2022 年 1 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。

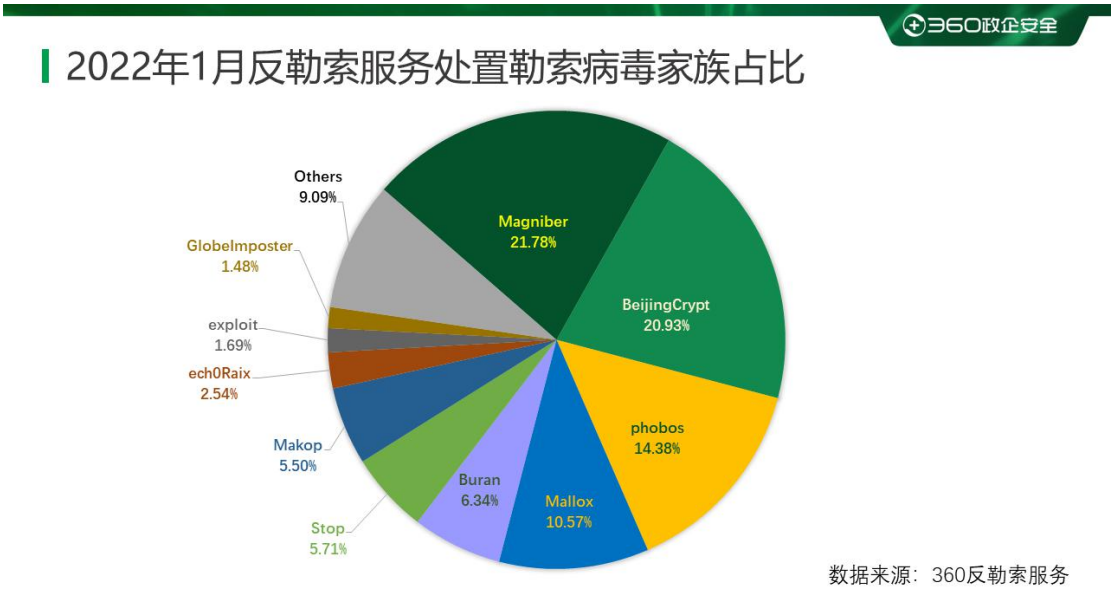
2022 年 1 月，全球新增的活跃勒索病毒家族有：Coffee、Night Sky、DeadBolt、Koxic、Trap、EvilNominatus 等家族，其中 NightSky 是本月新增的双重勒索病毒，利用 Log4j 漏洞对 VMwaer Horizon 服务器发起攻击；DeadBolt 是一款针对 QNAP 网络存储设备进行攻击的勒索病毒，该团伙向 QNAP 索要 50BTC 以提供万能密钥。

感染数据分析

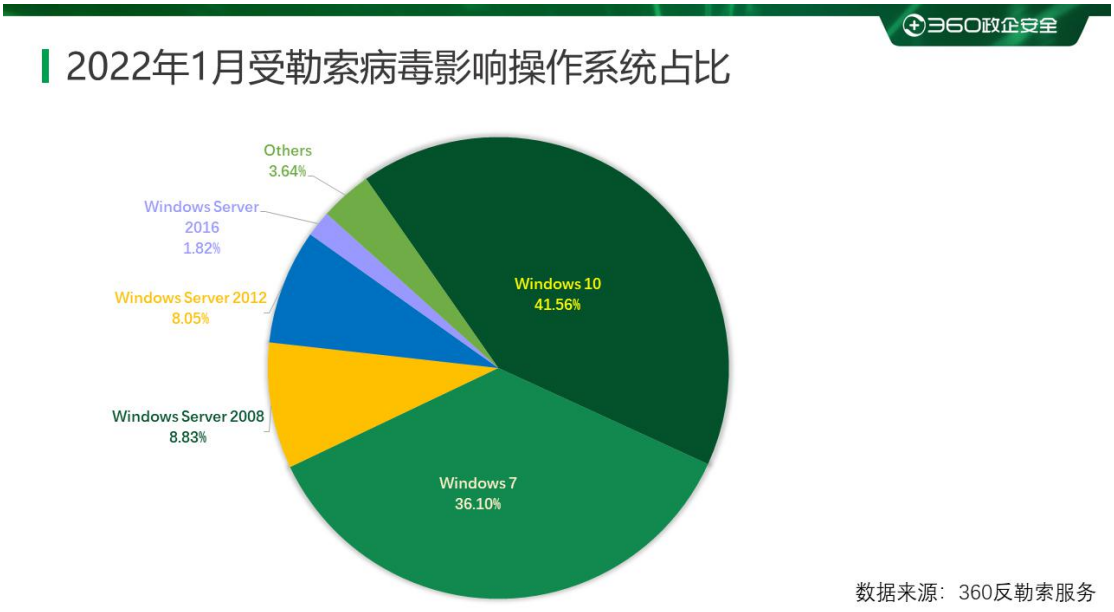
针对本月勒索病毒受害者所中勒索病毒家族进行统计，Magniber 家族占比 21.78%居首位，其次是占比 20.93%的 BeijingCrypt，phobos 家族以 14.38%位居第三。

根据 360 安全大脑监控到的数据显示：

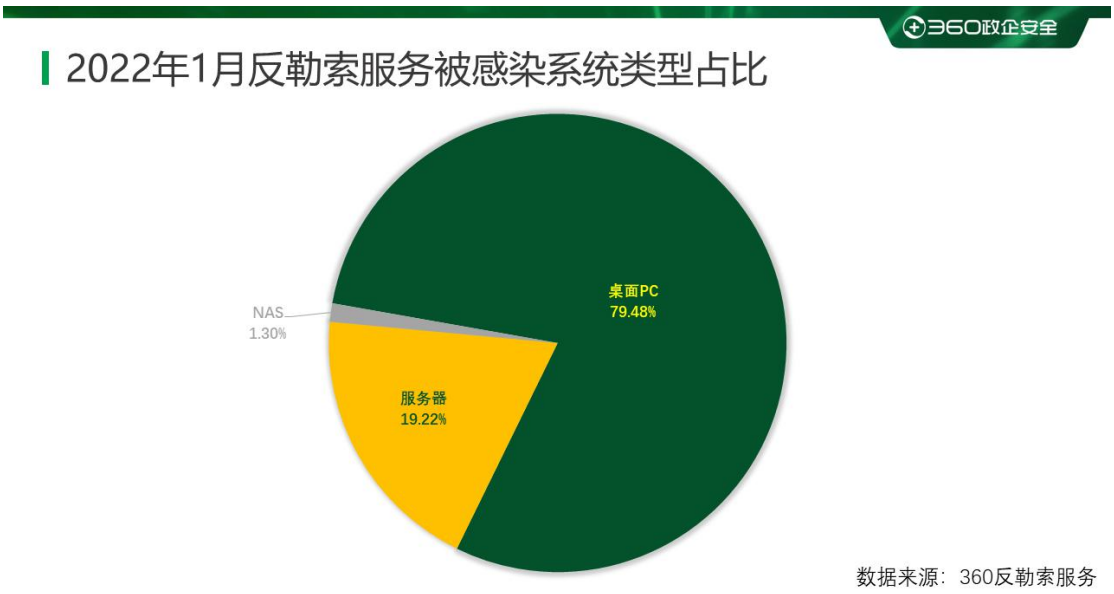
- 本月 BeijingCrypt 勒索病毒家族的传播量有上升，该家族对其传播渠道进行了扩展，将数据库弱口令攻击方式作为另一主要传播方式。
- 本月扩展传播渠道的还有 Mallox 勒索病毒家族，本月发现该家族还使用到了匿影僵尸网络。
- 本月首次在国内发现由 Babuk 泄露代码衍生而来的 Rook 勒索病毒。



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。



2022 年 1 月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型仍以桌面系统为主。与上个月相比，无较大波动。



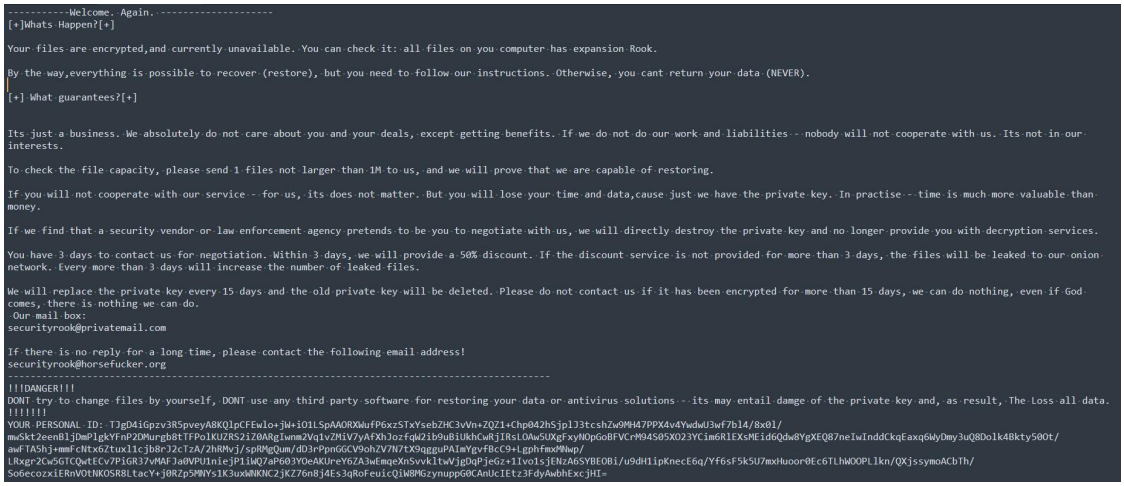
勒索病毒事件

Rook 勒索病毒可能会令数据永久丢失

2021 年 11 月 360 安全大脑监控到由 Babuk 泄露代码衍生而来的 Rook 勒索病毒开始采用双重勒索的模式进行传播。截止该家族 2022 年 1 月 8 日最后一次公布受害者名单，已有 7 个公司/组织遭遇该家族攻击。

在本月底，360 安全大脑监控到该家族通过匿影僵尸网络开始在国内传播，修改被加密文件后缀为.rook,rook2,rook3。从勒索提示信息看，此轮攻击虽提到会将从受害者处窃取到的数据公布到暗网，但该家族的数据泄露网站目前仍无法访问。同时，该团伙称他们将会

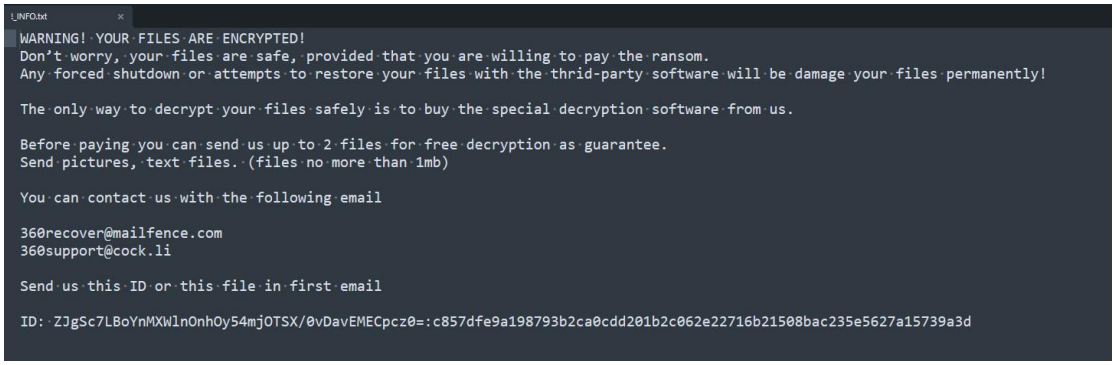
每 15 天更换一次私钥，而旧的私钥将被删除。如果文件被加密已超过 15 天，他们也将无法恢复。



BeijingCrypt 最新变种修改后缀为.360

根据 360 安全大脑数据，发现活跃勒索病毒家族 BeijingCrypt 出现新变种——被加密文件后缀变为“.360”，黑客的联系邮箱则变更为“360support@cock.li”和“360support@mailfence.com”。

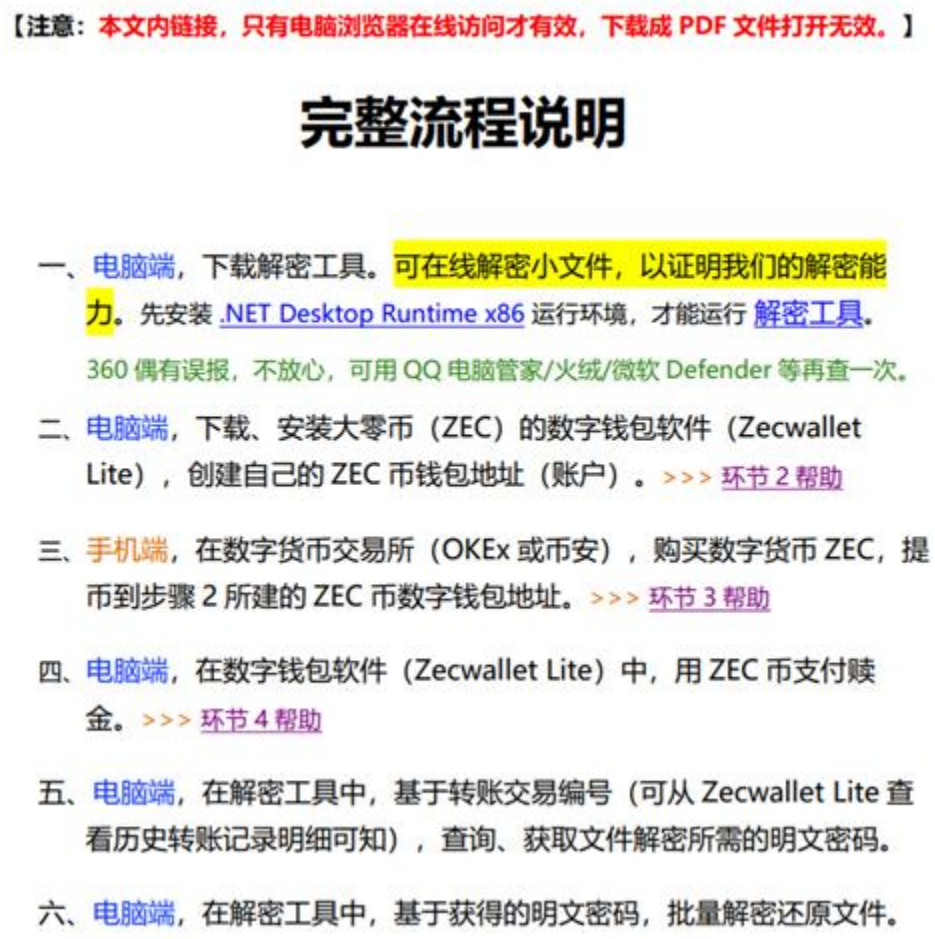
该勒索病毒家族因其早期将文件后缀修改为“beijing”而得名（beijing 后缀当前仍在使用）。自 2020 年 6 月出现以来，其就利用远程桌面弱口令在国内传播，并在 2021 年开始传播量越来越逐月上升，最终跃升至国内勒索病毒传播量 Top10 榜单。目前该家族已经历了 genesis、beijing、520、file、360 等多个后缀变种且传播越发活跃。在本月，该家族还通过爆破破解获取数据库口令后向受被攻击设备下发勒索病毒。



本土勒索病毒家族 Coffee 开始传播

根据 360 安全大脑数据，发现国内新出现勒索病毒家族 Coffee。该家族以其将加密后的文件后缀修改为 coffee.xxxx(x 为随机字符)而得名。Coffee 病毒是一个具有蠕虫性质的勒索病毒，一般通过软件捆绑和 QQ 群钓鱼传播，能够感染系统中常用软件，同时还可以主动将自己发往 QQ 群传播。该家族向受害者索要 ZEC（零币）这一较为罕见的虚拟货币作为

赎金。其不仅提供了中文的勒索信息，还附带了非常详细且“贴心”的全中文支付教程——指导用户如何对 ZEC 进行安装、购买和支付。从目前捕获到的信息看，该病毒会向受害者索要价值 500 美元的 ZEC。

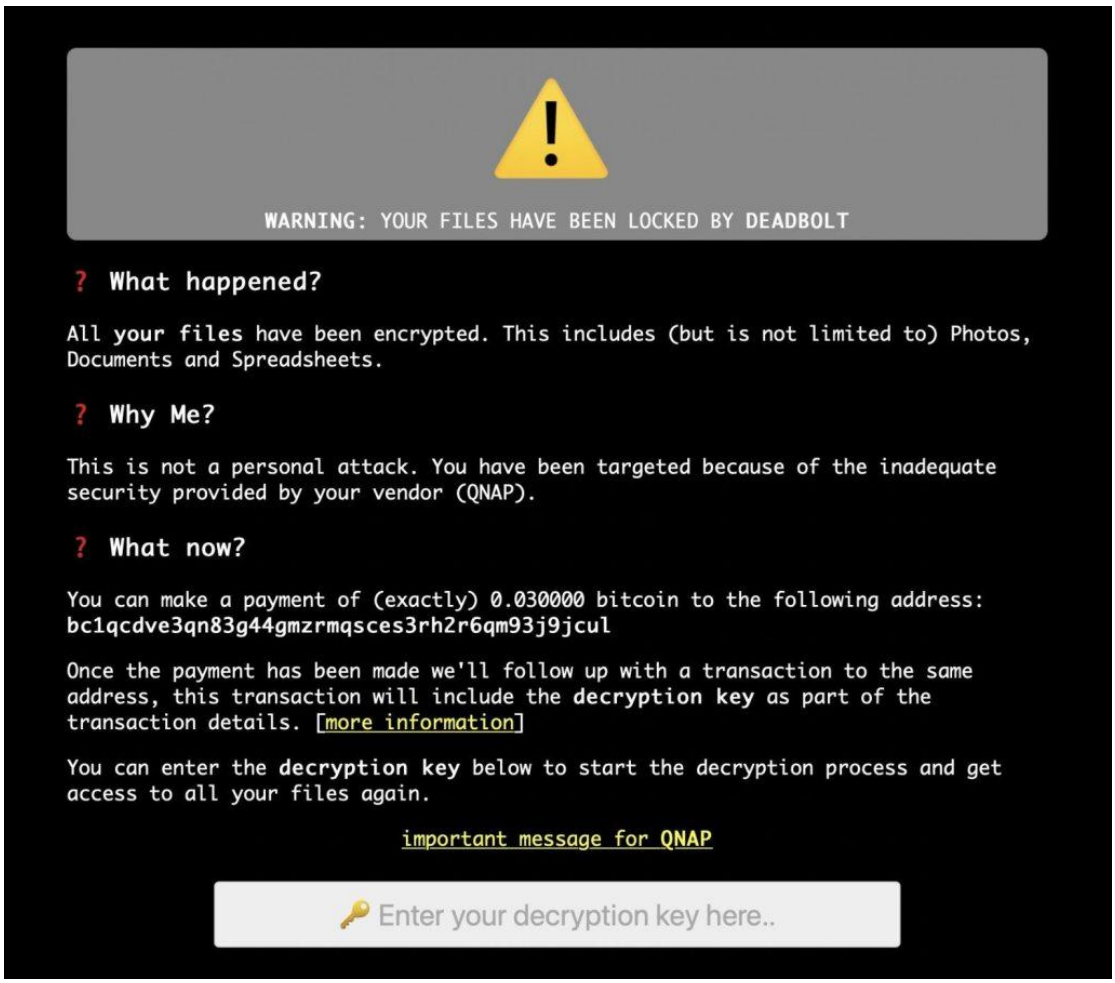


新勒索病毒 DeadBolt 瞄准 QNAP 设备，索要 50 BTC 提供万能密钥

新兴勒索病毒 DeadBolt 声称他们正在使用设备软件的 0day 漏洞对全球 QNAP NAS 设备进行加密攻击。

攻击于 1 月 25 日开始，中招的 QNAP 设备会突然发现其文件被加密，设备中存储的文件的文件名会被追加一个名为.deadbolt 的文件扩展名。而设备的登录页面会被劫持显示一个勒索页面：内容为“警告：您的文件已被 DeadBolt 锁定”等。该页面会向受害者索要 0.03 个比特币作为赎金。

此外病毒还在勒索页面中声称，如果 QNAP 向他们支付 5 个比特币，DeadBolt 勒索软件团伙将提供 0day 漏洞的全部详细信息。同时他们还愿意以 50 个比特币的售价向 QNAP 出售可以为所有受害者解密文件的主密钥和 0day 信息。



黑客信息披露

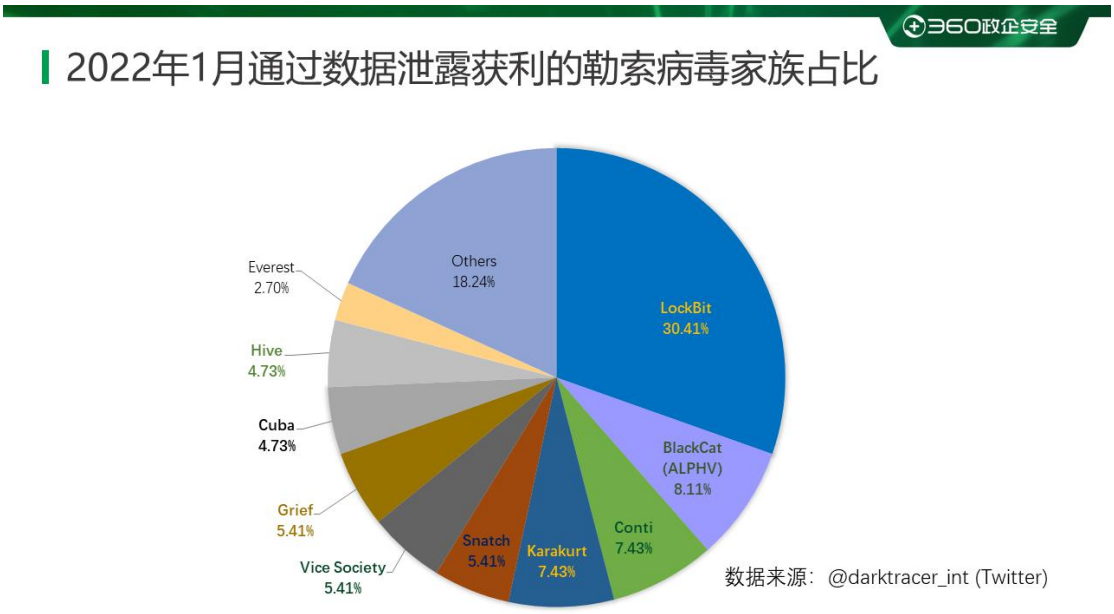
以下是本月收集到的黑客邮箱信息：

mallox@cock.li	qazqwe@onionmail.org	FilesRecoverEN@gmail.com
floy2020@cock.l	steriok@mail2tor.com	asiarecoverydata@cock.li
Elbowtalk@my.com	phobos_helper@xmpp.jp	proper12132@tutanota.com
zitenmax@cock.li	Myfiles.sir@gmail.com	restaurera@safeswiss.com
temloown@tuta.io	decypt20@firemaill.cc	beijing5200@mailfence.com
BillScars@gmx.com	keepserver2020@cock.li	jackrasal@privatemail.com
qazqwe@msgsafe.io	Jeseekuer@tutanota.com	malloxdatac@mailfence.com
ghxyz@fonix.email	anony.alex22@gmail.com	beijing520@horsefucker.org
360support@cock.li	walter1964@mail2tor.com	FobosAmerika@protonmail.ch
temloown@gmail.com	ofizducwel11988@aol.com	recoveryfiles@techmail.info
monster666@tuta.io	360helper@mailfence.com	veronikstreem@protonmail.com
helpunlock@aol.com	tsuppor@privatemail.com	cigleperation@protonmail.com
restaurera@rbox.co	6lilium6@protonmail.com	securityrook@horsefucker.org
support@sysmail.ch	360support@mailfence.com	securityrook@privatemail.com
guan_yu@tutanota.com	phobos_helper@exploit.im	isecondhelperforunlockyourfiles@airmail.cc

mrpicokins@gmail.com	psychopath7@tutanota.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 147 个组织/企业遭遇勒索攻击，其中包含中国 2 个组织/企业在本月遭遇了双重勒索/多重勒索。

RRD	Division-D	chervongroup.com
XAL	AKIJ GROUP	Atlantic Asphalt
Cle	Iwis Group	Maple Lodge Farms
DURA	www.paw.eu	Northern Contours
EDSI	Gardenworks	Thomson Broadbent
STIMM	bayview.com	Bank of Indonesia
Subex	Fdcbuilding	harrisshelton.com
izo.es	snapmga.com	centralbankfl.com
PLACON	bricofer.it	Mecanico Cairo SL
HAPOLO	supersave.ca	onlinesalespro.com
Arcese	bernheim.org	Hall Cross Academy
joda.de	Abdi ibrahim	JALEEL TRADERS LLC
ipec.ro	cbibanks.com	fairnessforall.com
RIVADIS	NORDFISH SRL	Perennials Fabrics
UNICRED	Little Giant	Imperial Logistics
Moncler	rightsys.com	lee-associates.com
CSEG.CN	aulss6.veneto.it	huntsville4rent.com
48Forty	elitemate.com	salesiancollege.com
Arc Com	elmonterv.com	themisautomation.com

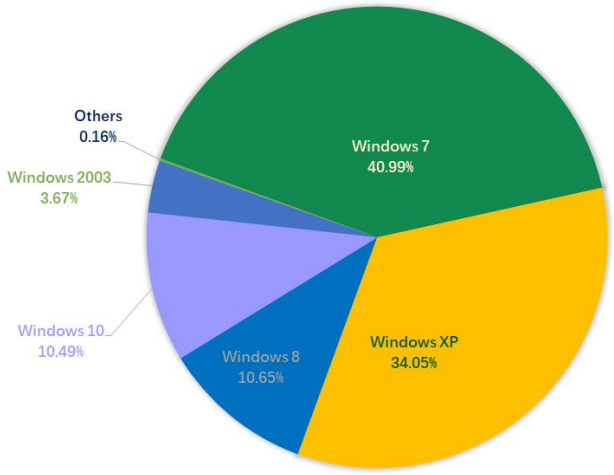
Sectrio	saintcloud.fr	Vehicle Service Group
Optionis	ambau-team.de	Lyon-Waugh Auto Group
estpm.fr	optimissa.com	Lewis & Clark College
Mtlcraft	mfkmakina.com	lhotellerie-restauration.fr
Redbadge	Acuity Brands	northsideplumbing.com
Hensoldt	Hanon Systems	securiteassurance.com
Regulvar	amerplumb.com	girlguidinglaser.org.uk
Mab Group	Amaveca Salud	independentprinting.com
efile.com	FrenchGourmet	Butler Community College
Safeguard	Weldco Beales	CIG de la Grande Couronne
Superfund	empireins.com	SAVANNAH State University
TaxNetUSA	Claro Colombia	The City of Pembroke Pines
Delinebox	bannerbuzz.com	The Public Safety Credit Union
Ezz Steel	Brookson Group	Cree Nation of Waskaganish
Huhtamaki	khattarlaw.com	東京コンピュータサービス
aquila.ch	Detroit Stoker	Creative Liquid Coatings INC
BainUltra	mcsmorandi.com	Carthage R-9 School District
CED Group	Summit College	Premium Transportation Group
NanoFocus	Visit Montréal	PAUL BEUSCHER PUBLICATIONS
KCA Deutag	plainviewmn.com	Rafael Advanced Defense Systems
justice.fr	Shutterfly inc.	ASL Napoli 3 Sud Network Seized
heubeck.de	Polen Implement	Butler County Community College
laponte.it	Info-Excavation	The Grand Bahama Port Authority
vbhlaw.com	thalesgroup.com	Union County Utilities Authority
isnardi.it	grupomakler.com	Caribbean Broadcasting Corporation
AFG Canada	Florida lawyer ‘s	Western Information Management Inc
D.F. Chase	Airspan Networks	Durham Cathedral Schools Foundation
Strongwell	kentkonut.com.tr	UTC Uniformes Town & Country Inc, Les
U.FORM SRL	crossroadshealth	Centre D’Odontologia Integrada Miret-Puig
atsair.com	torann-france.fr	NASS USA North American Substation Services

表格 2.受害组织/企业

系统安全防护数据分析

通过将 2022 年 1 月与 2021 年 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。

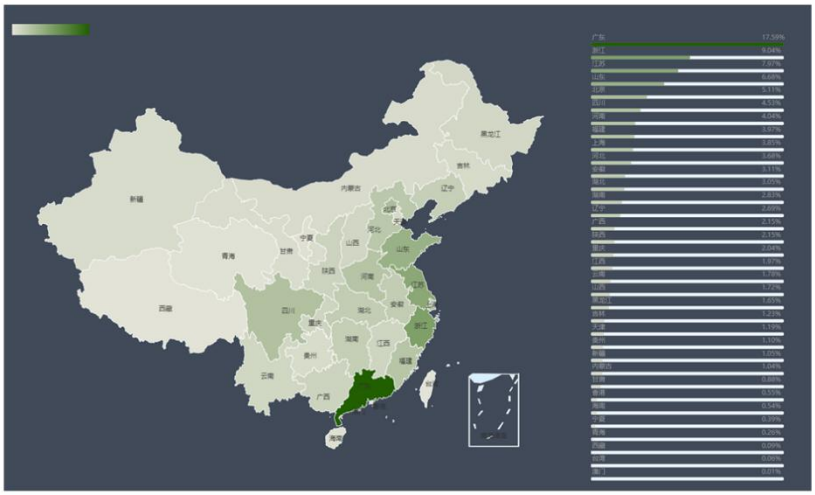
2022年1月弱口令攻击系统占比



数据来源：360反勒索服务

以下是对 2022 年 1 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。

2022年1月全国被弱口令攻击分布图



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。

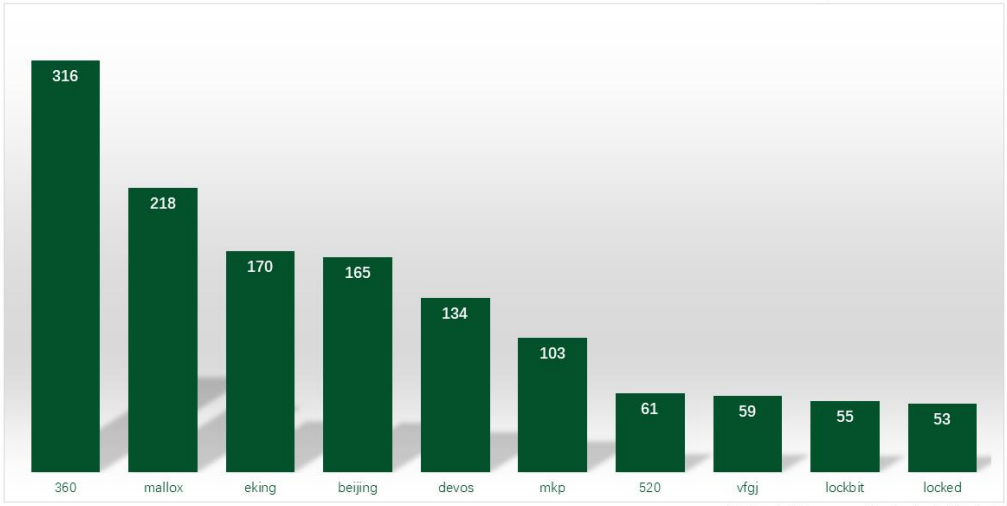
数据来源：360系统安全防护

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。

- 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。
- 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。此外 360 安全大脑监控到该家族本月还通过匿影僵尸网络进行传播。
- 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。
- beijing：同 360 。
- 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。
- mkp：属于 Mako 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。
- 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。
- vfgj:属于 Stop 勒索病毒家族，由于被加密文件后缀会被修改为 vfgj 而成为关键词。该家族的主要传播方式为:通过伪装成破解软件或者激活工具诱导用户下载运行进行传播。
- 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。
- Locked:locked 曾被多个家族使用，但在本月使用该后缀的家族是 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。

2022年1月360勒索病毒搜索引擎关键词检索量Top10



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。

2022年1月解密大师解密量

数据来源：反勒索服务统计数据