2021 年 12 月勒索病毒态势分析

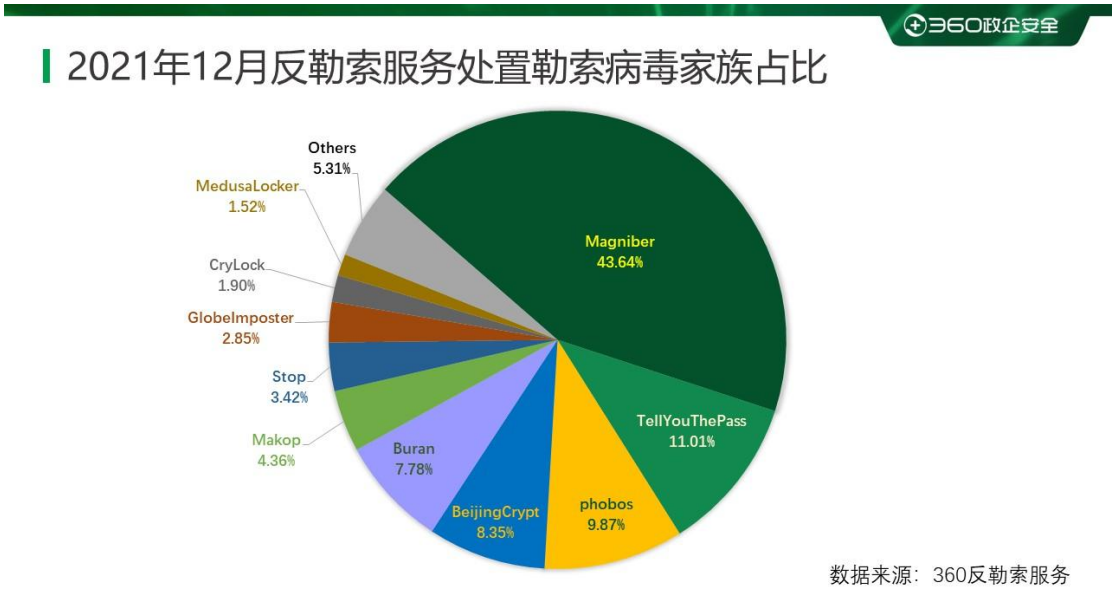
勒索病毒传播至今，360 反勒索服务已累计接收到上万勒索病毒感染求助。随着新型勒索病毒的快速蔓延，企业数据泄露风险不断上升，勒索金额在数百万到近亿美元的勒索案件不断出现。勒索病毒给企业和个人带来的影响范围越来越广，危害性也越来越大。360 安全大脑针对勒索病毒进行了全方位的监控与防御，为需要帮助的用户提供 360 反勒索服务。

2021 年 12 月，全球新增的活跃勒索病毒家族有：CarckVirus、Miner、Razer、Youneedtopay、Bl@ckt0r、Karakurt 等家族，其中 Bl@ckt0r、Karakurt 为本月新增的双重勒索病毒家族。在本月消失很长一段时间的 TellYouThePass 勒索病毒家族，利用 Log4j2 漏洞卷土重来。

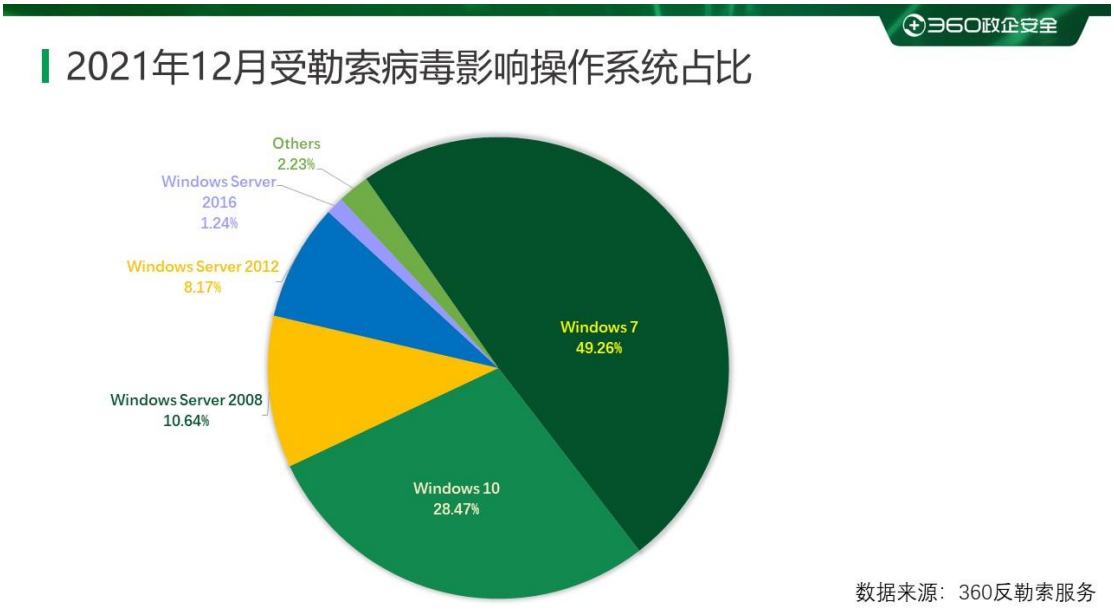
感染数据分析

针对本月勒索病毒受害者，所中勒索病毒家族进行统计，Magniber 家族占比 43.64%居首位，其次是占比 11.01%的 TellYouThePass，phobos 家族以 9.87%位居第三。

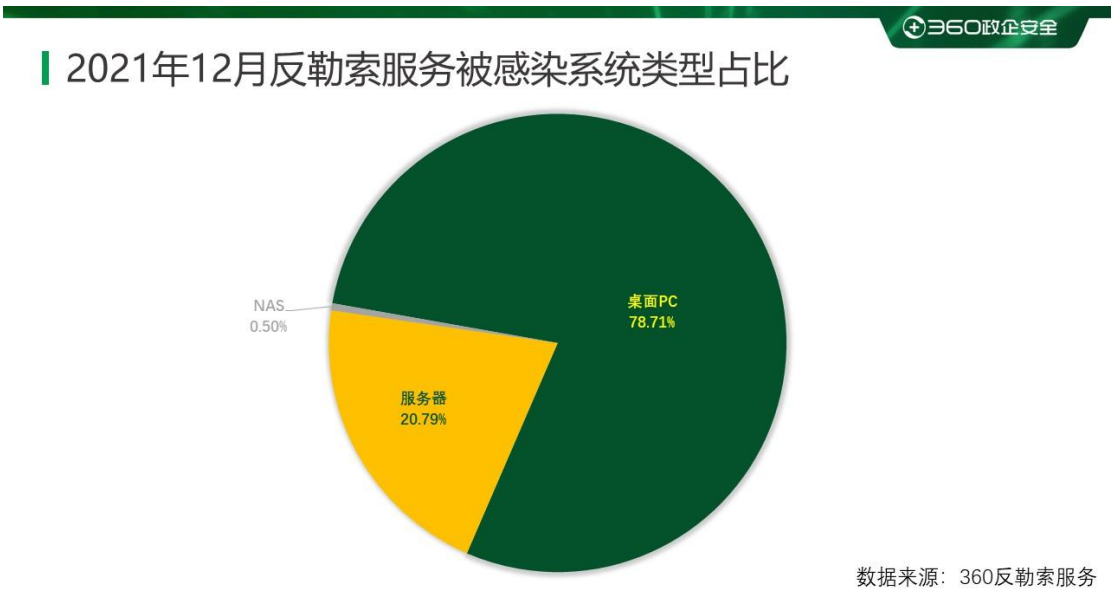
根据 360 安全大脑监控到的数据显示，12 月初，攻击者开始利用最新的 Log4j2 RCE 漏洞（CVE-2021-44228）传播 TellYouThePass 勒索病毒家族，使用某 OA 用户受灾严重。



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 7、Windows 10、以及 Windows Server 2008。



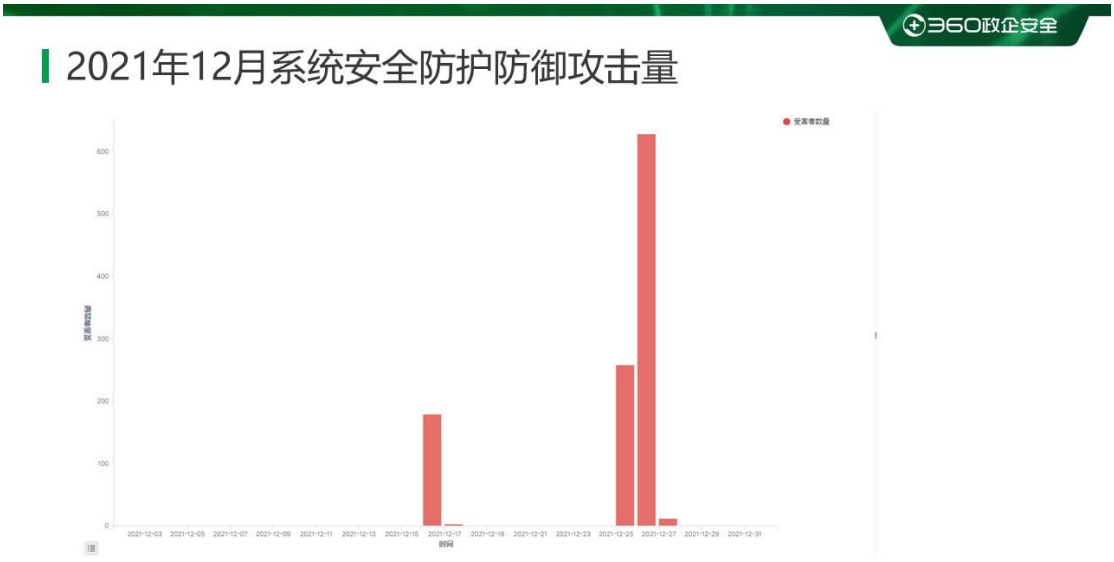
2021 年 12 月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型仍以桌面系统为主。与上个月相比，无较大波动。



勒索病毒疫情分析

Log4j2 漏洞被勒索病毒广泛利用

本月 Apache 的 Log4j2 组件被发现重大漏洞(CVE-2021-44228,远程代码执行漏洞)，该漏洞在 12 月 9 日被披露，在 12 月 11 日便出现大量针对 Log4j2 进行的恶意攻击行为。360 安全大脑监控到，曾消失了很长一段时间的 TellYouThePass 勒索病毒，在 12 月 17 日携 Log4j2 漏洞利用卷土重来，对某 OA 系统发起针对性攻击(该系统使用到了 Log4j2 组件)。该家族在传播时并没有像传统的勒索病毒一样选择持续性攻击，而是间断性的攻击。其在 12 月 27 日出现最大攻击量，单日被攻击设备超 600 台。



数据来源：360系统安全防护

由于 Log4j2 漏洞利用方式简单、危害严重，在本月还曾被多个勒索病毒家族使用。本月勒索病毒相关案件还有：

- 本月中旬，研究人员发现新型勒索病毒 Khonsari 尝试利用 Log4Shell 进行传播。攻击者利用 Log4Shell 远程执行代码漏洞从远程服务器下载.NET 二进制文件，该二进制文件对目标机器上的文件进行加密，并将扩展名.khonsari 添加到每个文件中。该病毒还会发出勒索信息，要求以比特币支付赎金。
- 本月下旬，著名勒索病毒家族 Conti 勒索病毒开始使用 Log4J 的相关漏洞来快速攻击 VMware vCenter Server 实例并加密虚拟机中的数据。
- 微软提醒自托管的 Minecraft 服务器管理员升级到最新版本，以抵御利用 Log4J2 漏洞进入系统的 Khonsari 勒索攻击。
- 越南最大的加密交易平台之一 ONUS 因其支付系统使用了带有漏洞 Log4j 导致遭到网络攻击。随后便找到攻击者威胁说已窃取其将近 200 万用户的数据，并索要 500 万美元的赎金。

洛杉矶计划生育协会遭遇勒索病毒攻击

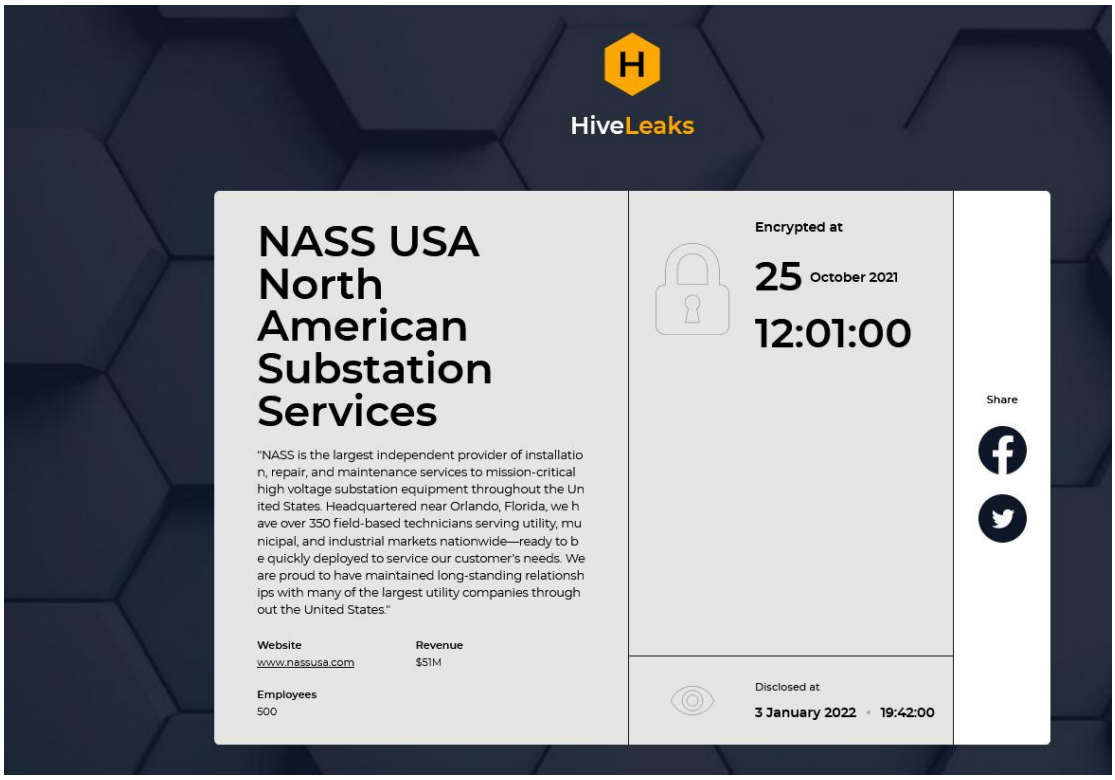
数据泄露带来的危害越来越明显，不仅影响企业/组织的正常运营，还将其负面影响逐步渗透到大众的生活。在本月，根据洛杉矶计划生育协会(PPLA)发送给患者的通知中透露的消息：该协会在 2021 年 10 月 9 日至 17 日之间遭受勒索病毒攻击(攻击者在其内网中潜伏了长达一周，通过这段时间在内网中寻找并窃取高价值信息数据)，导致 40 万名患者数据被黑客窃取，其中包含患者的地址、保险信息、出生日期、临床信息等。黑客在后续的勒索中，不仅向洛杉矶计划生育协会索要赎金，同时也将魔爪伸向了个人信息泄露的 40 万名患者。参考此前类似案例，黑客可能会利用这些会影响患者的名誉或工作的特点私密信息，以泄露给患者朋友或雇主为名，对患者本人勒索赎金。

Hive 勒索病毒组件大联盟，四个月内攻击数百个目标

通过安全研究员直接从 Hive 的管理小组收集到的信息发现，Hive 勒索病毒团伙可能比

其泄密站点显示的更加活跃，自该行动于 6 月下旬曝光以来，其下属组织平均每天攻击 3 家公司，其下属组织在四个月的事件入侵了超过 350 个企业或组织。

该团伙的数据泄露站点目前仅列出了 71 家未支付赎金的公司，表明有大量 Hive 勒索病毒受害者支付了赎金。保守估计，仅在 10 月到 11 月之间，Hive 勒索病毒团伙的利润就高达数百万美元。



Rook 勒索病毒是 Babuk 泄露代码的新一代衍生品

Babuk 勒索病毒家族在 2021 年 4 月攻击华盛顿警方后，因对从警方窃取到的 250GB 数据处理意见始终无法达成一致，最终内部分裂。在 6 月份其生成器被恶意泄露，在 9 月其完整的源代码被公开发布在暗网。

近期的网络攻击中出现的一款名为 Rook 的新型勒索病毒，其技术细节、传播链条以及方式，都与 Babuk 勒索病毒非常相似。该团伙自称急需通过破坏公司网络和加密设备来赚取“大量资金”。截止 2021 年 12 月 31 日，该家族已在其数据泄露网站公开发布过 6 名受害企业/组织信息。同时，从该家族的数据泄露网站发布的信息看，该家族陈，如果发现其网站不能被正常访问，将会立即发布受害者信息，企图通过威胁的手段阻止第三方（网络安全公司、执法部门等）攻击其基础设备。

We Are Rook!!!

We have not yet thought about how to introduce us.
We are a new group and our energy is very strong.
Time will witness our growth.
We hope that the media will make our introduction public.
contact us
rook@securityrook.com
securityrook@securityrook.com
Dear cyber security company, if we find that our server is inaccessible, we will immediately disclose the data.

Home **Archives** **About**

Data breach summary

2021-12-01 1 min read

黑客信息披露

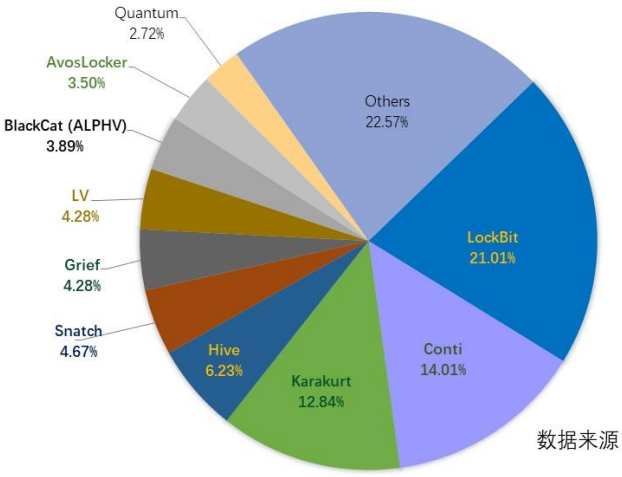
以下是本月收集到的黑客邮箱信息：

albertpattisson1981@protonmail.com	decryptionx@inboxhub.net	rook@securityrook.com
steven1973parker@libertymail.net	recover520@mailfence.com	sorryneedbtc@gmx.com
yourlovelysupport@mailfence.com	johnwilliams1887@gmx.com	malloxx@tutanota.com
helprestoremanager@airmail.cc	karenkhonsari@gmail.com	ecrypt24@nerdmail.co
securityrook@securityrook.com	bothelper@mailfence.com	cr0prop@firemail.cc
decryptyourfiles@firemail.cc	GoodDay@privatemail.com	filemanager@cock.li
Victorcrou@privatemail.com	Helper@privatemail.com	kingbo@tutanota.com
grejkugulik@onionmail.org	makopsupp@tutanota.com	code1024@keemail.me
decryptionx@onionmail.org	arnoldgladys88@gmx.com	2021@onionmail.org
yourlovelysupport@xmpp.jp	dr.helper@tutamail.com	encrypt11@cock.li
tSupport@privatemail.com	Dekrypt24@tutanota.com	fileback@tuta.io
edljackson@onionmail.org	webweb321@firemail.cc	fileback@cock.li
JimThompson@ctemplar.com	file-manager@email.tg	rpd@keemail.me
willettamoffat@yahoo.com	rapid@aaathats3as.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病毒家族越来越多，勒索病毒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病毒家族占比，该数据仅为没有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）。

2021年12月通过数据泄露获利的勒索病毒家族占比



数据来源：@darktracer_int (Twitter)

以下是本月被双重勒索病毒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 258 个组织/企业遭遇勒索攻击，其中中国仅有 1 个组织/企业在本月遭遇了双重勒索/多重勒索。

DFL	THONI ALUTEC	jpbdselangor.gov.my
LAVI	wagstaff.com	benlineagencies.com
Finq	ytlcement.com	Strataworldwide.com
RCMS	CHR Solutions	urbandevelop.com.au
RKPT	Unexca.edu.ve	lipinskilogging.com
LAVA	g1group.co.uk	Economos properties
HOULE	robroelaw.com	Bernd Siegmund GmbH
Ruwac	rbauction.com	Decorator Industries
Saand	tt-network.dk	hp.icon-institute.de
MEETH	Valley Realty	proximitysystems.com
Leuze	Pursell Farms	Nordic Choice Hotels
DENSO	PROFIL ALSACE	DuraTech Industries®
Seldin	maibroker.com	Meritus Associations
se.com	InTown Suites	Michael David Winery
Zepter	riverhead.net	ALPHA TRADING S.P.A.
Yanmar	ENVASES GROUP	sintesiautomotive.it
Raveco	Amigo-Kids.com	DEUTSCHE SEE Holding
WOLSEY	RLD Associates	Unified Technologies
Prenax	Altrux Medical	fr.shop-orchestra.com
Sodiba	Interiorscapes	Unique Home Solutions
Uriach	hsisensing.com	Powell Transportation
TUI UK	DOMICIM Agence	Contech TopSystems AG
Saksoft	Flanders Color	Data Access Worldwide
cgm.com	PACE Worldwide	Charles River Apparel
atlas.in	Kenall/Legrand	MIND Technology, Inc.

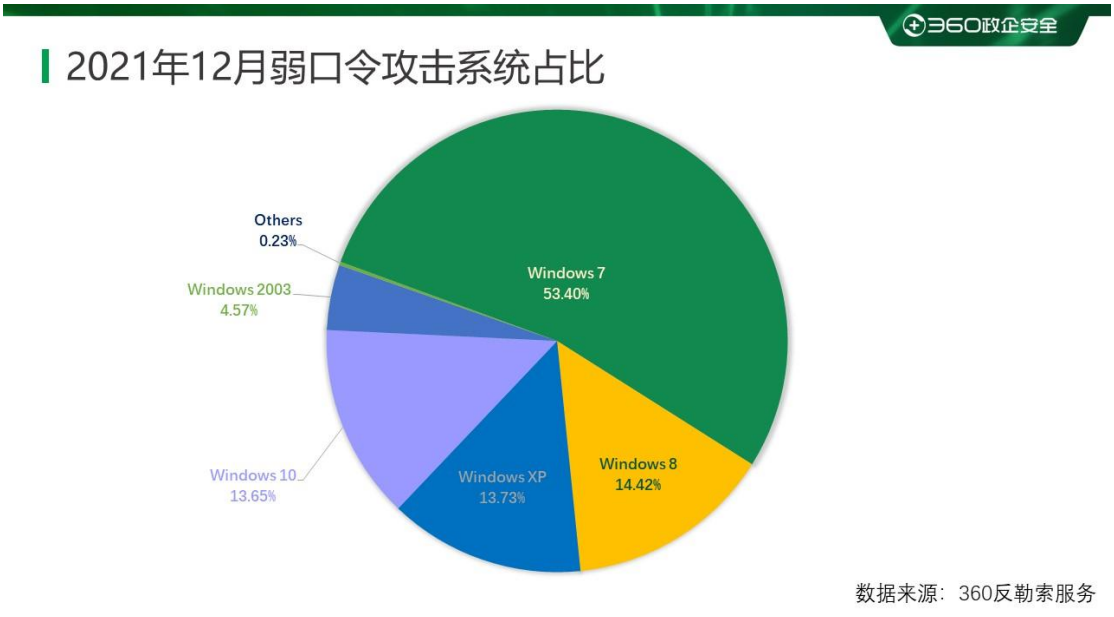
Jeffmoss	reliancenj.com	OPENROADAUTOGROUP.COM
Atlasdie	DUTTONFIRM.COM	cunninghamgolfcar.com
Lahebert	atskorea.co.kr	Haselden Construction
Biotique	smiimaging.com	prairiesedgecasino.com
Metro.Us	iGuzzini Group	Rosendahl Design Group
comark.ca	American Dream	The Execu|Search Group
nowiny.pl	CareFirst CHPDC	Dental Health Products
CS ENERGY	Versatrim, Inc.	The Kessler Collection
serta.com	caudillseed.com	Bohlin Cywinski Jackson
mswood.ba	clubpilates.com	SAS SUD TRADING COMPANY
ducab.com	P&R ENTERPRISES	Trigyn Technologies Ltd
UMW Group	Chantelle Group	Social Enterprise (SEC)
EBZ GROUP	Fiberstar, Inc.	The Preston Partnership
FC Dallas	Rossell Techsys	Skyxe Saskatoon Airport
Sonomatic	Eisai Co., Ltd.	Divestco Geoscience Inc
GryphTech	The Briad Group	SICAME AUSTRALIA PTY LTD
baa.legal	burgsimpson.com	NewWave Technologies Inc
Madix Inc	cbjblawfirm.com	PRIDE Community Services
MediaMarkt	Hako Technology	Five Star Products, Inc.
Clementoni	Charles Kendall	Kangean Energy Indonesia
vestas.com	Metamorph Group	Turner Enterprises, Inc.
Fittingbox	Texsource, Inc.	Fastline Media Group, LLC
Quanticate	Hahn Engineering	Mount Franklin Foods, LLC
Comtec USA	psmportraits.com	Douglas Shaw & Associates
Gym Source	Bemis Associates	Oroian Guest and Little PC
Wet Design	northstarice.com	Industrial Network Systems
KBKB, Ltd.	COMUNE DI TORINO	Component Assembly Systems
hajery.com	pacifichills.com	www.hillsdalefurniture.com
McMenamins	tamerholding.com	Bay and Bay Transportation
SVP Groupe	Petro Serve USA.	Arbor Contract Carpet Inc.
SNOP GROUP	skinnertrans.com	summit-christian-academy.org
Groupe LDLC	LIGHT CONVERSION	Bohlke International Airways
ORNATOP SRL	Holiday Builders	Hellmann Worldwide Logistics
MST LAWYERS	murrayscheese.com	MAX International Converters
bsm.upf.edu	Spencer Gifts LLC	CANAR OFFICE SYSTEMS COMPANY
Ktmtriallaw	apexbrasil.com.br	Faber Industrial Technologies
KOBE BUSSAN	Shoring Engineers	Kohinoor International School
TALIS GROUP	Jones Studio Inc.	The Technord industrial group
Amoria Bond	Katz & Associates	The Adelaïde Group (Verlingue)
agrofair.nl	CASINO WINNAVEGAS	Hawthorn The Community Pub Co.
Tegravendas	travel-general.com	RI Analytical Laboratories Inc
Sit'N Sleep	mainstreamdata.com	Newman, Newman & Kaufman, LLP.
JCWHITE.COM	roemer-lueftung.de	Family Christian Health Center

SPERONI SPA	kerrylogistics.com	Chattanooga Chamber of Commerce
Maad McCann	Unita Locale Socio	Drake & Scull International PJSC
lozzaspa.it	Mechanical Degrees	Pontificia Universidad Javeriana
Evalueserve	MTMRECOGNITION.COM	MIM TECH ALFA SL (EXTEN EBER SL.)
Lootah Group	KMG Prestige, Inc.	Western Heating & Air Conditioning
promhotel.fr	kssenterprises.com	Institute For Systems And Robotics
Kellersupply	continuumenergy.in	Remedial Construction Services L.P.
inperium.org	tlpterminal.com.my	Premier Crane & Transportation, Inc.
volkswind.de	Medical Pharmacies	Heritage Palms Professional Building
ENPRECIS.COM	Comerio Ercole spa	TRI-COUNTY ELECTRIC COOPERATIVE, INC.
masselin.com	Implant Concierge™	Wine & Spirits Retail Marketing, Inc.
Ncmutuallife	Better World Books	Digital Workplace Services & Solutions
vipsmotel.it	van Eupen Logistik	New City Commercial Corporation (NCCC)
ABC Seamless	Lincoln Industries	AL-SOOR FUEL MARKETING COMPANY K.S.C.P
WEBER_OTT AG	ConForm Automotive	SparJames Hall & CompanyHeron and Brearley
piolax.co.th	pestbusters.com.sg	The Jewelry Exchange is the Nations #1 Diamond Store.
dcashpro.com	Polysciences, Inc.	OFFICE OF THE NATIONAL BROADCASTING AND TELECOMMUNICATIONS COMMISSION
ABE Courtage	Sadbhav Engineering	

表格 2.受害组织/企业

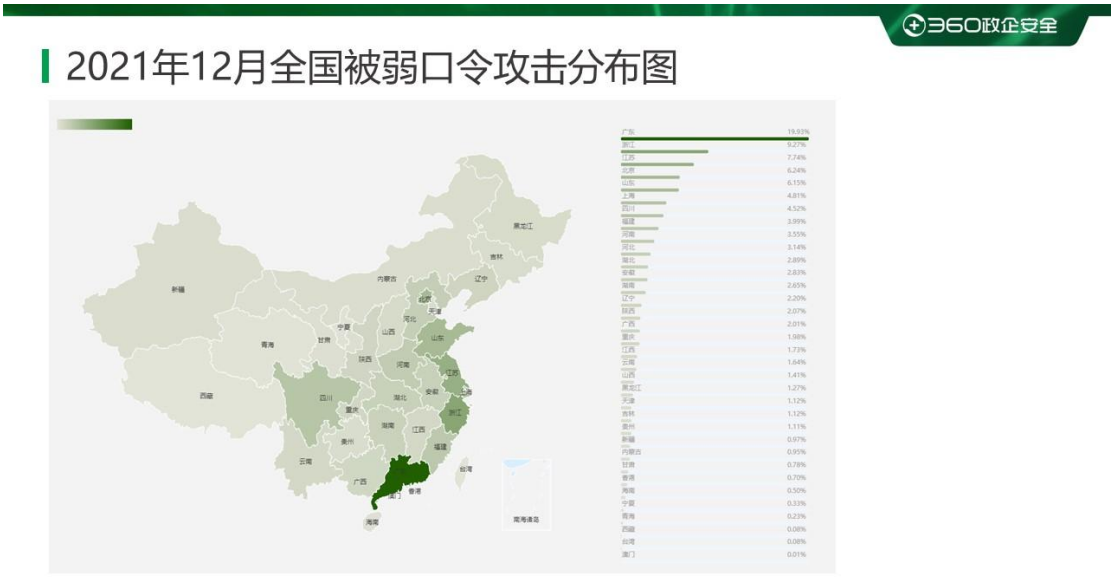
系统安全防护数据分析

通过将 2021 年 11 月与 12 月的数据进行对比，本月各个系统占比变化均不大，位居前三的系统仍是 Windows 7、Windows 8 和 Windows 10。



以下是对 2021 年 12 月被攻击系统所属地域采样制作的分部图，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。



数据来源：360系统安全防护

通过观察 2021 年 12 月弱口令攻击态势发现，RDP 弱口令攻击和 MYSQL 弱口令攻击整体无较大波动。MSSQL 弱口令攻击虽有波动，但无大的变动，整体呈下降态势。

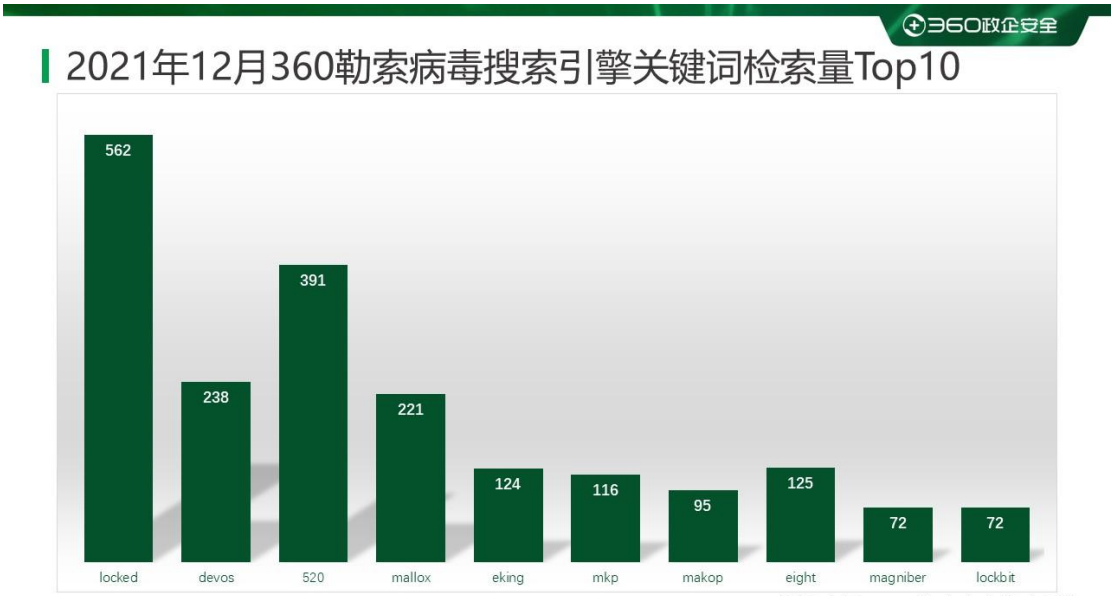
数据来源：360系统安全防护

勒索病毒关键词

以下是本月上榜活跃勒索病毒关键词统计，数据来自 360 勒索病毒搜索引擎。

- Locked:属于 TellYouThePass 勒索病毒家族，由于被加密文件后缀会被修改为 locked 而成为关键词。该家族本月主要的传播方式为：通过 Log4j2 漏洞进行传播。
- devos：该后缀有三种情况，均因被加密文件后缀会被修改为 devos 而成为关键词。但本月活跃的是 phobos 勒索病毒家族，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。
- 520：属于 BeijngCrypt 勒索病毒家族，由于被加密文件后缀会被修改为 520 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。

- Mallox:属于 Mallox 勒索病毒家族，由于被加密文件后缀会被修改为 mallox 而成为关键词。通过 SQLGlobeImposter 渠道进行传播。
- eking：同 devos。
- mkp：属于 Makop 勒索病毒家族，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。
- Makop：该后缀有两种情况，均因被加密文件后缀会被修改为 makop 而成为关键词：
  - 属于 Makop 勒索病毒家族，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。
  - 属于 Cryptojoker 勒索病毒家，通过“匿隐” 进行传播。
- eight:同 devos。
- Magniber: 被该家族加密的文件，后缀均被修改为随机字符串，其主要传播方式为：通过挂马网站进行传播。
-
- hauhitec：属于 YourData，由于被加密文件后缀会被修改为 hauhitec 而成为关键词。通过“匿隐” 僵尸网络进行传播。
- LockBit：LockBit 勒索病毒家族，由于被加密文件后缀会被修改为 lockbit 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。



数据来源：360勒索病毒搜索引擎

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，其次是被 CryptoJoker 家族加密的设备。

2021年12月解密大师解密量

数据来源：反勒索服务统计数据