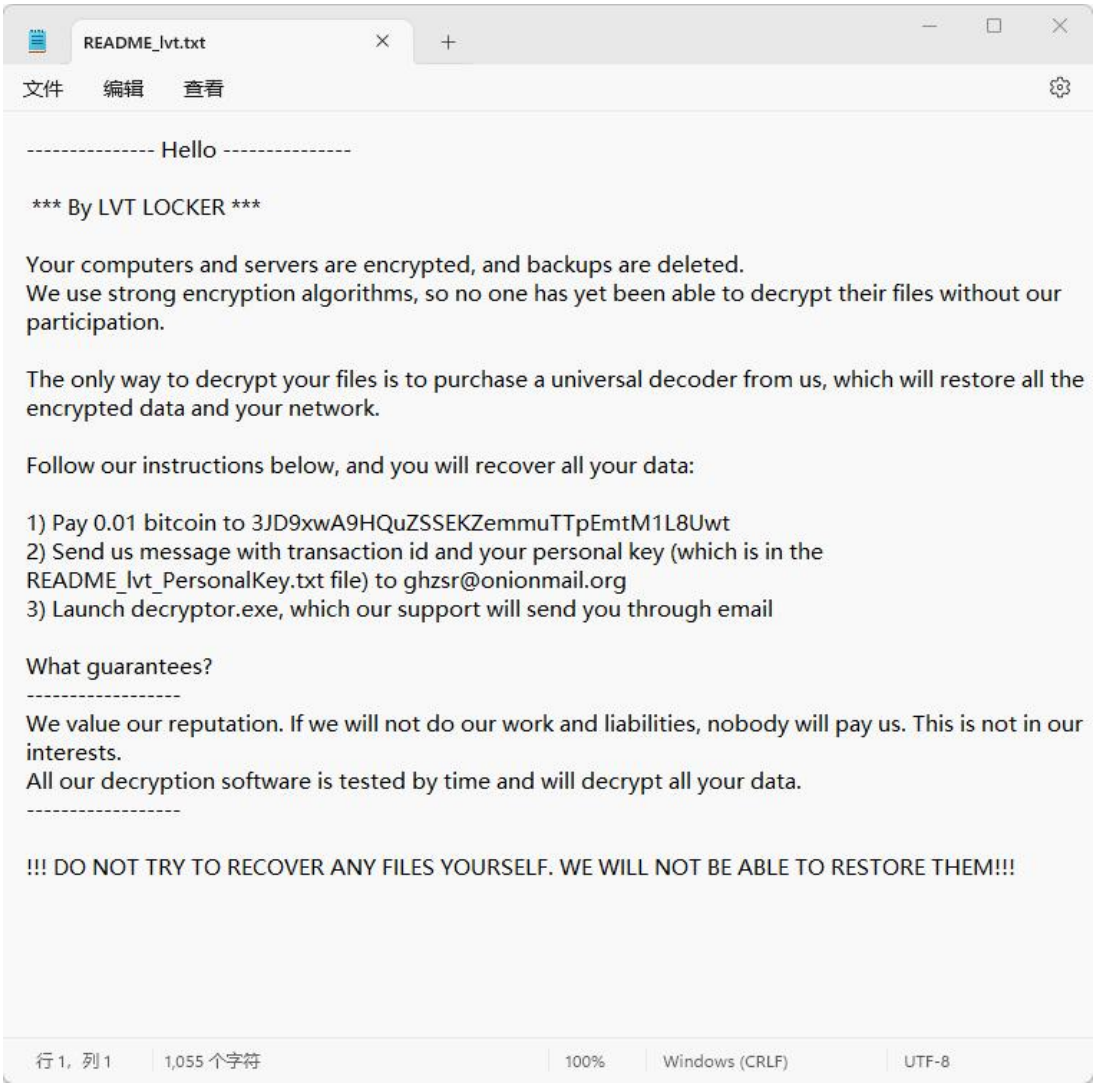
通过对 360 的大数据分析研判，发现此次勒索软件入侵事件主要是通过两种途径进入到受害用户的 NAS 设备中：

1. 利用该 NAS 设备系统中存在的一些 RCE 漏洞，比如下面一些漏洞，允许未经身份验证的用户获取 root 权限：

- CVE-2020-28188
- CVE-2022-24989
- CVE-2022-24990

2. 直接通过弱口令暴力破解，之后登录投毒。

以下为该家族勒索软件在执行完加密流程后投放的勒索信息文件：



黑客信息披露

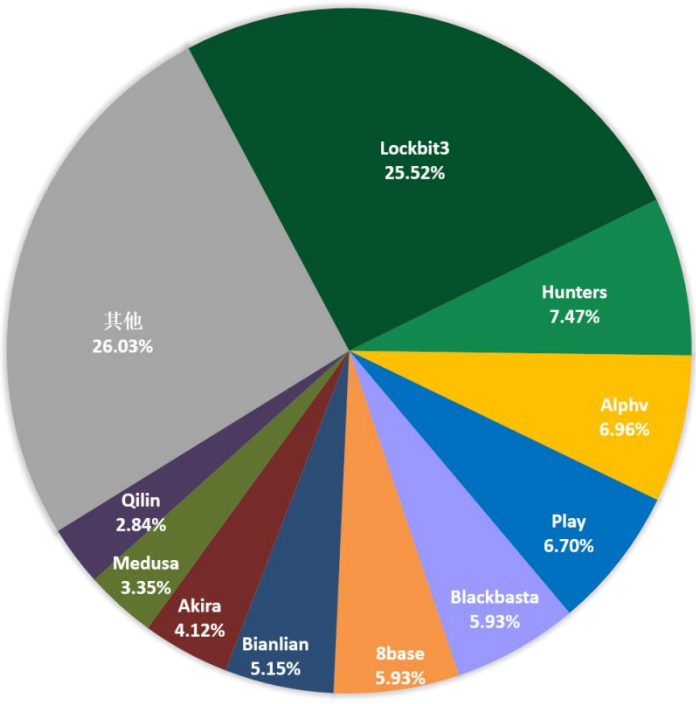
以下是本月收集到的黑客邮箱信息：

ferafont22@cock.li	Waygrafwadeta@gmx.com	Luiza.li@tutanota.com
avaveetren@tutanota.com	Helpdec@aol.com	bill.gTeam@gmx.com
fastbackdata@skiff.com	helpdec10@gmail.com	MatheusCosta0194@gmx.com
errormirror@tutanota.com	Hackjoker2002@gmail.com	blair_lockyer@aol.com
mirrorrorrim@cock.li	Cryptblack@mailfence.com	mccreight.ellery@tutanota.com
tpyrcedrorrim@tuta.io	aquaman@rambler.ua	CarlJohnson1948@gmx.com
support@freshingmail.top	mantiticvi1976@protonmail.com	megaport@tuta.io
target@msg.ws	fahydremu1981@protonmail.com	cashonlycash@gmx.com
M3ytRkZEI@gmail.com	frosculandra1975@protonmail.com	miadowson@tuta.io
zohodzin@tuta.io	trafyralhi1988@protonmail.com	chocolate_muffin@tutanota.com
zohodzin@cock.li	sanctornopul1986@protonmail.com	MichaelWayne1973@tutanota.com
bitcoin_qq@tuta.io	ringpawslanin1984@protonmail.com	claredrinkall@aol.com
phobosdata@cock.li	liebupneoplan19@protonmail.com	normanbaker1929@gmx.com
phobosdata@msgsafe.io	stivobemun1979@protonmail.com	clausmeyer070@cock.li
duckjahana@onionmail.com	guifullcharti1970@protonmail.com	nud_satanakia@keemail.me
jerryjobransom@gmail.com	phrasitliter1981@protonmail.com	colexpro@keemail.me
zzart3xx@onionmail.org	elsleepamlen1988@protonmail.com	please@countermail.com
becsec@tutanota.com	southbvilolor1973@protonmail.com	cox.barthel@aol.com
panda2024@msgsafe.io	glocadboysun1978@protonmail.com	precorpman@onionmail.org
panda2024@tutanota.com	carbedispgret1983@protonmail.com	recovery2021@inboxhub.net
Helpolenu10@gmail.com	listun@protonmail.com	everymoment@tuta.io
HELBULENU@onionmail.com	mirtum@protonmail.com	recovery2021@onionmail.org
Dec24hepl@aol.com	maxgary777@protonmail.com	expertbox@tuta.io
Dec24hepl@cyberfear.com	ranosfinger@protonmail.com	SamuelWhite1821@tutanota.com
cyberrestore2024@onionmail.org	bootsdurslecne1976@protonmail.com	fastway@tuta.io
bobgreen12@tuta.io	rinmayturly1972@protonmail.com	SaraConor@gmx.com
bobgreen12@cock.li	niggchiphoter1974@protonmail.com	fquatela@techie.com
swift_1@tutamail.com	lebssickronne1982@protonmail.com	secdatltd@gmx.com
swift@onionmail.com	daybayriki1970@protonmail.com	fredmoneco@tutanota.com
recovery8files@onionmail.org	elanor35runte35@myrambler.ru	skymix@tuta.io
delacruz007@zohomail.eu	bl00dyadmin@dnmx.org	getdata@gmx.com
reserve.cruz@onionmail.com	filedecryptionsupport@msgsafe.io	sory@countermail.com
vinsulan@tutanota.com	jimyjoy139@proton.me	greenbookBTC@gmx.com
vinsulan@cock.li	freaqzer@proton.me	spacegroup@tuta.io
msmuae@yandex.ru	deblackbithelp@gmail.com	greenbookBTC@protonmail.com
cryptblack@mailfence.com	AlbetPattisson1981@protonmail.com	stafordpalin@protonmail.com
decrypthelp0@gmail.com	henryk@onionmail.org	helperfiles@gmx.com
backmydata@inbox.ru	atomicday@tuta.io	starcomp@keemail.me

helper@mailum.com	info@fobos.one	helpermail@onionmail.org
draggonblack@yahoo.com	axdus@tuta.io	xdone@tutamail.com
byaki_buki@aol.com	it.issues.solving@outlook.com	helpfiles@onionmail.org
protonhelper2023@proton.me	barenuckles@tutanota.com	xgen@tuta.io
malignant@tuta.io	JohnWilliams1887@gmx.com	helpfiles102030@inboxhub.net
server.ransomext@tutanota.de	Bernard.bunyan@aol.com	xspacegroup@protonmail.com
orderok@tuta.com	jonson_eight@gmx.us	helpforyou@gmx.com
equalitytrust@disroot.org	bill.g@gmx.com	zgen@tuta.io
hudsonL@cock.li	joshuabernandead@gmx.com	helpforyou@onionmail.org
tH3_CyberXY@proton.me	bill.g@msgsafe.io	zodiacx@tuta.io
intelrestore2022@onionmail.org	LettoIntago@onionmail.com	bill.g@onionmail.org
acekui@tuta.io		

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）。



以下是本月被双重勒索软件家族攻击的企业或个人。未发现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 391 个组织/企业遭遇勒索攻击，其中有 14 个组织/企业未被标明，因此不在以下表格中。

Allan Berger & Associates	manchesterfertility.com	AbelSantosyAsociados
Artissimo Designs	Borah Goldstein Altschuler Nahins & Goidel	Tandem
scullionlaw.com	bandcllp.com	Southwark Council
alanritchey.com	Gilmore & Associates	stemcor.com
HSPG & Associates	Faison	dms-imaging
Dinamic Oil	Array Networks	hvd.host
easternshipbuilding.com	fcw.ch	Erwat
Bangladesh Police	Benthanh Group	goodinabernathy.com
DTN Management Company	gapsolutions.com.au	haas4.com
sundbirsta.com	HAL Allergy	sunharbormanor.com
Orange Public School District	J A Piper Roofing	Essential Labs
Acies Srl	Hypertension Nephrology Associates, P.C.	Hotel Avenida, Hostal Espoz y Mina, Hostal Arriazu, Pension Alemana
verbraucherzentrale hessen	Medall Healthcare Pvt Ltd.	etairoshealth.com
npgandour.com	abtexelgroup.com	Change Healthcare - Optum - UnitedHealth
moore-tibbits.co.uk	Saudia MRO	vertdure.com
WEL Partners	ROYAL INSIGNIA	Frencken
metal7.com	Ireland's Department of Foreign Affairs	Bertani Trasporti Spa
Penn Cinema	EpicGames	RWF Frömelt
BAZAARVOICE.COM	Ann & Robert H. Lurie Children's Hospital of Chicago	JS International
The Professional Liability Fund	Ironrock	Electro Marteix
S+C Partners	prattindustries.com	ch-armentieres.fr
Pot O' Gold Coffee	GCA Nederland	PEDDIE.ORG
crbgroup.com	Southwest Industrial Sales	Headwater Companies LLC
magierp.com	Bjuvs kommun	Angeles Medical Centers
Spine West	silganholdings.com	Webber International University
kinematica.ch	AL SHEFA FARM	ernesthealth.com
Family Health center	nationaldentex.com	dunaway.com
gatesshields.com	Wangkanai Group	equilend.com
Pressco Technology	Roncelli Plastics	BRADSHAW-MEDICAL.COM
C and J Industries, Inc.	Welch's	GRUPOCREATIVO
PEER Consultants	remkes.nl	IJM Corporation
nfllp.com	APEX - apexspedition.de	Rapid Granulator
birchallfoodservice.co.uk	mnorch.org	Acorn
Hardeman County Community Health Center	Innovex Downhole Solutions	ANDFLA SRL
Desarrollo De Tecnologia y Sistemas	mtmrobotics.com	Quik Pawn Shop

Ltda		
Austen Consultants	climatech.com	abcor.com.au
Helical Technology	dilweg.com	usmerchants.com
taloninternational.com	KHSS (You have 3 days)	zircodata.com
River Delta Unified School District	HRTec Inc	Lancaster
Raocala	dasteam.ch	Marchassociates
se.com	Axel Johnson	doneff.com
ki.se	Robert D. Clements Jr Law Group, LLLP	lexcaribbean.com
aeromechinc.com	Finlay Screening & Crushing Systems	INFINITIUSA.COM
bucher-strauss.ch	loransrl	advancedprosolutions.com
Greater Napanee	First Professional Services	soco.be
Aftrp	Compression Leasing Services	aivi.it
Wapiti Energy	carlfischer.com	Westward 360
Prudential Financial	VSP Dental	Bimbo Bakeries
The Chas. E. Phipps	Tiete Automobile	http://antunovich.com
davidsbridal.com	Chicago Zoological Society	Voice Technologies
tormetal.cl	PSI	BS&B Safety Systems L.L.C
spaldingssd.com	LoanDepot	CP Communications
Griffin Dewatering	delia.pl	www.cogans.ie
von Hagen	BRAM Auto Group	BRONSTEIN-CARMONA.COM
Mechanical Reps	Concello de Teo	etisalat.ae
DuBose Strapping	theclosingagent.com	pacifica.co.uk
Asam	Dobrowski Stafford & Pierce	Ribe-Groupe
ASP Basilicata - ASM Matera - IRCCS CROB	Norman, Fox	LD Davis
sitrack.com	Onclusive	HR Ewell & Hy-tec
centralepaysanne.lu	SilverLining	MeerServices
calcomp.co.th	Advantage Orthopedic & Sports Medicine Clinic	Schuster Trucking Company
BM Catalysts bmcatalysts.co.uk	champion.com.co	Hawbaker Engineering
vanwingerden.com	hatsinteriors.com	coreengg.com
kabat.pl	ASA Electronics [2.7 TB]	pradiergranulats.fr
UNIFER	studiogalbusera.com	bombaygrills.com
mmiculinary.com	America Movil	Nekoosa School District
rajawali.com	KALEEDS	FALCO Electronics
ffppkg.co.uk	wsnelson.com	conseguros
globalrescue.com	Institutional Casework, Inc	fultoncountyga.gov
ROOSENS BÉTONS	adioscancer.com	ATB SA Ingénieurs-conseils SIA
doprastav.sk	motilaloswal.com	giraud
Trans-Northern Pipelines	patriziapepe.com	barberemerson.com
auruminstitute.org	ssmnlaw.com	btl.info
garonproducts.com	universalservicesms.com	leonardssyrups.com

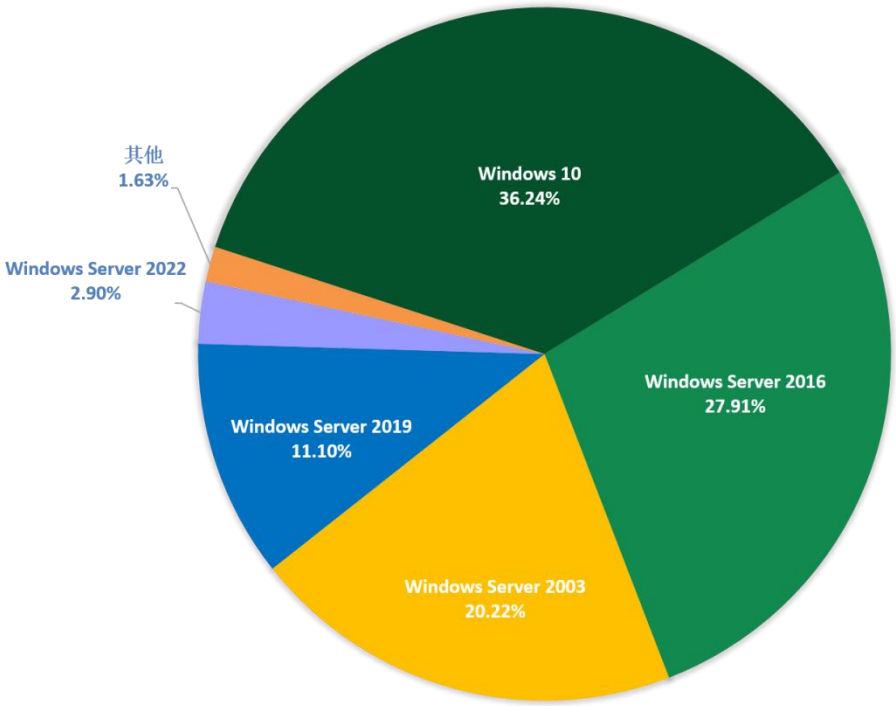
DHX–Dependable Hawaiian Express	The Source	Communication Federal Credit Union
etsolutions.com.mx	Procopio	ArcisGolf
Lower Valley Energy, Inc	Satse	New Indy Containerboard
germaintoiture.fr	tecasrl.it	Sanok Rubber CompanySpólka Akcyjna
Freedom Munitions	Forgepresion.com	Antunovich Associates
robs.org	Rush Energy Services Inc [You have 48 hours]	CNPC Peru S.A.
isspol.gov	Modern Kitchens	SERCIDE
envie.org	Disaronno International	vhprimary.com
fidcornelis.be	Arlington Perinatal Associates	Allmetal Inc.
textiles.org.tw	parkhomeassist.co.uk	jacksonvillebeach.org
camarotto.it	lyon.co.uk	grotonschools.org
Amoskeag Network Consulting Group LLC	sealco-leb.com	dienerprecisionpumps.com
YKP LTDA	plexustelerad.com	paltertonprimary.co.uk
Nastech	silverairways.com	cabc.com.ar
Impact Energy Services	Kadac Australia	Kreyenhop & Kluge
Carespring Health Care	lacolline-skincare.com	LILI'S BROWNIES
maddockhenson	Village of Skokie	Upper Merion Township
Pacific American Fish Company Inc.	Benchmark Management Group	Lancaster County Sheriff's Office
J.P. Original	Groupe Goyette	SOPEM Tunisie
Capozzi Adler, P.C.	Avianor Aircraft	Dalmahoy Hotel & Country Club
ZGEO	aisg-online.com	mranet.org
soken-ce.co.jp	water.cc	verdimed.es
willislease.com	TechNet Kronoberg AB	CTSI
seymourct.org	Drost Kivlahan McMahon & O'Connor LLC	magi-erp.com
posen.com	alfiras.com	Grace Lutheran Foundation
solveindustrial.com	maximumresearch.com	grupomoraval.com
originalfootwear.com	cdtmedicus.pl	indoramaventures.com
Western Municipal Construction	bsaarchitects.com	northseayachtsupport.nl
transaxle.com	macqueeneq.com	moneyadvicetrust.org
Worthen Industries	Ducont	parksite.com
Anderco PTE LTD	Jewish Home Lifecare	perkinsmfg.com
Karl Rieker GmbH and Co. KG	Southwest Binding & Laminating	Distecna
vimarequipment.com	PWS - The Laundry Company	TeraGo
B&B Electric Inc	CERALP	PJ Green Inc
Hbl Cpas, P.C.	Tetrosyl Group Limited	Harinck
spbglobal.com	YRW Limited - Chartered Accountants	Therme Laa Hotel and Silent Spa
Ready Mixed Concrete	Shipleys LLP	axsbolivia.com
McMillan Pazdan Smith	AVer Information	deltron.com
Perry-McCall Construction	ArpuPlus	Celeste

Douglas County Libraries	Northeastern Sheet Metal	gocco.com
themisbourne.co.uk	Mason Construction	Greenwich Leisure
davis-french-associates.co.uk	Virgin Islands Lottery	Hannon Transport
noe.wifi.at	Leaders Staffing	Albert Bartlett
semesco.com	Vail-Summit Orthopaedics & Neurosurgery (VSON)	Premier Facility Management
philogen.com	Campaign for Tobacco-Free Kids	asecos.com
portline.pt	GRTC Transit System	hutchpaving.com
cxm.com	ultraflexx.com	VCS Observation
pbwtulsa.com	prima.com	ksa-architecture.com
manitou-group.com	DOD contractors you are welcome in our chat.	tgestiona.br
Law Office of Michael H Joseph	Commonwealth Sign	logtainer.com
DIROX LTDA (Vietnã)	Digitel Venezuela	Cole, Cole, Easley & Sciba
FEPCO Zona Franca SAS	Abelsantosyasoc.com.ar	

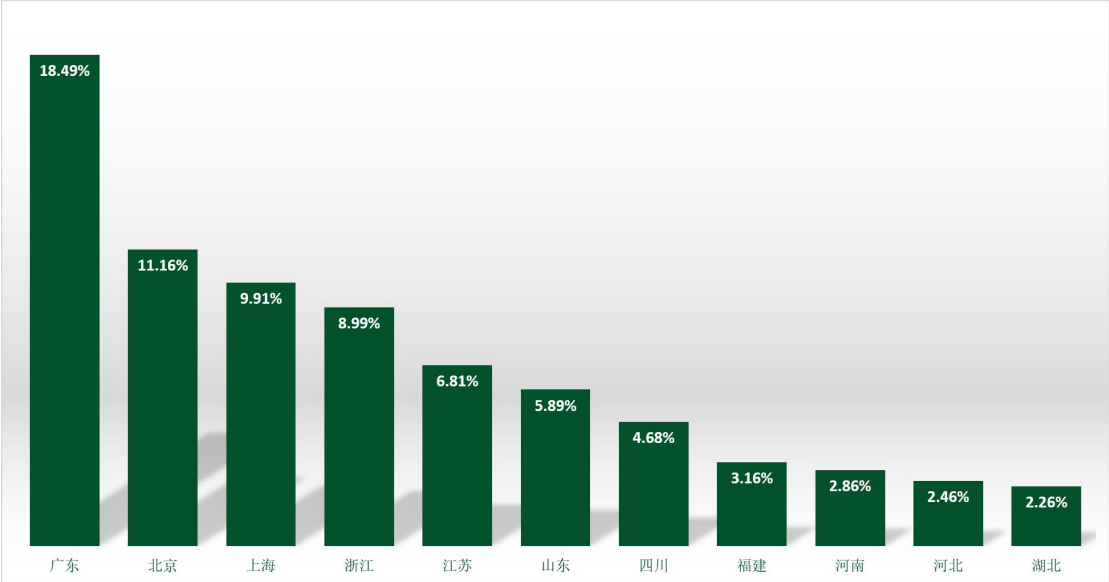
表格 2. 受害组织/企业

系统安全防护数据分析

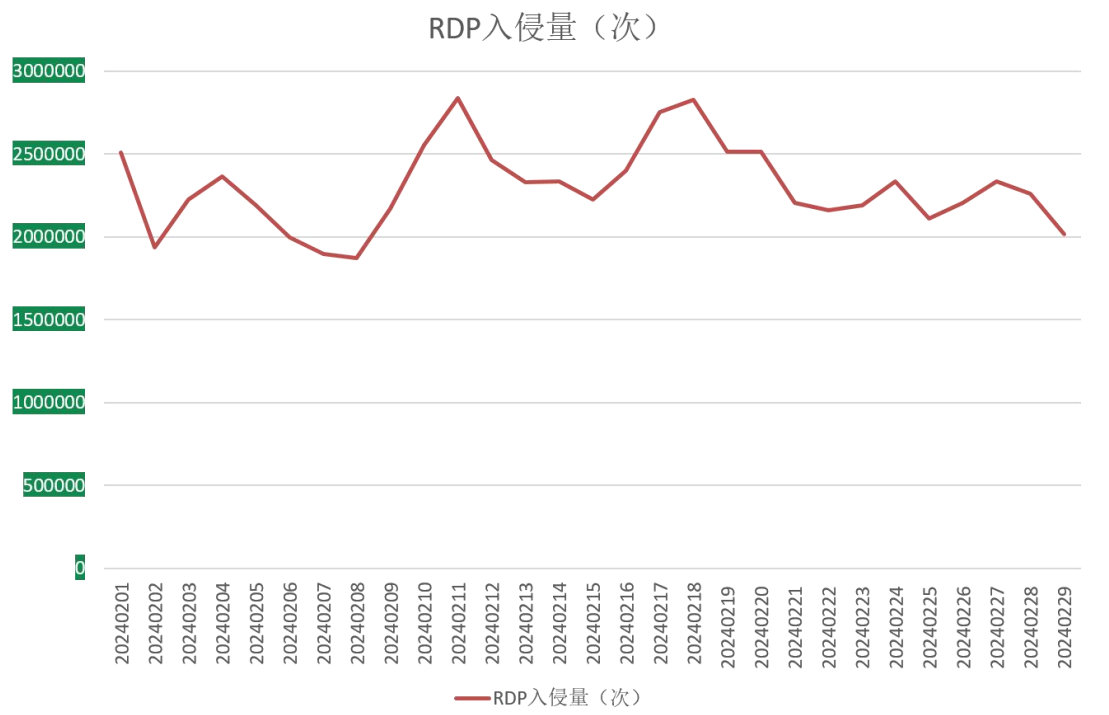
360 系统安全产品，目前已加入黑客入侵防护功能。在本月被攻击的系统版本中，排行前三的依次为 Windows 10、Windows Server 2016 以及 Windows Server 2003。

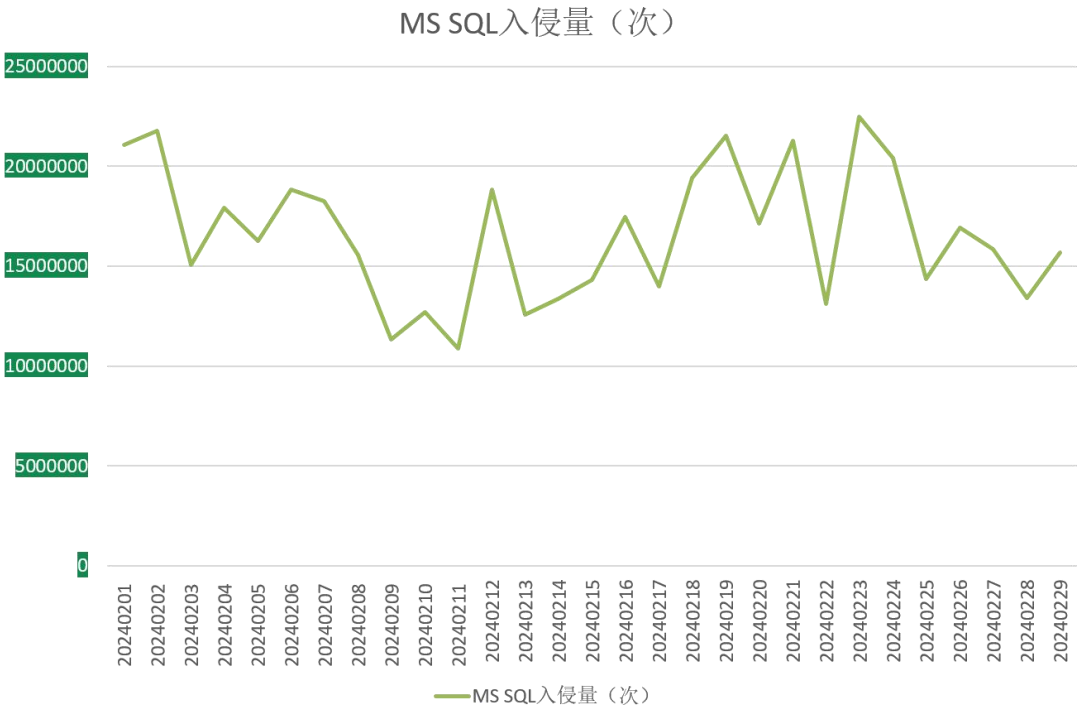


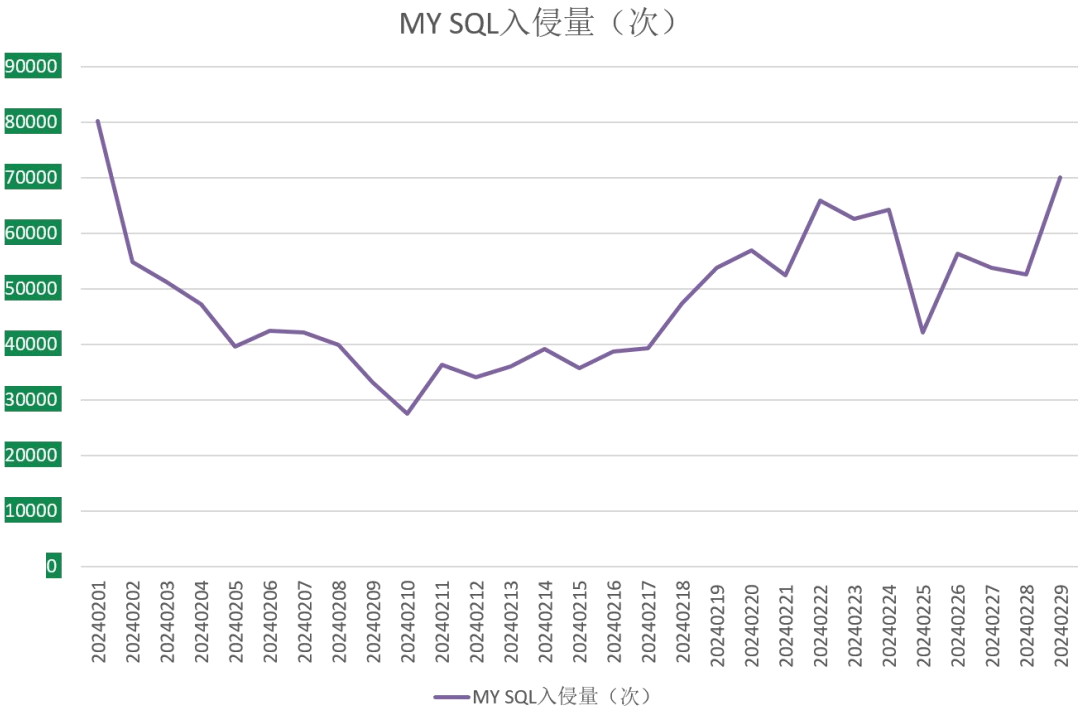
对 2024 年 2 月被攻击系统所属地域统计发现，与之前几个月采集到的数据进行对比，地区排名和占比变化均不大。数字经济发达地区仍是攻击的主要对象。



通过观察 2024 年 2 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。

- 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。

- wis：同 mkp。

- 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。

- mallox：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。

- lvt：属于 LvtLocker 勒索软件家族，由于被加密文件后缀会被修改为 lvt 而成为关键词。主要通过漏洞利用与弱口令暴破攻击 Nas 平台，在本月春节期间集中爆发。

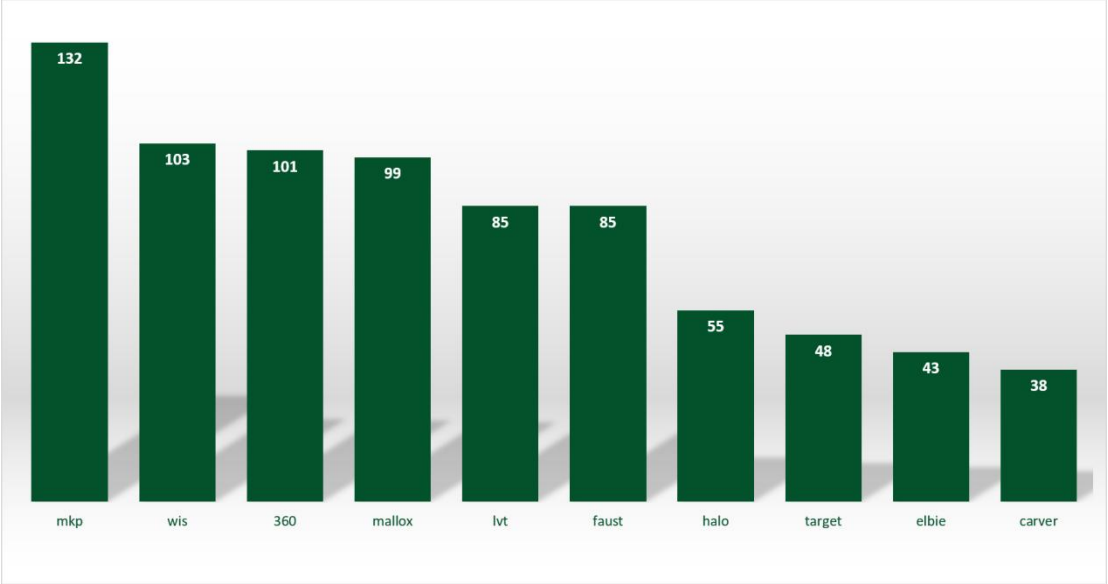
- faust： phobos 勒索软件家族，该家族的主要传播方式为：通过暴力破解远程桌面口令成功后手动投毒。

- halo：同 360。

- target：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。

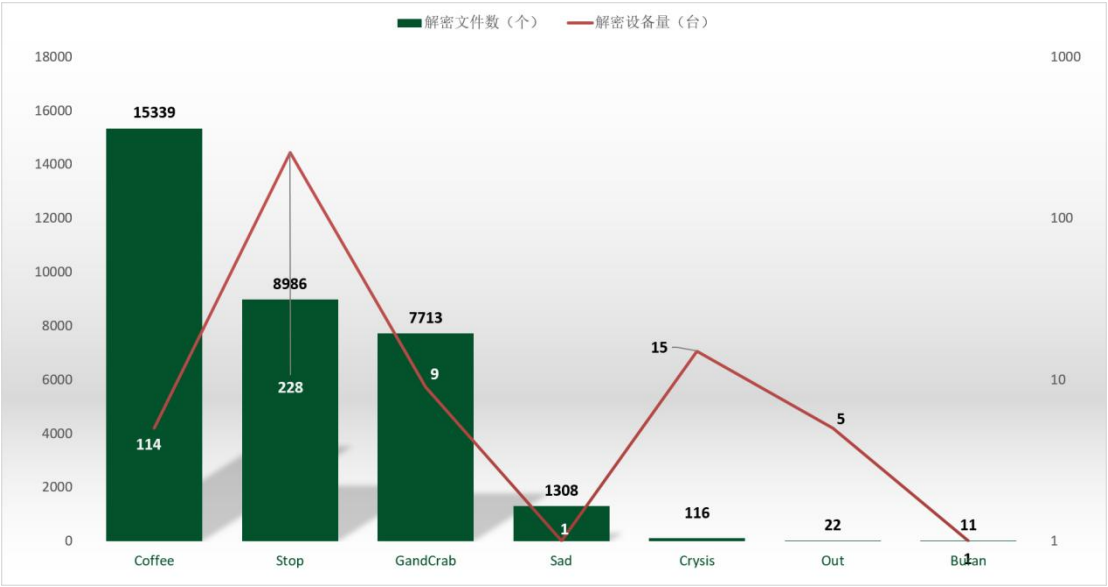
- elbie：同 faust。

- carver：同 faust。



解密大师

从解密大师本月解密数据看，解密量最大的是 Coffee，其次是 Stop。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。



另外值得一提的是，FBI 宣称放出了 LockBit3.0 的解密器。但经过我们验证，放出的所谓解密器并未集成解密功能，也就是说目前仍无法通过公开渠道获取到 LockBit3.0 的解密支持。


360数字安全
数 字 安 全 的 领 导 者
360安全大脑