2022 年 7 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。勒索病毒给政府机关、企业和个人带来的影响越来越广，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测与防御，为需要帮助的用户提供了 360 反勒索服务。

2022 年 7 月，全球新增的活跃勒索病毒家族有:Stop247、RoBaj、RedAlert、Checkmate、Lilith、Luna、BianLian、Omega 等家族，其中 RedAlert、Lilith、BianLian、Omega 均为双重勒索家族；Checkmate 为针对 NAS 设备发起攻击的勒索病毒；yanluowang 勒索病毒虽不是本月新增，但该勒索病毒家族在本月开始公开发布受害者数据。

以下是本月最值得关注热点：

一、新型勒索病毒 Checckmate 针对 NAS 设备发起攻击。

二、万代南梦宫在受到 AlphV 勒索病毒攻击后数据遭泄露。

三、LockBit 勒索病毒通过虚假的版权侵权邮件传播。

四、通过外挂程序进行传播的 SafeSound 勒索病毒已被破解。

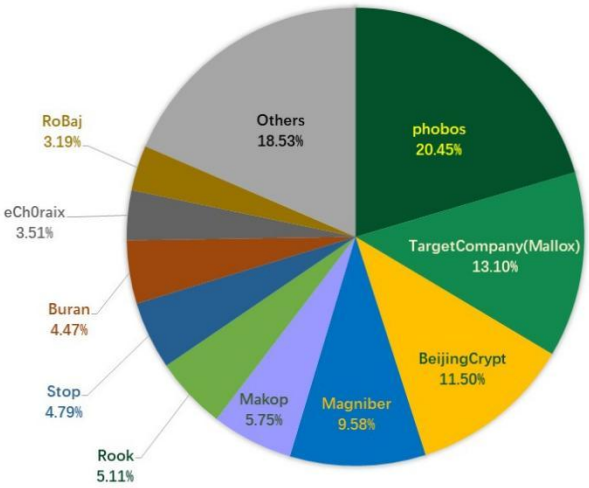
基于对 360 反勒索数据的分析研判，360 政企安全集团高级威胁研究分析中心(CCTGA 勒索软件防范应对工作组成员）发布本报告。

感染数据分析

针对本月勒索病毒受害者所中勒索病毒家族进行统计，phobos 家族占比 20.45%居首位，其次是占比 13.10%的 TargetCompany(Mallox)，BeijingCrypt 家族以 11.50%位居第三。

进入 TOP10 的几个家族中，Rook 勒索病毒再次变种，修改文件后缀为.lock，勒索提示信息内容也不再使用中文；Magniber 勒索病毒不再通过伪装成 msi 文件进行传播，而是伪装成杀毒的更新程序进行传播，同时主要传播目标也改为中国香港和中国台湾两地区；RoBaj 勒索病毒是本月新增的一款勒索病毒，目前发现该家族主要通过暴力破解远程桌面密码后手动投毒。

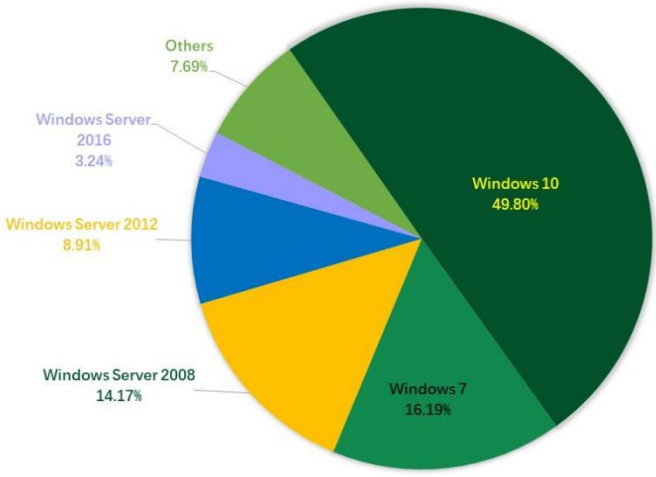
2022年7月反勒索服务处置勒索病毒家族占比



数据来源：360反勒索服务

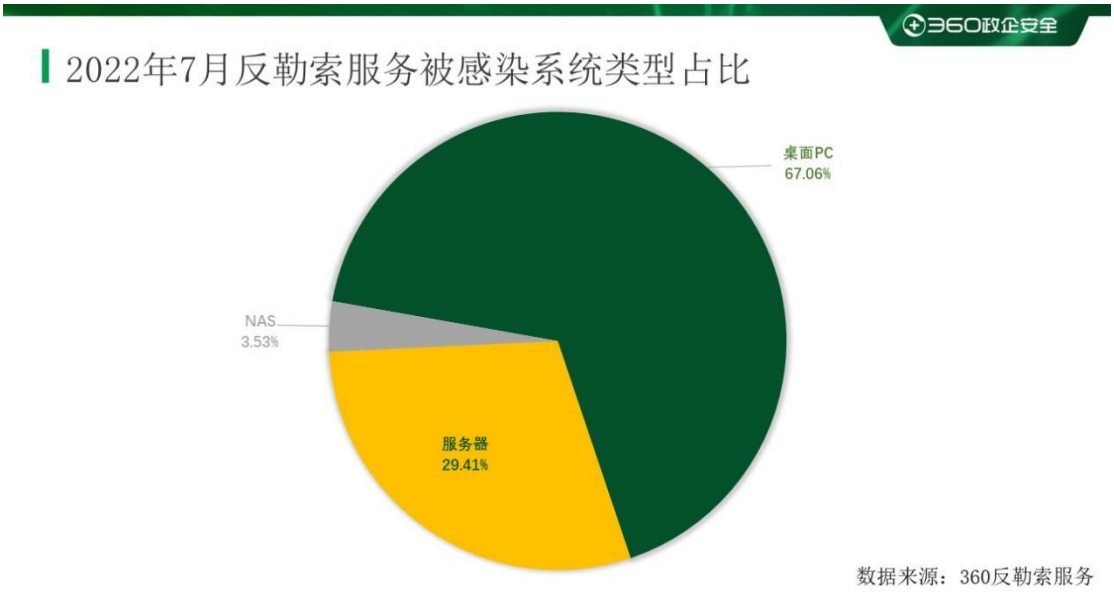
对本月受害者所使用的操作系统进行统计，位居前三的是：Windows 10、Windows 7、以及 Windows Server 2008。

2022年7月受勒索病毒影响操作系统占比



数据来源：360反勒索服务

2022 年 7 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

新型勒索病毒 Checkmate 针对 NAS 进行攻击

NAS 设备供应商 QNAP 警告用户称：要警惕 Checkmate 勒索病毒对 QNAP 的 NAS 设备发动攻击。这些攻击主要集中在启用了 SMB 服务且暴露在互联网中的设备上，且主要是一些登录口令较弱的帐户——这些帐户很容易在弱口令暴力破解的攻击中沦陷。

Checkmate 是最近新发现的勒索病毒。其首次出现在 5 月 28 日左右的攻击中，该病毒会将被加密的文件添加扩展名.checkmate 并放置一个名为“！CHECKMATE_DECRYPTION_README”的勒索文件。向受害者索要价值 15000 美元的比特币来解密。

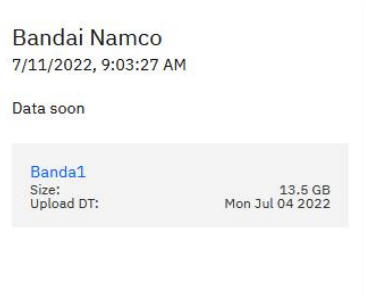
```
You was hacked by CHECKMATE team.
All your data has been encrypted, backups have been deleted.
Your unique ID: bc75c720f835********************
You can restore the data by paying us money.
We have encrypted 267183 office files.
We determine the amount of the ransom from the number of encrypted office files.
The cost of decryption is 15000 USD.
Payment is made to a unique bitcoin wallet.
Before paying, you will be able to make sure that we can actually decrypt your files.
For this:
1) Download and install Telegram Messenger https://telegram.org/
2) Find us https://t.me/checkmate_team
3) Send a message with your unique ID and 3 files for test decryption. Files should be no more than 15mb each.
4) In response, we will send the decrypted files and a bitcoin wallet for payment. Bitcoin wallet is unique for you, so we can find out what you paid.
5) After the payment is received, we will send you the key and the decryption program.
```

继 6 月披露威联通连续遭遇 eChOraix 和 DeadBolt 两款勒索病毒后，国内被勒索病毒感染的 NAS 设备量有所上涨，同时这已是第五款针对 NAS 设备发起攻击的流行勒索病毒。

万代南梦宫在受到 AlphV 勒索病毒攻击后数据遭泄露

本月初，BlackCat 勒索病毒（又名 AlphV）声称在一起攻击事件中攻陷了万代南梦宫的服务器并窃取了该公司的数据，并破坏了除日本以外的亚洲地区办事处的内部系统。

虽然万代南梦宫没有提供有关网络攻击的任何技术细节，但根据 BlackCat 数据泄漏网站所公布的数据条目及相关声明来看，万代南梦宫极有可能就是遭到了 BlackCat 的攻击。从公开显示的数据来看，万代南梦宫被窃取了 13.5GB 数据，但尚未被公开发布。



虽在 7 月的被公开数据中尚未有出现国内受害者，但 360 安全大脑监控到该家族在本月已成功攻击两个公司/组织。

LockBit 勒索病毒通过虚假的版权侵权邮件传播

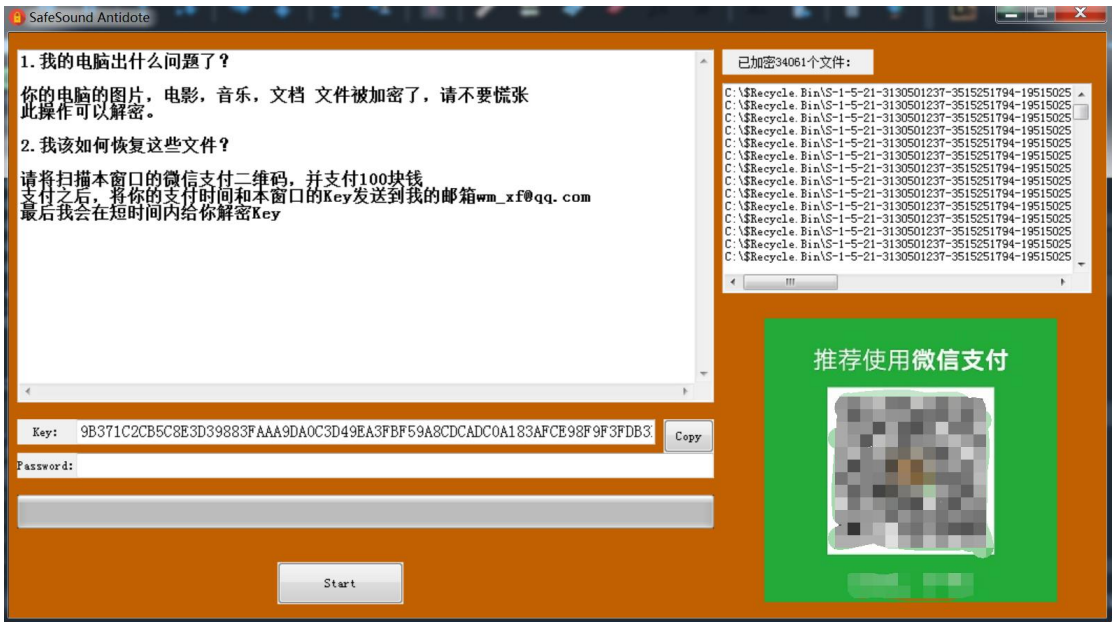
LockBit 勒索病毒正通过将恶意软件伪装成版权声明邮件来传播自身。这些电子邮件会警告收件人侵犯版权，声称收件人在未经创作者许可的情况下使用了某些媒体文件。邮件要求收件人从其网站中删除侵权内容，否则将面临法律诉讼。

目前分析人员捕获到的电子邮件内容中，并没有具体指出是哪些文件发生了侵权行为，而只是告诉收件人下载并打开附件以查看侵权内容。附件是一个受密码保护的 ZIP 存档，其中包含一个压缩文件，而该文件又是一个伪装成 PDF 文档的可执行文件（NSIS 安装程序）。

这种层层压缩和密码保护的手法主要是为了逃避电子邮件安全工具的检测。而一旦受害者打开所谓的“PDF”以了解具体的“侵权原因”，恶意软件便会释放 LockBit 2.0 勒索病毒对设备进行加密。

SafeSound 勒索病毒已被破解

本月一款国产勒索病毒通过“穿越火线”、“绝地求生”等外挂进行传播，被加密文件后缀会被修改为.SafeSound,并弹出勒索提示信息，需要受害者扫描微信二维码向黑客支付 100 元人民币作为赎金。



由于该勒索病毒制作存在缺陷，经过 360 政企安全集团高级威胁研究分析中心分析确认，可以进行技术破解。目前 360 解密大师已支持对该勒索病毒的解密。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

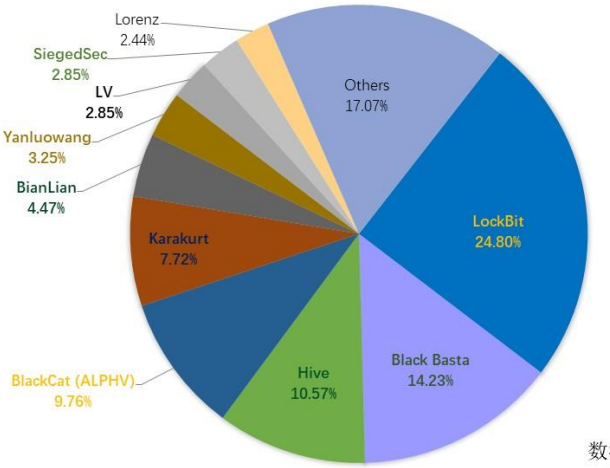
StephenJoffe@tutanota.com	StephenJoffe@protonmail.com	15010050@tutamail.com
17042102@tutamail.com	17042102@tutamail.com	43rgwe723E94@tutanota.com
LoryEstside@protonmail.com	henderson@cock.li	agares_helpdesk@tutanota.com
technopc@tuta.io	Angelbkup@protonmail.com	wixawm@gmail.com
helpshadow@india.com	helprecovery@gnu.gr	cyborgyarraq@protonmail.cn

webroothooks@tutanota.com	kardon@firemail.cc	henderson@cock.li
Trebaler@goat.si	Forbitlog@privatemail.com	ferguson@cock.li
sacipaws@tutanota.com	st3v3njansen@onionmail.org	justdoit@onionmail.org
okyd.dtt@mailfence.com	okyddd@protonmail.com	gtimph@protonmail.com
cupermate@elude.in	cupermate@protonmail.com	blefbeef@elude.in
vinilblind@protonmail.com	imperial755@protonmail.com	imperial@mailfence.com
jj.greemsy@mailfence.com	greemsy.jj@protonmail.ch	johny3@mailfence.com
johny2recoveryusa@protonmail.com	finbdodscokpd@privatemail.com	jorge.smith@mailfence.com
mally@mailfence.com	mallyrecovery@protonmail.ch	recoverfiles@ctemplar.com
recoverfilesquickly@ctemplar.com	primethetime@protonmail.com	ssdfsdfsdf@protonmail.com
ssdfsdfsdf@mailinfence.com	rickowens@onionmail.org	rickowens@mailfence.com
john.blues3i7456@protonmail.com	mario.jolly@mailfence.com	niss.brook@onionmail.org
niss.brandon@mailfence.com	Juli1992@mailfence.com	Juli1990@mailfence.com
stephenjoffe@privatemail.com	henderson@cock.li	helprecovery@gnu.gr
energyhack@cock.li	Trebaler@goat.si	recoverlokidata@gmail.com
yourecoverdatda@proton.me	yourecoverdata@proton.me	energyhack@cock.li
metro777@cock.li	arenotto@tutanota.com	henderson@cock.li
stop@onionmail.com	microd3c@tuta.io	dataappip@tutanota.com
mkpdec@hotmail.com	BluemanTeam@my.com	goodbooom@tutanota.com
gotocompute@tutanota.com	AntiLock@keemail.me	AntiLock@cock.li
rdecrypt@mailfence.com	Rdecrypt@yandex.com	Kardon@firemail.cc
NormanBaker1929@gmx.com	world2022decoding@jabb.im	world2022decoding@onionmail.com
yourecoverdata@proton.me	yourecoverdata@proton.me	alco2022decoding@onionmal.com
kat6.16st6r@tutanota	lordcracker@protonmail.com	CoronaCrypt[u.contact@aol.com
support@bestyourmail.ch	henderson@cock.li	nooli492@gmail.com
dqsupport@protonmail.com	sacipaws@tutanota.com	ferguson@cock.li
Juli1990@mailfence.com	energyhack@cock.li	selivrecovery@mail.ee
Forbitlog@privatemail.com	dagsdruyt@onionmail.org	dagsdruyt@cumallover.me
irishman@tutanota.de	irishman@onionmail.com	Nordteam@mail.ee
Nordtalk@tutanota.com	KingMail7@cock.li	LordCracker2@aol.com
top65hun@tuta.io	microd3c@xmpp.jp	microd3c@proton.me

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）。

2022年7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 246 个组织/企业遭遇勒索攻击，其中包含中国 7 个组织/企业在本月遭遇了双重勒索/多重勒索。

BAFNAGROUP.COM	get.es	AI Supercomputer
TLSBZ	Babylou	Destinigo
FPT Education	DISTRICT MUNICIPALITY OF HUACHAC	vytelle.com
emunworks.com	Creos Luxembourg	autoliv.com
Hong Kong Special Care Dentistry Association Limited	fruca.es	armassist.ie
tnq.co.in	herc.com.br	correounir.com.ar
Gage Brothers	coarc.org	JOHN A. BODZIAK ARCHITECT AIA
Fandeli	CIMEX	groupe-helios.com
Weidmueller	CUCA FRESCA	WAYAN NATURAL WEAR
Artistic Stairs & Railings	Baltholding OÜ	studioteruzzi.com
cheungwoh.com.sg	ymaunivers.com	sieam.fr
Empress EMS	APPLEXUS.COM	ginko.com.tw
eclipse-print.com	OptiProERP	agenziaentrate.gov.it
legacy-hospitality.com	SRM Technologies	riken.co.jp
daytonsuperior.com	KKJM Lawfirm	roedeanschool.co.za
Hometrust Mortgage Company	thep**********.com	sppc.com.sa
WARTSILA.COM	Yong Mao Environmental Tech. Co.,Ltd	laneprint.com.au
Baliwag Maritime Academy	osde.com.ar	taylorstafford.com
lanormandise.fr	townofstmarys.com	bizebra.com
Fairfax	Crum & Forster	CHDE POLSKA
HANDLER Bau GmbH	CREMO	a2-pas.fr
Site-technology	ocrex.com	mwd.digital
Chen Moore and Associates	Edenfield	lexingtonnational.com

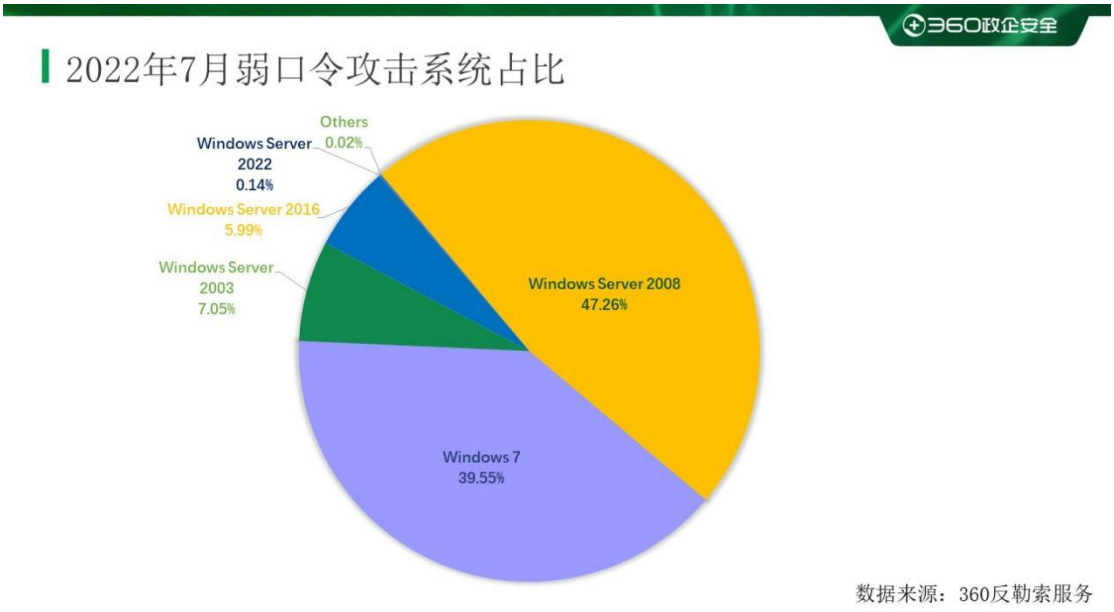
mec.com	Tom Barrow	LaVan & Neidenberg
COS2000	MAI	The Minka Group
SPINNEYS.COM	competencia.com.ec	addconsult.nl
coastalmedps.com	XQUADRAT GmbH	San Luis Coastal Unified School District
GENSCO Inc.	An Insurance Company	hcp*******.com
keystonelegal.co.uk	cpicfiber.com	madcoenergi.com
rovagnati.it	clestra.com	crbrandsinc.com
christianaspinecenter.com	columbiagrain.com	fedefarma.com
Turnberry Associates	Delon Hampton & Associates, Chartered	Autohaus
Broshuis | Driving innovation	Fedfina	FederalBank
bizframe.co.za	integrate.ch	aresfoods.ca
An British Financial Company	Eka(Business/Productivity Software)	sig.id
Oklahoma Ordnance Works Authority	ryanhanley.ie	ISGEC Heavy Engineering
VERITAS Solicitors	Conway Electrics	M****
Carrolls Irish Gifts	Metropolitan Associates	C2CORP
KNAUF	ttdwest	WALLWORKINC
augustacoop	paradise	Montmorency College
Rain the Growth Agency	Unisuper S.A.	Behavioral Health System
FMT	RALLYE-DOM	CITY-FURNITURE
frederickco.gov	ZEUS Scientific	etgworld.com
RTVCM	Exela Technologies	APETITO
Epec.PL	AdaptIT	Van Ausdall & Farrar, inc
Biothane usa	Gresco	GROUP4 AUSTRALIA
Authentic Brands Group	SANDO	Waskaganish
dudafresh.com	duda.com	viera.com
vierabuilders.com	Podhurst Orseck	iis.ac.uk
Mackenzie Medical	Anderson Insurance Associates	High Power Technical Services
Mooresville Schools	American International Industries	Makeready
Shanghai Hanbell Precise Machinery Co Ltd	Summit Care	Uppco
PSA	vlp.nl	Maxey Moverley
The Royal Commission for Riyadh City (RCRC)	Bandai Namco	Hydraelectric
Pontal Engineering	Meritus	vahanen.com
An International Shipping Company	Trade-Mark Industrial Inc.	lapostemobile.fr
Rewash	John Moore Services	Stm.com.tw
carnbrea.com.au	The Wiener Zeitung media group	LOKALTOG
RENZEL	Wagstaff Piling	Wipro HealthPlan Services
Sierra Pacific Industries	Jinny Beauty Supply	LOSSEWERK
BOERNER-GRUPPE	Jakob Becker	RBBUSA
SCHMIDT Gruppe Service GmbH	WENZEL + WENZEL	TMI

DEKIMO	BAUER	Young & Pratt
Gatewayrehab	LYDECKERLAW	OLYMPIATILE
Dusit D2 Kenz Hotel Dubai	Lamoille Health	Assura Group
DPP	alpachem.com	cabbageinc.com
idex.fr	Sinclair Wilson	syredis.fr
Solví Group	Adler Display	Pontal Engineering Constructions and Developments
V-Soft Consulting	Wis-Pak, Inc	Vectalia group
Goodwill industries	The Green Factory	The Janesville Gazette
A Lord Brasil é	DIRECTFERRIES	Hamlyns Limited
Sappi	Holland CPA	NETWORK4CARS
WWSTEELE	CAN.COM	AUM
KDE	Yurtiçi Kargo	Massy Distribution Limited
MHIRE	Montrose Environmental Group, Inc	CAPSONIC
V2 Logistics Corp	OLDPALMGOLFCLUB	plravocats.fr
slpcolombus.com	axelcium.com	faacgroup.com
lesbureauxdelepargne.com	bosco-avocats.com	expeditors.com
inces.com	Timios Inc.	boxerproperty
Shorr.com	tmsw.com	havi.com
various organizations	Walmart	Cincinnati bell
HANSA KONTAKT	Amalfitana Gas Srl	Continental Management

表格 2. 受害组织/企业

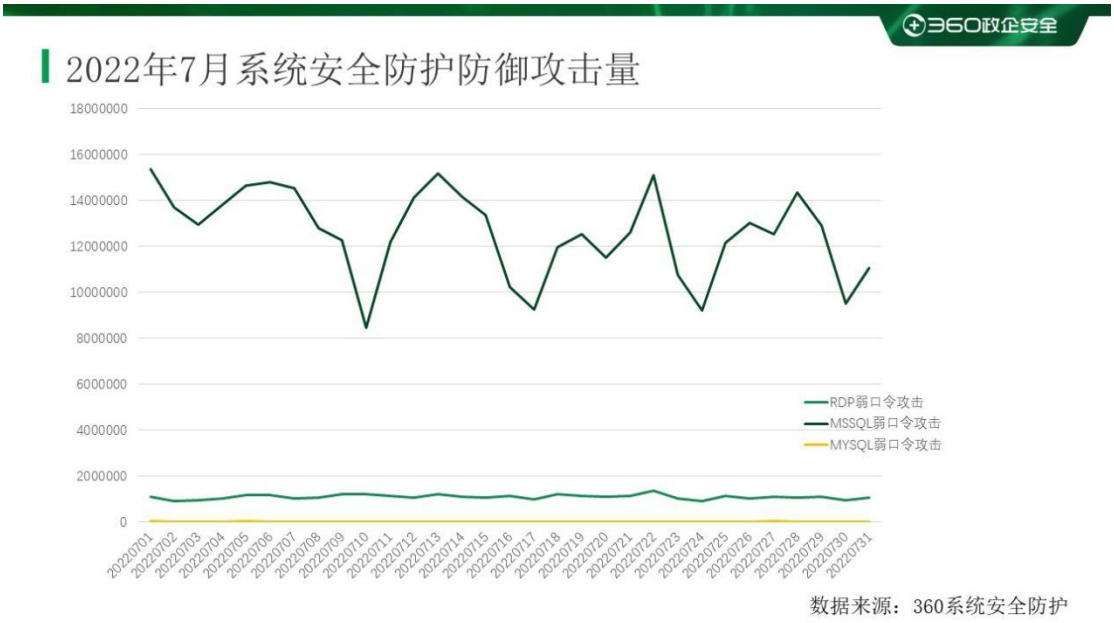
系统安全防护数据分析

360 系统安全产品，针对服务器进行全量下发系系统安全防护功能，针对非服务器版本的系统仅在发现被攻击时才下发防护。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 Server 2003。



对 2022 年 7 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。

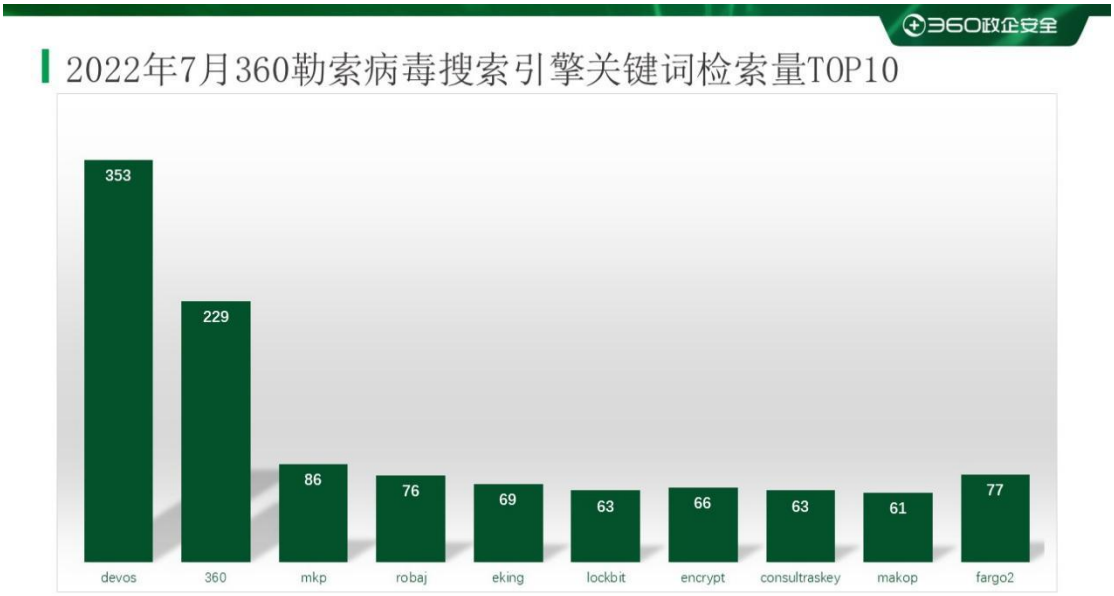
通过观察 2022 年 7 月弱口令攻击态势发现,RDP 弱口令攻击、MYSQL 弱口令攻击和 MSSQL 弱口令攻击整体无较大波动.



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。

- 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。
- 360：属于 BeijngCrypt 勒索病毒家族，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成功后手动投毒，本月新增通过数据库弱口令攻击进行传播。
- 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。
- RoBaj：属于 RoBaj 勒索病毒家族，由于被加密文件后缀会被修改为.RoBaj 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。
- eking：属于 phobos 勒索病毒家族，由于被加密文件后缀会被修改为 eking 而成为关键词。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。
- lockbit:属于 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。被该家族加密还可能涉及数据泄露的风险，该家族有一个大型团伙，其攻击手法多样化，不仅仅局限于弱口令爆破，还包括漏洞利用，钓鱼邮件等方式进行传播。
- encrypt：属于 eCh0raix 勒索病毒家族，由于被加密文件后缀会被修改为.encrypt 而成为关键词。该家族是一款针对 NAS 设备进行攻击的勒索病毒，主要通过漏洞攻击威联通设备，同时还曾对群辉设备采取桌面弱口令攻击。
- consultraskey: 属于 TargetCompany(Mallox)勒索病毒家族，由于被加密文件后缀会被修改为 consultraskey-id。该家族传播渠道有多个，包括匿隐僵尸网络、横向渗透以及数据库弱口令爆破。
- makop：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。
- fagro2:同 consultraskey。



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 Crysis，其次是 CryptoJoker。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，其次是被 Crysis 家族加密的设备。

其中 SafeSound、Yanluowang 和 7Locker 为本月新增解密家族。

数据来源：反勒索服务统计数据