勒索软件流行态势分析

2024 年 1 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次勒索软件感染求助。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 1 月，全球新增的活跃勒索软件家族有 0mega、USDLocker、TOLKONEPERDITE 等。其中 0mega 家族采用多重勒索方式运营。

以下是本月值得关注的部分热点：

1. 能源巨头施耐德电气遭 Cactus 勒索软件攻击

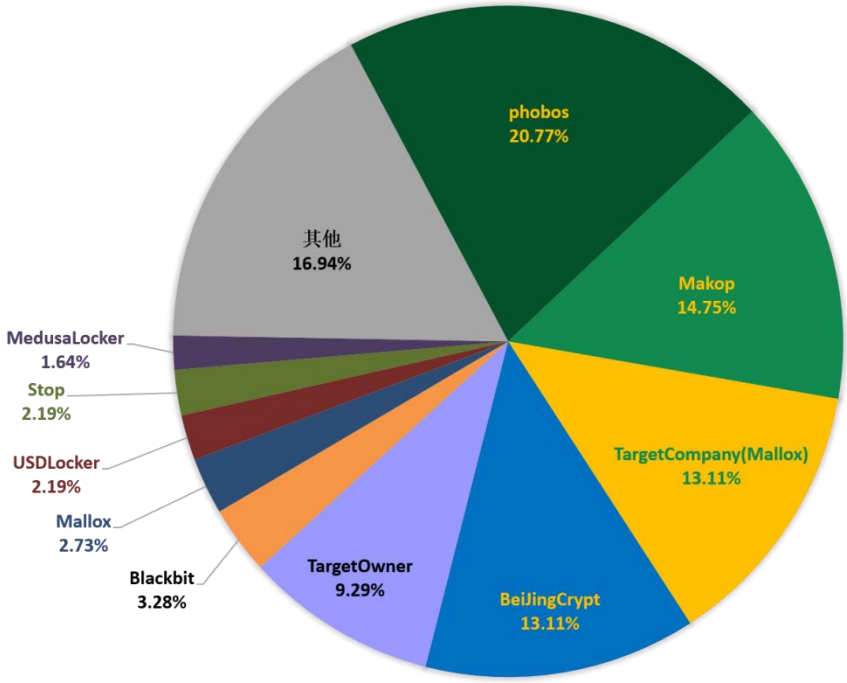
2. Tietoevry 勒索软件攻击导致瑞典企业和城市停电

3. 中国凉茶品牌加多宝遭遇 LockBit 勒索软件攻击

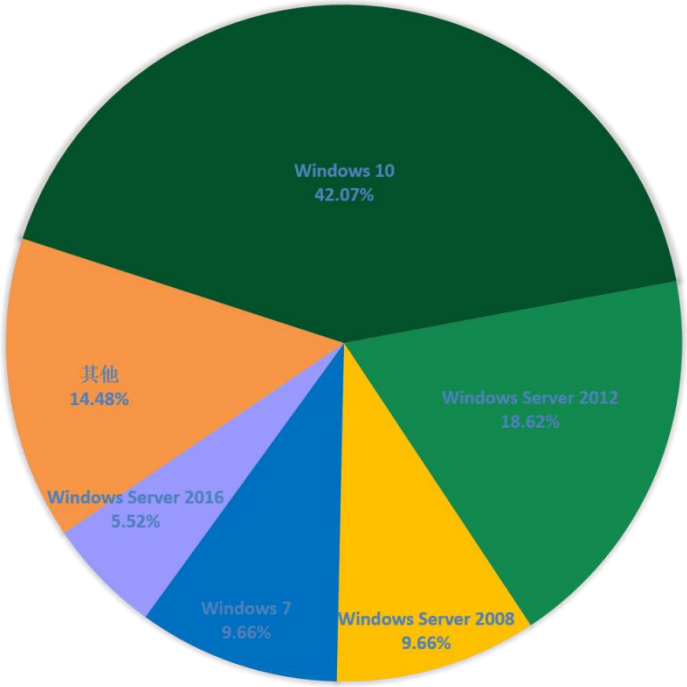
基于对 360 反勒索服务数据的分析研判，360 数字安全集团高级威胁研究分析中心（CCTGA 勒索软件防范应对工作组成员）发布本报告。

感染数据分析

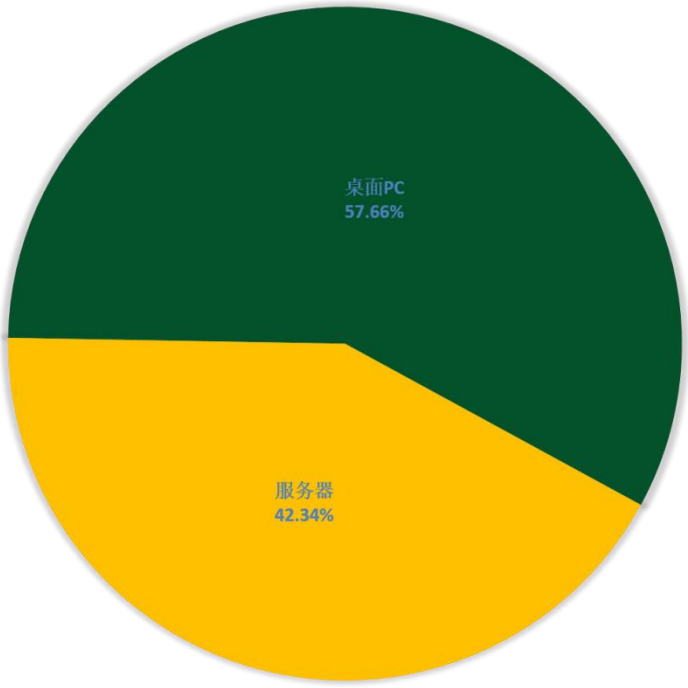
针对本月勒索软件受害者设备所中病毒家族进行统计：phobos 家族占比 20.77%居首位，第二的是占比 14.75%的 Makop，TargetCompany(Mallox)家族以 13.11%位居第三。



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 2012 以及 Windows Server 2008。



2024 年 1 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 比服务器系统略高一些。



勒索软件热点事件

能源巨头施耐德电气遭 Cactus 勒索软件攻击

据知情人士透露，法国能源业巨头施耐德电气遭到了 Cactus 勒索软件攻击，导致公司数据被盗。据悉勒索软件攻击开始于 1 月 17 日，而遭到攻击的是该公司的可持续发展业务部门。本次攻击扰乱了施耐德电气的部分资源顾问云平台，这些平台至今仍处于中断状态。

据报道，勒索软件团伙在网络攻击期间窃取了以 TB 计的公司数据，并以此威胁该公司。虽然尚不清楚被盗数据的类型，但可持续发展业务部门为企业组织提供咨询服务就可再生能源解决方案提供建议并帮助他们满足全球公司复杂的气候监管要求，所以被盗数据可能包含有关客户用电、工业控制和自动化系统以及环境和能源法规合规性的敏感信息。

目前尚不清楚施耐德电气是否会支付赎金，但该公司在声明中证实其可持续发展业务部门确实遭受了网络攻击，并且确认攻击者获取到了内部数据。不过该公司同时也表示此次攻击仅限于该部门，并未影响公司其他部门。

Tietoevry 勒索软件攻击导致瑞典企业和城市停电

芬兰 IT 服务和企业云托管提供商 Tietoevry 在 1 月 21 日证实，其在 19 日晚上到 20 日早上受到 Akira 勒索软件攻击，此次攻击影响了他们位于瑞典的一个数据中心。Tietoevry 立即隔离了受影响的平台，勒索软件攻击并未影响公司基础设施的其他部分。而该数据中心用于该公司的企业管理云托管服务，此次事件导致瑞典多个客户出现服务中断。

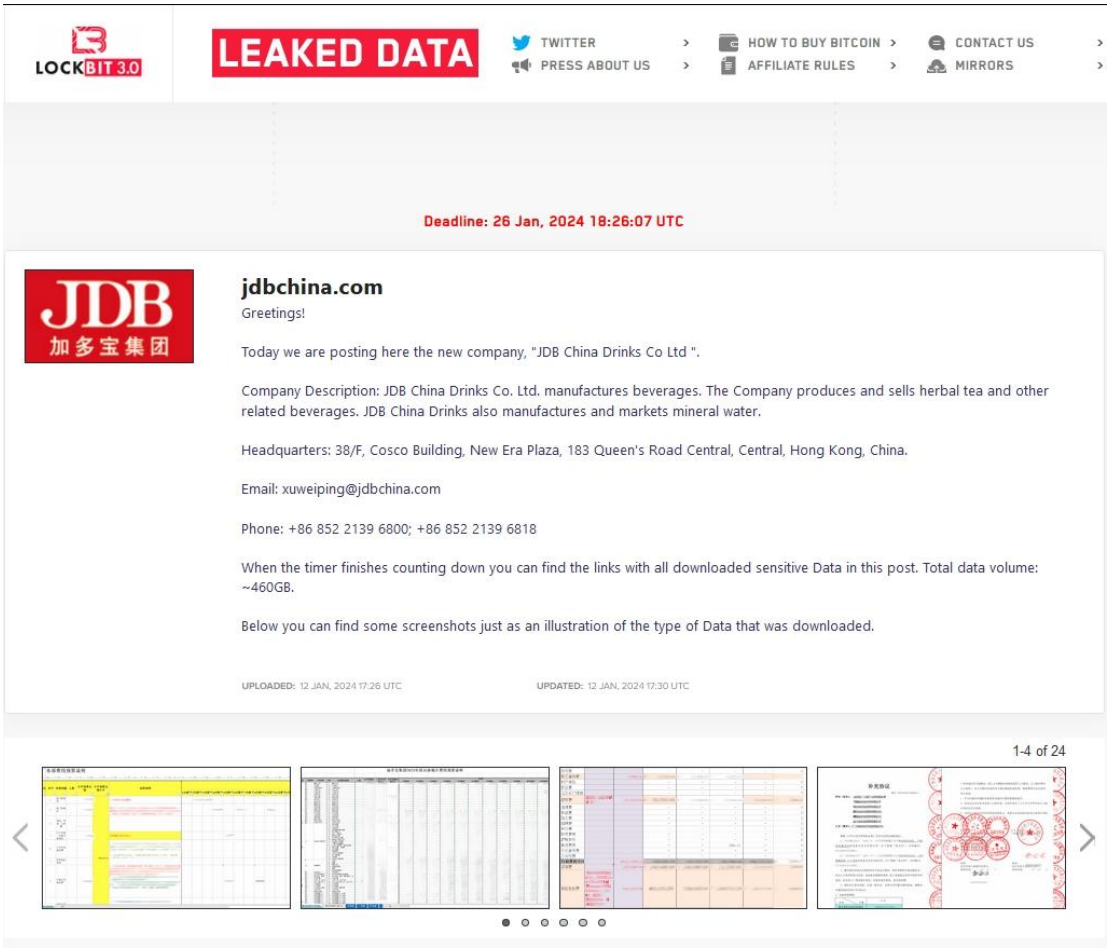
该公司表示他们正在恢复基础设施和服务，但客户在服务器恢复上线时仍然受到影响。而据报道，此次攻击对该公司的虚拟化和管理服务器进行了加密，这些服务器用于托管瑞典众多企业的网站或应用程序。瑞典最大的连锁影院 Filmstaden 已确认他们受到了此次攻击的影响，因此无法通过网站或移动应用程序在线购买电影票。此外，折扣零售连锁店 Rusta、原材料供应商 Moelven 和农业供应商 Grangnården 也受到了影响。这次中断还影响了 Tietoevry 的薪资和人力资源管理系统 Primula，该系统被瑞典政府、大学和学院广泛使用。该国受影响的大学和学院包括卡罗林斯卡学院、SLU、西大学、斯德哥尔摩大学、隆德大学和马尔默大学。

Primula 所受到的攻击还影响了瑞典的众多政府机构和市政当局，包括 Statens 服务中心、Vellinge 市和乌普萨拉县。对于乌普萨拉来说，系统的终端还影响了该地区的医疗保健记录系统。

中国凉茶品牌加多宝遭遇 LockBit 勒索软件攻击

Lockbit 勒索组织在 2024 年 1 月 12 日发布了加多宝集团的勒索信息，并于 2024 年 1 月 26 日公开了发布了他们窃取到的 460GB 数据。

从勒索组织发布的数据示例截图看，相关数据涉及各类财务信息、供应商信息、员工劳动合同等。



黑客信息披露

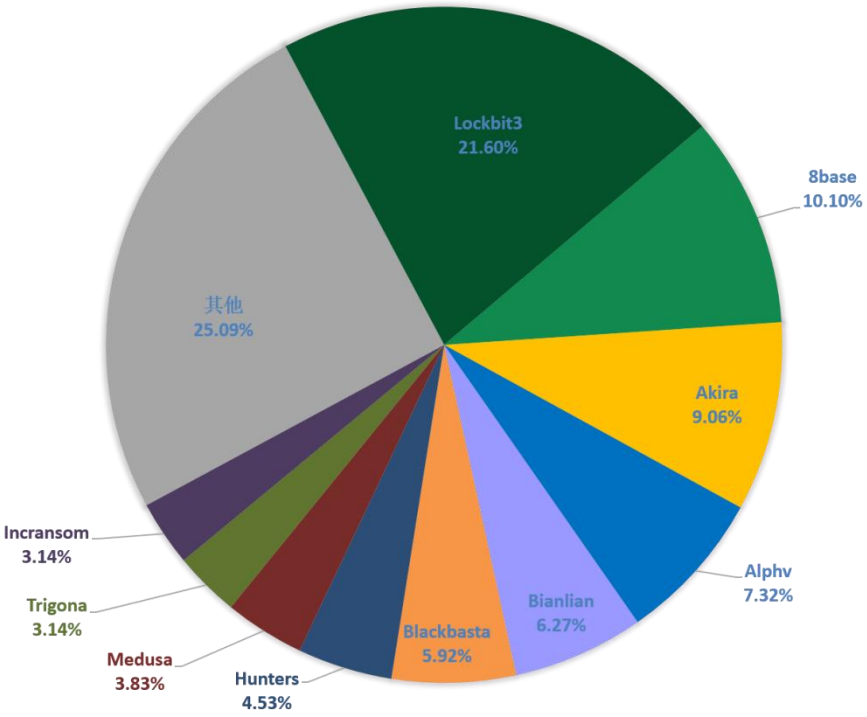
以下是本月收集到的黑客邮箱信息：

datenklause0@gmail.com	support1@puzins.com	QbXcTRSds@gmail.com
getbyback@protonmail.com	support2@tagorix.com	tolkoneperdite@onionmail.org
albabat.help@protonmail.com	new_pings@tutanota.com	data.ru@tutanota.com
blacksupport@onionmail.org	datasrv@tutanota.com	gotmydatafast@skiff.com
decryption@msgsafe.io	targetowner@tutanota.com	decdata@tutanota.com
decryptor@waifu.club	onionmail@onionmail.org	decdata@onionmail.org
max.winkler@onionmail.org	foryou1@tuta.io	medusa.serviceteam@protonmail.com
tutu@onionmail.org	aerossh@nerdmail.co	zero.cool0@onionmail.org
HowToDecryptReserve@proton.me	aerossh@cock.li	zero.cool0@msgsafe.io
cookieshelper@tutanota.com	aerossh@proton.me	ContactMesSec@protonmail.com
karsovrop@tutanota.com	covina1@skiff.com	chinahelp2023@nigge.rs
admencrypt@gmail.com	decryption@mallox.homes	datahelp2023@cyberfear.com
admdecrypt@gmail.com	thedecryptor@decoymail.com	amike1096@gmail.com
a.wyper@worldtravelnotebook.com	omegatechit@protonmail.com	onion746@onionmail.com
khanhthuan145@gmail.com	omegatechit@tuta.io	pings@mailum.com
Apriliasanjani18@gmail.com	keyseller@mailfence.com	onionransom@decoymail.com
DonCryptor@aol.com	keyseller@skiff.com	onionransom@tutanota.com
blacksup@tutanota.com	keyseller@zohomail.eu	montanarecover@cock.li
bernell@zohomail.eu	key.medusa.serviceteam@protonmail.com	montanarecover@aol.com
recoveryallfiles@onionmail.org	GavinGonzalez@protonmail.com	status.inbox1@gmail.com
recoveryallfiles@bingzone.net	angelomartin-1980@protonmail.com	status.inbox2@gmail.com
someordinarygamers@nanozebra.com	rpd@keemail.me	datarestorehelpyou@airmail.cc
dr.help780@gmail.com	rapid@aaathats3as.com	support@freshmail.top
dr.locker780@gmail.com	nicolasmarvinlor@outlook.com	Rdpstresstest@proton.me
helpbit911@cocaine.ninja	ithelpconcilium@tutanota.com	rdpstresstest@keemail.me
helpbit911@cock.li	helper2@biehes.com	datadownloader@proton.me
suppblackbit@gmail.com	helper2@aveuva.com	datadownloader@tutanota.com
suppblackbit@tutanota.com	dirhelp@keemail.me	MleK1x7uY@gmail.com
spotify.exe@proton.me	cmd@jitjat.org	kGQ6wNCwB@gmail.com
Write here belingmor@cock.li	felleskatalogen@protonmail.com	zenhao007@gmail.com
reserve admin@cuba-supp.com	offer@tuta.com	decryptprof@onionmail.org
jabber cuba_support@exploit.im	ac7d33419d00c1d9@tutanota.com	decryptfile@onionmail.org
staer@cock.li	HarpyRage@cyberfear.com	doctorhelperss@gmail.com
crazyfrog1233@tutanota.com	avanziahelp@cock.li	helpersdoctor@outlook.com
crazyfrog1233@rape.lol	avanzirest@tuta.io	ithelp02@securitymy.name

Teikobest@gmail.com	ojmFoDUoA@gmail.com	ithelp15@securitymy.name
Loxoclash@gmail.com	GDqyiQMfP@gmail.com	Cyblade@zohomail.eu
deltatechit@protonmail.com	BgQPTvPKl@gmail.com	Cyblade@skiff.com
deltatech@tuta.io	JkpmAeVAW@gmail.com	dx31@mail.com
getmydata@list.ru	ffreefix@outlook.com	dx31@usa.com
datatradetower@gmail.com	DNQZyVfiQ@gmail.com	

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。若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 286 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 1 个组织/企业未被标明，因此不在以下表格中。

Aspiration Training	North Hill	mnorch.org
apeagers.au	derrama.org.pe	Galaxy Fireworks, Inc
SportsMEDIA Technology	LeClair Group	Hydraflow
Sefin	Ausa	Genesis Motors

CMG Drainage Engineering	Daher Contracting	Elliott Wave International
VVD Elettrotecnica Srl	Basin Trucking and Oilfield Services LLC	Nbbl
Meag Va-system AB	S 茅 quano	Geographe
Diamond Technical Services, Inc.	Able One a Quadbridge Company	mrm.com.mx
sahchicago.org	clackamas.edu	MA Engineering
TECHNICA - HACKED AND MORE THEN 300 GB DATA LEAKED!	Black Butte Coal Co	Waterford Country School Inc
Benjamin Plumbing Inc	CORBETT EXTERMINATING Inc	North American University
grimme.dk	ese.com	crowe.com.za
Lomma Crane & Rigging	Castilleja School	Get Away Today
Safe Plating	Chamber of Deputies of Romania (Camera Deputa 蒽 ilor din Rom 芒 nia)	ABECOM LTDA
Dutton Brock	Cislo and Thomas LLP	mordfin
oogp.com	vidalung.ai	jaygroup.com
Kansas City Area Transportation Authority	Cislo & Thomas LLP	Image Craft
Shoma group	ehsd.org	sipicorp.com
Brazilian Business Park	elandenergy.com Eland Energy	Valley TeleCom Group
securinux.net	Draneas Huglin Dooley LLC	Lush
OrthoNY, Orthopedic Care	Four Hands LLC	CloudFire Italy
leclairgroup.com	NOVA Business Law Group	The Wiser Financial Group
ANI Networks	caravanclub.co.uk	Toronto Zoo
wannagocloud	neafidi	Brightstar Care
Hawbaker Engineering	Charles Trent	Innovative Automation
Tamdown	Thorite Group	SANDALAWOFFICES.COM
Southeast Vermont Transit (MOOver)	Integritylnc.org Integrity Inc	https://www.carri.com
https://www.gadotbio.com/ Gadot Biochemical Industries Ltd	icn-artem.com	accolade-group.com + levelwear.com +Taiwan microelectronics(CRM).
a24group.com ambition24hours.co.za	https://www.mikeferry.com	Dirig Sheet Metal
Winona Pattern & Mold	Signature Performance Insurance	MBC Law Professional Corporation
Groupe Sweetco	Bikesportz Imports	La Ligue
Midwest Service Center	Sunfab Hydraulics AB	Glimstedt
synergyfinancialgrp.com	micrometals.com	lyonshipyard.com
sierrafrontgroup.com	Cryopak	fairmontfcu.com
ktbslaw.com	dupont-restauration.fr	kivibros.com
haes.ca	cinfab.com	prudentpublishing.com
unitedindustries.co.nz	stemcor.com	Wilhoit Properties
Milestone Environmental Contracting	Total Air Solutions	R.C. Moore Trucking
envea.global	Herrs (You have 72 hours)	Smith Capital - Press Release
ARPEGE	C and F Packing Company Inc.	Double Eagle Development
Waldner's	HOE Pharmaceuticals Sdn Bhd	davidsbridal.com
agc.com	southernwater.co.uk	Pozzi Italy

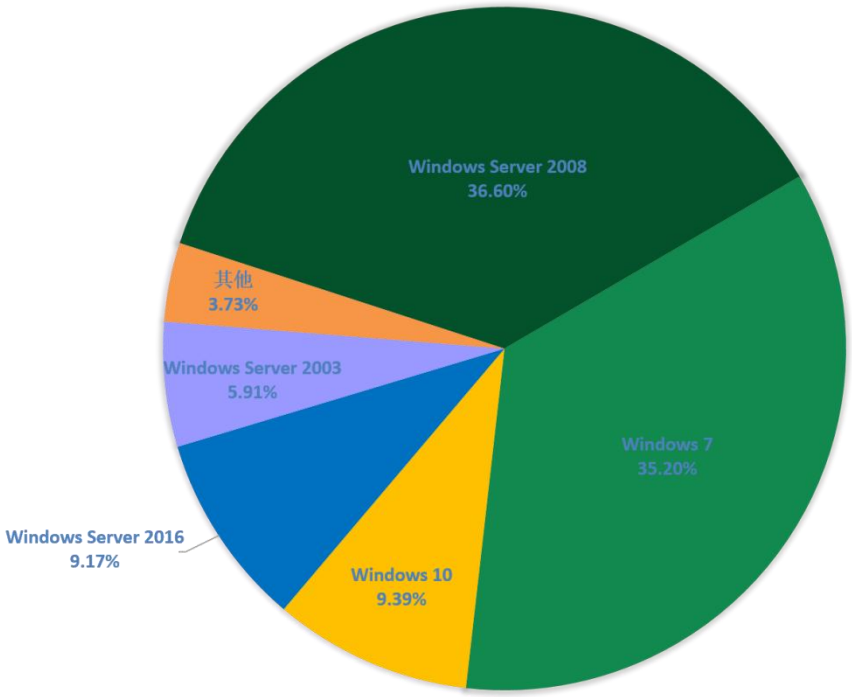
The Gainsborough Bath	Richmond Fellowship Scotland	ANS COMPUTER [72hrs]
deknudtframes.be	synnex-grp.com	gattoplaters.com
duconind.com	wittmann.at	qtc-energy.com
hughessupplyco.com	umi-tiles.com	cmmt.com.tw
shenandoahtx.us	cct.or.th	stjohnrochester.org
jasman.com.mx	North Star Tax And Accounting	KC Pharmaceuticals
Martinaire Aviation	bmc-cpa.com	subway.com
tvjahnrheine.de	home-waremmien.be	marxan.es
wendy.mx	swiftair.com	Worthen Industries [You have three days]
Sykes Consulting, Inc.	Busse & Busee, PC Attorneys at Law	Anna Jaques Hospital
pratt.edu	seiu1000.org	dywidag.com
TPG Architecture	jdbchina.com	Hamilton-Madison House
Hydratek	evit.edu	Alupar Investimento SA
PROJECTSW	foxsemicon.com	Malongo France
Groveport Madison Schools	Samuel Sekuritas Indonesia & Samuel Aset Manajemen	Premier Facility Management
Fertility North	Vision Plast	uffs.edu.br
GROWTH by NCRC	LT Business Dynamics	digipwr.com
jaffeandasher.com	Gallup McKinley County Schools	aercap.com
Stone, Avant & Daniels	JspPharma	DENHAM the Jeanmaker
Axfast AB	Syndicat G茅n茅ral des Vignerons de la Champagne	Washtech
SIVAM Coatings S.p.A.	Nexus Telecom Switzerland AG	nobleweb.com
selmi.com.br	onyx-fire.com	millgate.co.uk
Becker Logistics	Bestway Sales	TGS Transportation
Premium Guard	F J O'Hara & Sons	Donear Industries
Beit Handesai	shinwajpn.co.jp	maisonsdelavenir.com
vasudhapharma.com	hosted-it.co.uk	Ausa
Northeast Spine and Sports Medicine's	Hartl European Transport Company	American International College
Republic Shipping Consolidators, Inc	www.kai.id "FF"	amenitek.com
turascandinavia.com	Lee Spring	Charm Sciences
Malabar Gold & Diamonds	Banco Promerica	arrowinternational.com
thecsi.com	pharrusa.com	Builcore
hotelcontinental.no	olea.com	asburyauto.com
Washington School For The Deaf	Former S.p.A.	International Trade Brokers and Forwarders
BALLAY MENUISERIES	Anderson King Energy Consultants, LLC	Sems and Specials Incorporated
acutis.com	dtsolutions.net	intercityinvestments.com
hi-cone.com	Alliedwoundcare	Primeimaging
Blackburn College	Vincentz Network	Limburg

Water For People	pactchangeslives.com	Triella
Ursel Phillips Fellows Hopkinson	SHIBLEY RIGHTON	automotionshade.com
R Robertson Insurance Brokers	molnar&partner	hartalega.com.my
twt.co.za	tiautoinvestments.co.za	Group Bogart
agnesb.eu	Delco Automation	Viridi
Ito Pallpack Gruppen	Corinth Coca-Cola Bottling Works	Precision Tune Auto Care
HALLEONARD	Van Buren Public Schools	Heller Industries
CellNetix Pathology & Laboratories, LLC	morganpilate.com	mciwv.com
capitalhealth.org	Agro Baggio LTDA	Maas911.com
GRUPO SCA	Televerde	Geologics
The Lutheran World Federation	Proax Technologies LTD	Somerset Logistics
ips-securex.com	Project M.O.R.E.	Thermosash Commercial Ltd
Gunning & LaFazia, Inc.	Diablo Valley Oncology and Hematology Medical Group - Press Release	Kershaw County School District
Bradford Health	Madison Capital & WPM & The Time Group	groupe-idea.com
SAED International	graebener-group.com	leonardsexpress.com
nals.com	MPM Medical Supply	DELPHINUS.COM

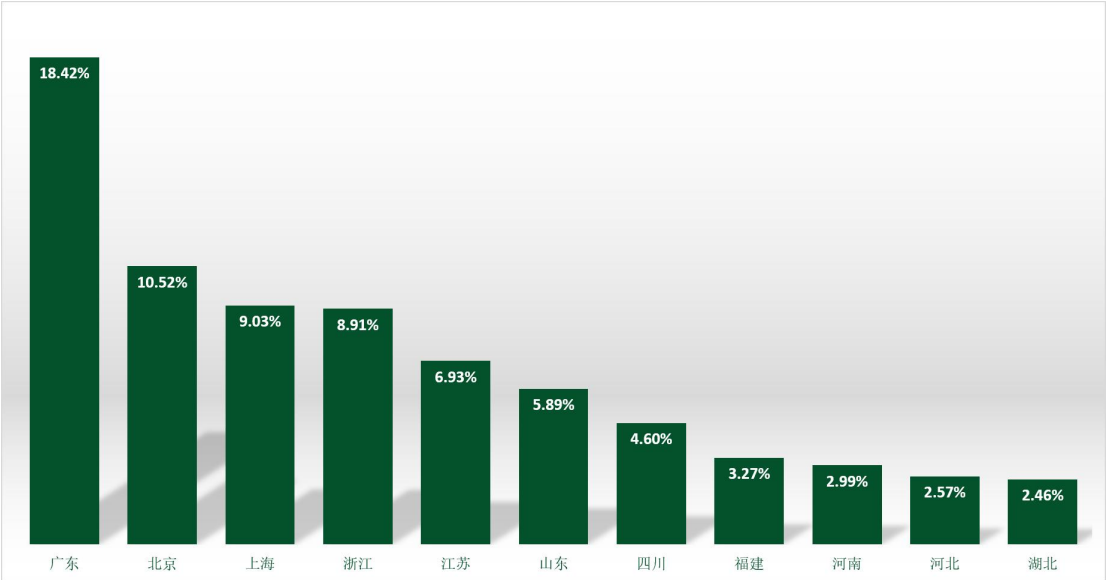
表格 2. 受害组织/企业

系统安全防护数据分析

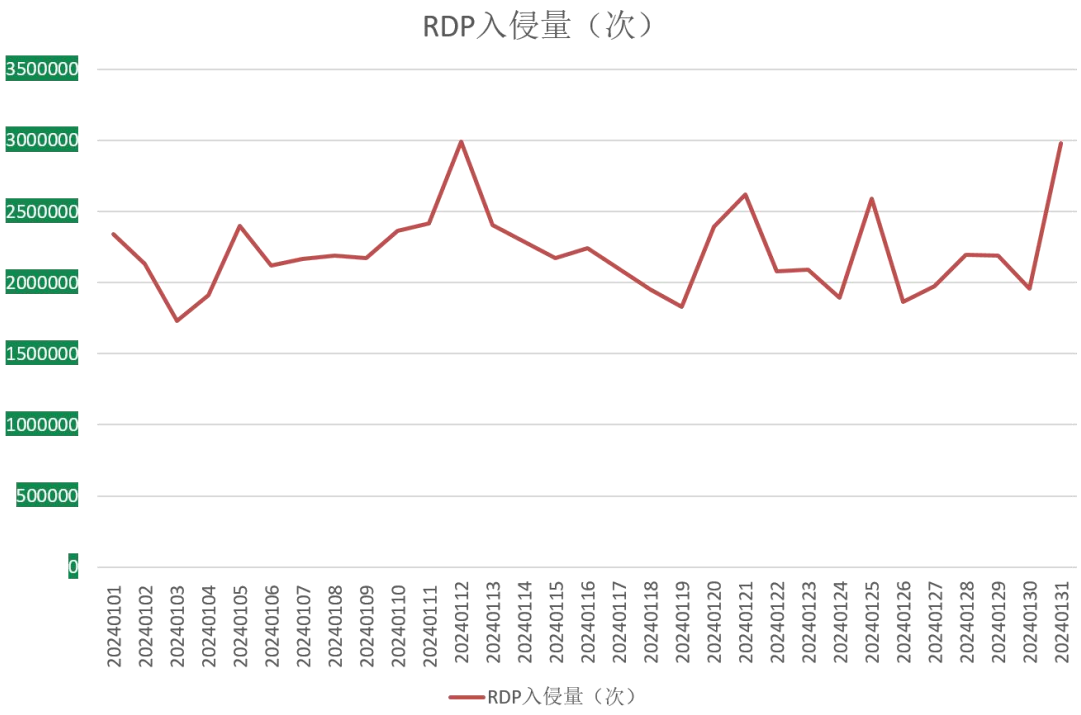
360 系统安全产品，目前已加入黑客入侵防护功能。在本月被攻击的系统版本中，排行前三的依次为 Windows Server 2008、Windows 7 以及 Windows 10。

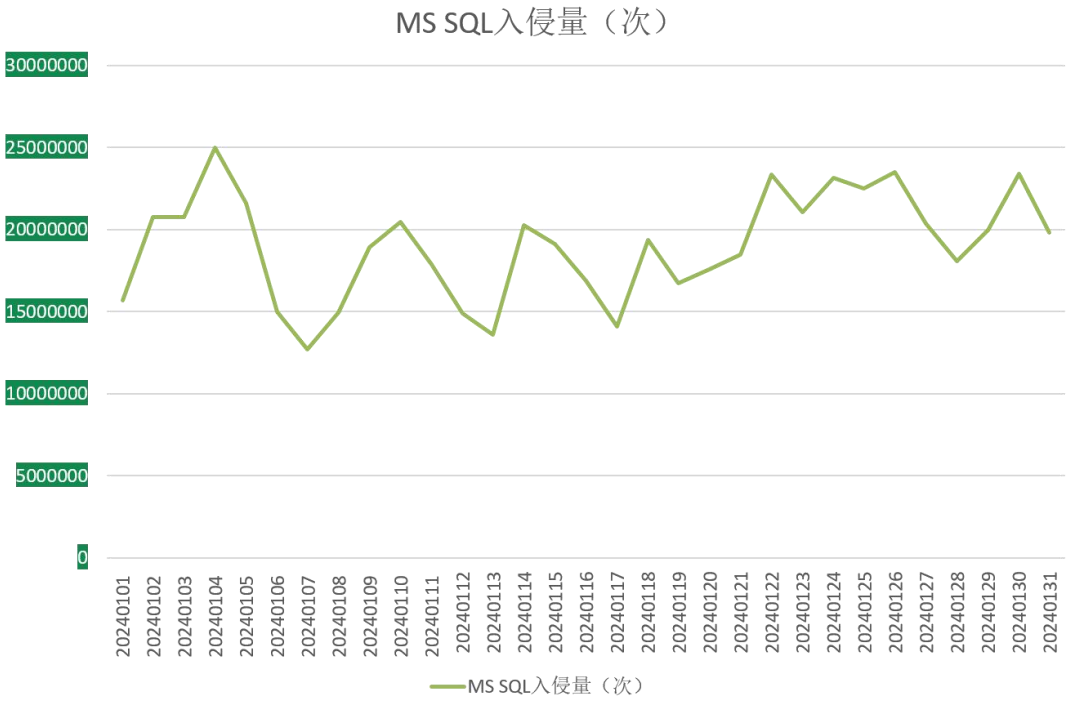


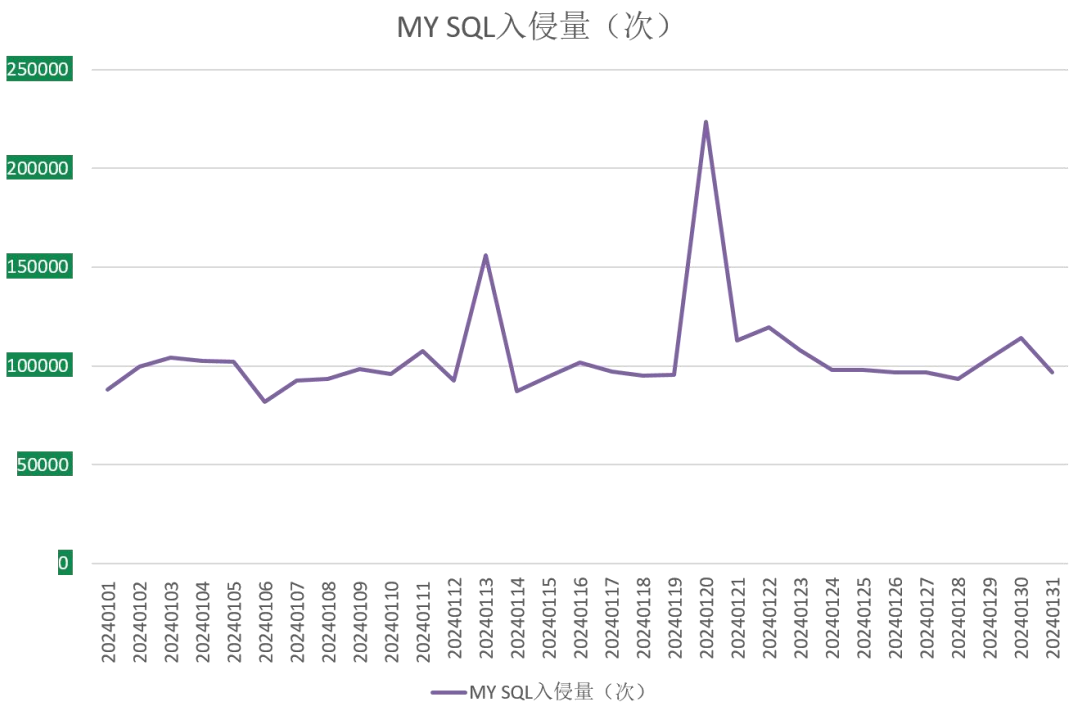
对 2024 年 1 月被攻击系统所属地域统计发现，与之前几个月采集到的数据进行对比，地区排名和占比变化均不大。数字经济发达地区仍是攻击的主要对象。



通过观察 2024 年 1 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。

- 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，本后缀为 10 月新增变种。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正通过匿影僵尸网络进行传播。

- 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。

- 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。

- 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。

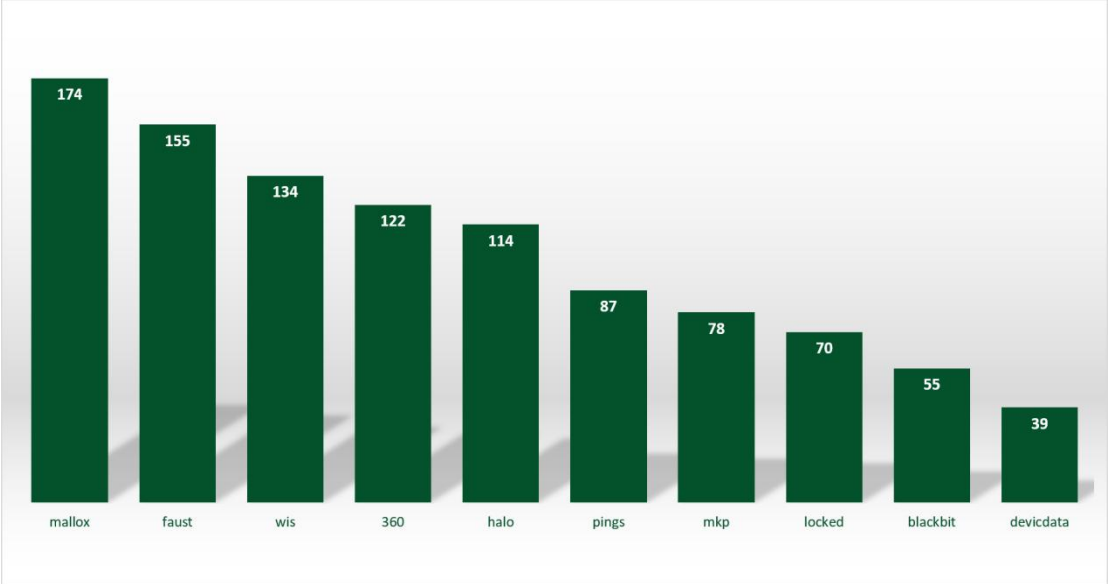
- pings：属于 TargetOwner 勒索软件家族，该家族的主要传播方式为：通过暴力破解远程桌面口令成功后手动投毒。

- mkp：同 wis。

- 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。

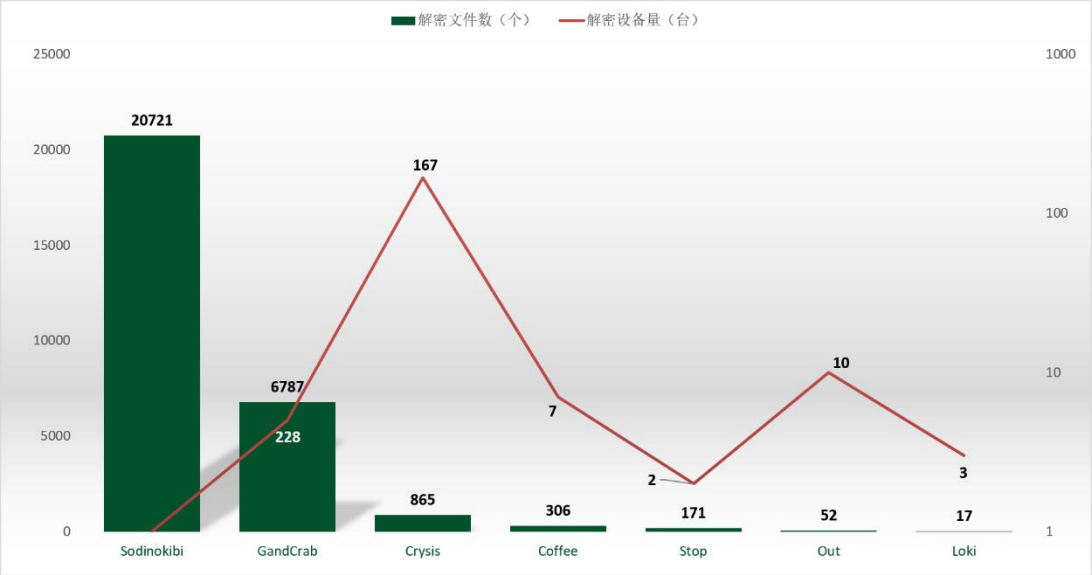
- blackbit：属于 Loki 勒索软件家族的分支变种，由于被加密文件后缀会被修改为 blackbit 而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。

- devicdata：同 mallox



解密大师

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




360数字安全
数 字 安 全 的 领 导 者
360安全大脑