2022 年 2 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反勒索服务。

2022 年 2 月，全球新增的活跃勒索病毒家族有:Sutur、D3adCrypt、Sojusz、Unlock、IIMxT 等家族。本月最值得关注的有三个热点：

一、Coffee 勒索病毒先后采用蠕虫和钓鱼邮件的传播方式对高校及科研院所发起针对性攻击。

二、勒索病毒的假旗攻击在俄乌战争中发挥重要作用，乌克兰连番遭遇多轮“擦除器”攻击，多个政府网站受到影响。

三、俄乌战争爆发后，Conti 勒索团伙，疑似内部分裂，大量内部数据被公开发布。

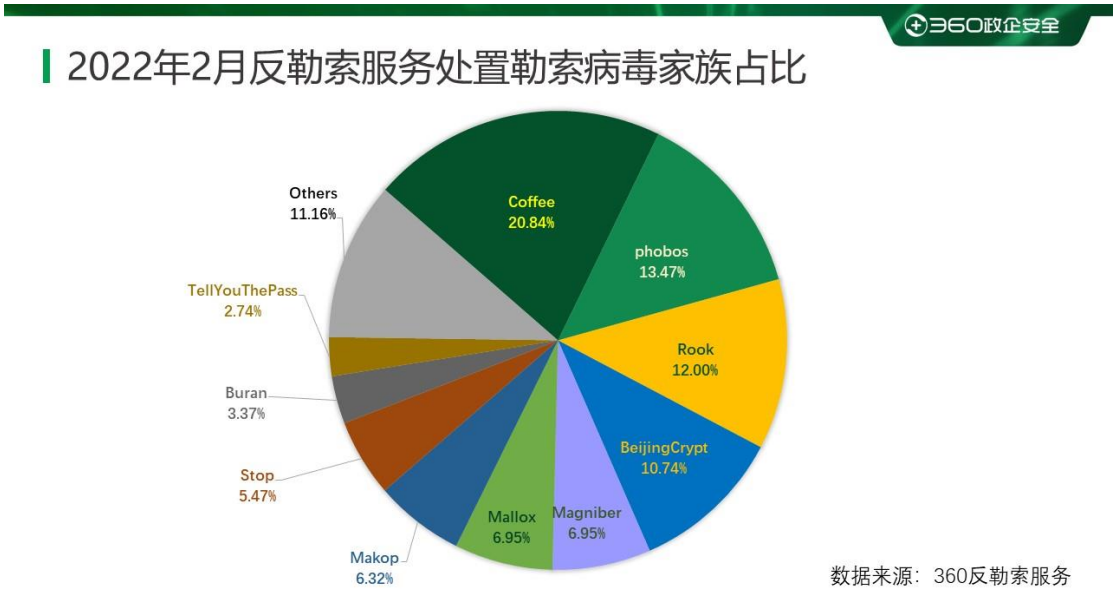
四、国内多家企业遭 BlackCat 攻击，存在数据泄露风险

感染数据分析

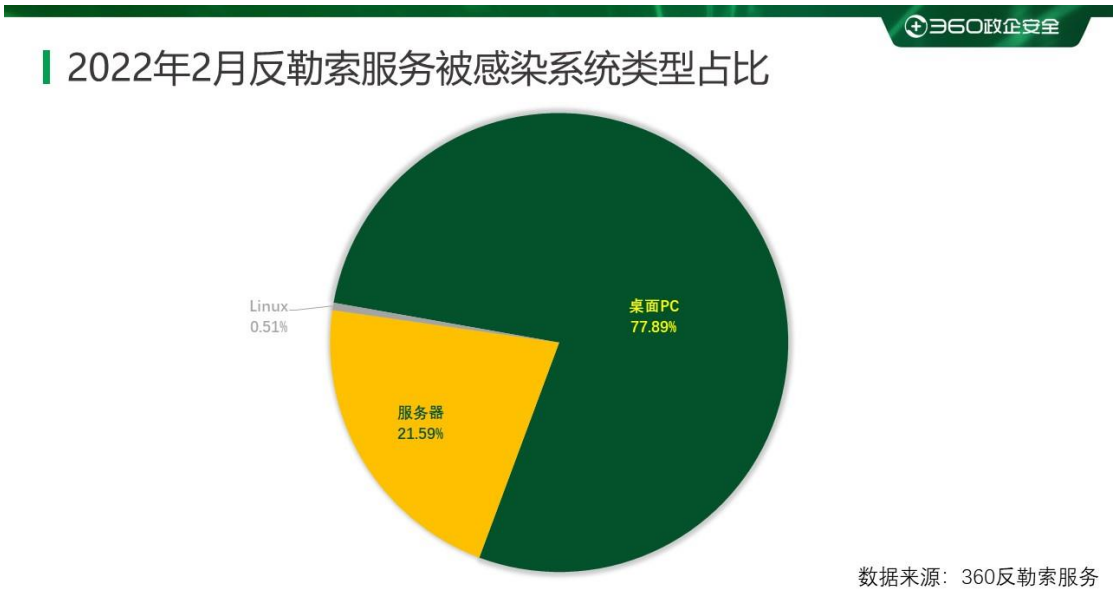
针对本月勒索病毒受害者所中勒索病毒家族进行统计,Coffee 家族占比 20.84%居首位，其次是占比 13.47%的 phobos，Rook 家族以 12.00%位居第三。

根据 360 安全大脑监控到的数据显示：

- 通过 QQ 蠕虫以及钓鱼邮件进行传播的 Coffee 在本月集中发作，导致感染 Coffee 家族的受害者数量上涨。
- 本月大量 Rook 勒索病毒受害者，因下载了带有恶意代码的 AutoCAD 注册机导致中招。该注册机会先通过在 powershell 的计划任务实现长期驻留，之后不断投递勒索病毒。同时该传播渠道也与匿影僵尸网络紧密相关。
- Mallox 在本月新增多个变种，包括 avasr、consultransom、DevicZz,其传播方式多样化，主要攻击目标为中大型企业，在拿下企业入口终端后，利用横向渗透的方式攻击企业内网其他设备。



2022 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

乌克兰连番遭遇多轮“擦除器”攻击

俄乌战争爆发后，出现了多轮针对乌克兰以破坏为目的的国家级网络战攻击，攻击活动包括分布式拒绝服务（DDoS）攻击、钓鱼欺诈、漏洞利用、供应链攻击、伪装成勒索软件的恶意数据擦除攻击等。经分析，这些网络攻击可能旨在造成乌克兰的混乱、阻碍通信、削弱乌克兰的政府、民间和军事机构，是一场策划已久的网络战。而 2 月底，更是出现了多轮针

对乌克兰的数据擦除恶意软件大规模传播事件。

第一轮攻击由 WhisperGate 数据擦除器发起，该软件在 1 月就已经出现，而随着俄乌战争的进行，其传播量力度和感染规模也随之大量增加。该病毒会先覆盖 MBR 并销毁所有分区，再通过 Discord 服务托管的 CDN 下载攻击载荷，最终执行文件擦除攻击。

而在 WhisperGate 获得成功后，同为“擦除器”的 HermeticWiper 及 IsaacWiper 则紧随其后，分别发动了第二、三轮擦除器攻击。这些攻击中，部分是由计划任务启动的，疑似通过控制内网域控和不同网络服务的漏洞利用进行投递植入。

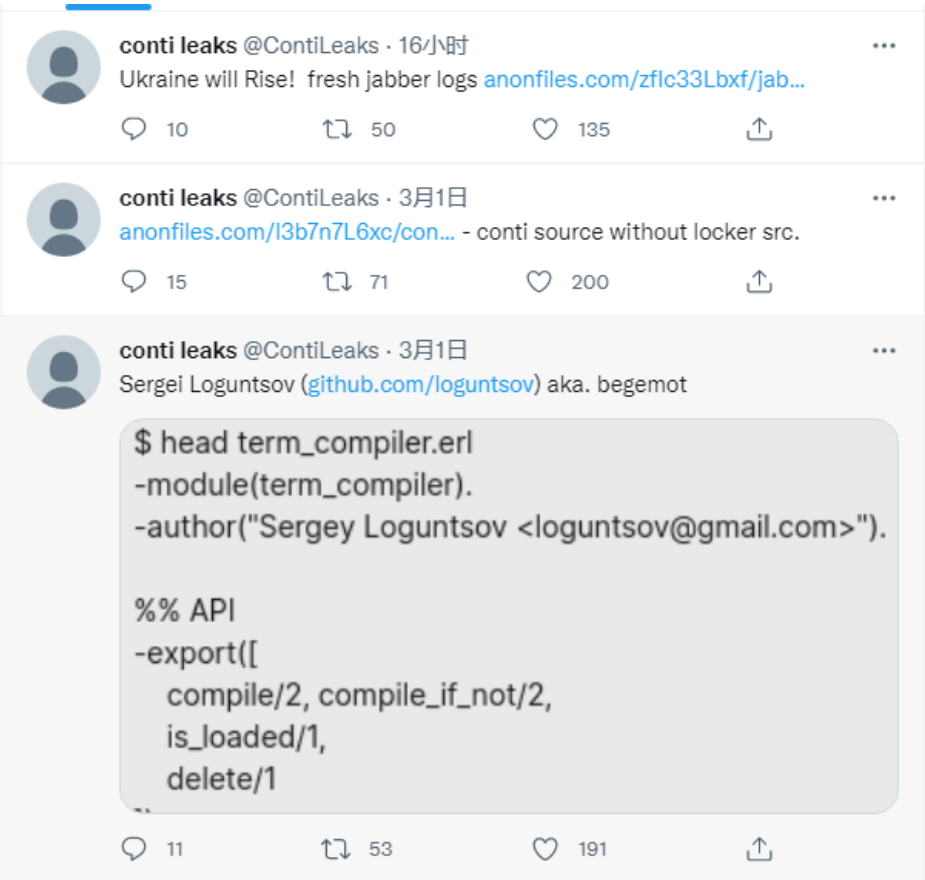
根据 360 高级威胁研究院的分析推演，在网络战中所实施的大规模破坏攻击行动，极有可能因为不受攻击者控制的情况而波及全球，相关组织机构需要提高警惕。

Conti 内部分裂，大量内部数据被公开发布

俄乌战争爆发后，Conti 勒索团伙因支持国家不同，引发内部分裂。一名 Conti 组织的内部成员（也有消息称是一名乌克兰安全研究员）将 Conti 组织的内部对话以及勒索病毒软件、控制面板等源代码等信息公开发布出来。

2 月底，有人以@ContiLeaks 的账号名义泄露了 393 份 JSON 文件，其中包括 Conti 和 Ryuk 勒索病毒组织的私人聊天记录。本三月初，此人进一步发布而更多数据——这次共有 148 各 JSON 文件，其中包括 107000 余条内部消息。

随后，这位名为@ContiLeaks 的账号继续发布了更多的消息，包括 Conti 的管理面板源码、BazarBackdoor API、数据服务器的截屏等。其中最重要的是一个包含了 Conti 勒索病毒加密器、解密器、构造器源码的存档。但该存档收到密码保护，目前尚没有被破解。



随着俄乌冲突持续，不少网络安全相关组织和勒索病毒团伙开始表明立场，例如：

- Lockbit 家族表示，该团伙成员来自多个国家，包括俄罗斯人也包括乌克兰人，他们不会卷入任何国际冲突，只专心进行勒索。
- Stormous 勒索病毒团伙正式宣布支持俄罗斯政府。
- 出现勒索病毒对乌克兰进行数据擦除攻击。
- 知名黑客论坛 Raidforums 则发出通知：禁止任何来自俄罗斯的访问。该论坛的一名成员甚至对“俄罗斯人”发出了警告，声称掌握了包含有俄罗斯联邦安全局的电子邮件及散列密码的数据库。
- 安全厂商 Emsisoft 也在 twitter 中公开表示站在乌克兰一方。

Coffee 潜伏期高达百日

本月，360 安全大脑监控到国产勒索病毒 Coffee 针对高校教师和科研人员发起勒索攻击，其中最早一次攻击通过软件捆绑和 QQ 群钓鱼传播且危害极大，不仅具备蠕虫性质，且潜伏期还高达数百日。

该病毒的第二轮攻击选择伪装成学校邮箱(jcc@eudumail.cloud)向各高校老师发送名为《2021 年度本单位职工个税补缴名单》的钓鱼邮件，通过对受害者分析发现受害者主要来自今年和去年申请《国家自然科学基金》项目的高校教师与科研院人员。

关于2021年度绩效结算个人所得税税收优化的情况通报（02181032）

发件人 "计财处" <jcc@edumail.cloud>

日 期 2022年02月18日 星期五 10:43

收件人 "zryan" <zryan@swpu.edu.cn>

附 件 1个（2021年度本单位职工个税补缴名单.rar）

关于2021年度绩效结算个人所得税税收优化的情况通报各单位：

根据《关于延续实施全年一次性奖金等个人所得税优惠政策的公告》（财政部税务总局2021年第42号公告），全年一次性奖金单独计税优惠政策，执行期限延长至2023年12月31日。

为确保广大职工充分享受该项税收优惠政策，2021年底计财处对每一名职工的全年工薪收入和各类扣除情况进行了分析测算，按政策将大部分职工年底发放的部分绩效结算金额按全年一次性奖金优化计税。优化后，有78.2%的职工可节约税金。在2022年2月底申报期完成全年一次性奖金纳税申报后，计财处会按程序将节约的税金发至职工银行卡上。

需要说明：经过对职工全年应缴税额和已扣税额对比，有部分职工需要补税（名单见附件），补税的金额将在后续发放的绩效中扣除。产生补税的原因主要是部分职工在2021年12月通过个人所得税APP修改了专项附加扣除，由于操作不当，导致全年专项附加扣除额度减少，从而应缴税额增加。建议这部分职工在使用个人所得税年度APP进行汇算清缴时，将专项附加扣除修改正确，可申请退回这部分税金。

计财处

2022年2月18日

虽然 Coffee 病毒有愈演愈烈的趋势，不过可喜的是 360 解密大师已经在第一时间支持了该勒索病毒解密。受到 Coffee 勒索病毒影响的用户，可尝试使用 360 解密大师解密或联系 360 安全中心寻求帮助。

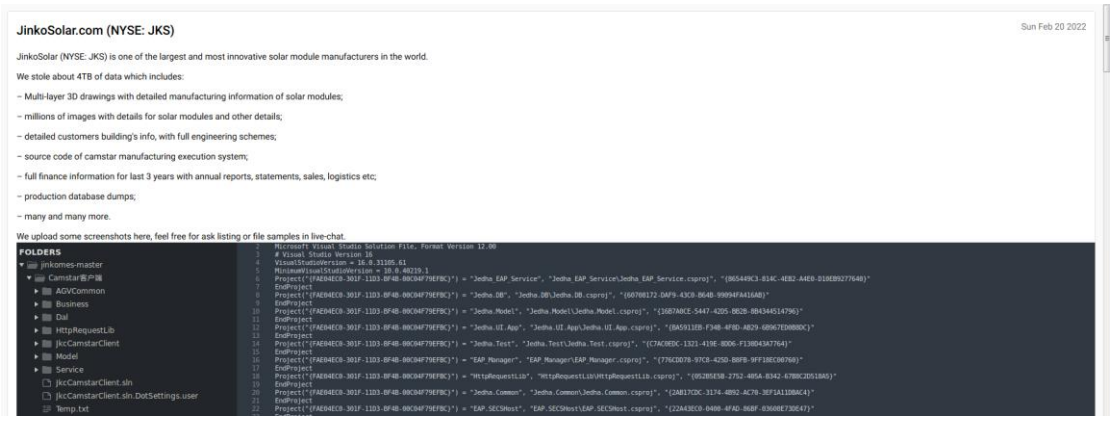
瞄准中大型企业的 Blackcat 勒索病毒

BlackCat 勒索病毒家族最早出现于 2021 年 11 月，又被称作 ALPHV 勒索病毒家族，采用 RaaS（勒索软件即服务）模式运营，其目标为中大型企业。该家族还在暗网论坛宣传：附属机构勒索到的赎金，附属机构自身可分得 80%~90%。这比之前任何一个勒索组织提供的分成都要高，从而得到大量攻击者的吹捧，迅速融入勒索市场。在成功部署勒索病毒后，向受害者索要价值 40 万至 2 千万美元不等的比特币或门罗币作为赎金。

该勒索病毒能迅速融入勒索病毒市场，还因为其存在以下多个特征：

- 高定制性:攻击者可根据自己的喜好进行定制,包括受害者公钥、被加密文件后缀、勒索提示信息文件名、每个文件加密大小、加密算法选择等。
- 高危害性：不仅会加密受害者文件，还会窃取数据、对未支付赎金受害企业/组织的基础设施采取分布式拒绝服务(DDOS)攻击、羞辱受害者等。
- 多平台性：该勒索病毒采用 Rust 语言编写，加密文件快，可在 Windwos 和 Linux 等主流平台运行。
- 攻击方式多样性：不仅收集被攻击企业/组织的登录凭据(远程桌面 RDP 的登录凭据、VPN 的登录凭据等)，还利用不同漏洞进行攻击。
- 私密性高：访问其谈判页面需要提供受害企业/组织对应的 token,否则无妨访问。避免被非受害者人员访问，接受无效沟通或恶意谈判。

目前该家族数据泄露网站已有 52 个受害者名单，其中有 5 个来自中国。其中包含本月被攻击的某新能源企业。攻击者宣称在此次攻击事件中，窃取了多达 4TB 的数据，包括太阳能组件详细制造信息 3D 图纸、数百万太阳能模块图像、客户建筑信息、制造执行系统源码、过去 3 年完整财务信息等，并公布了相应信息。



疑似遭泄露的部分数据

Puma 再次因勒索病毒攻击面临数据泄露

运动服装制造商 Puma 最早在 2021 年 8 月曾被 Marketo 攻击，被窃取包括其应用程序源码在内的 1GB 数据。在 2021 年 12 月，其北美人力管理服务提供商之一的 Kronos 被勒索病毒攻击后，Puma 相关数据再次遭到了泄露。

本月早些时候，Kronos 在向几家司法部长办公室提交的数据泄露通知称，攻击者在加密数据之前，从 Kronos 私有云(KPC)云环境中窃取了属于 Puma 员工及其家属的个人信息。Kronos 将 KPC 描述为使用防火墙、多因身份验证和加密传输保护免受攻击的安全存储。它

用作托管 Workforce Central、Workforce TeleStaff、Enterprise Archive、TeleTime IP、医疗保健扩展(EHC)和 FMSI 环境的服务器设施。

虽然通知中并没有提到有多少 Puma 员工的信息在攻击期间被盗，但提供给缅因州总检察长办公室的信息显示，勒索病毒运营者可能已经掌握了 6632 份个人相关数据。

黑客信息披露

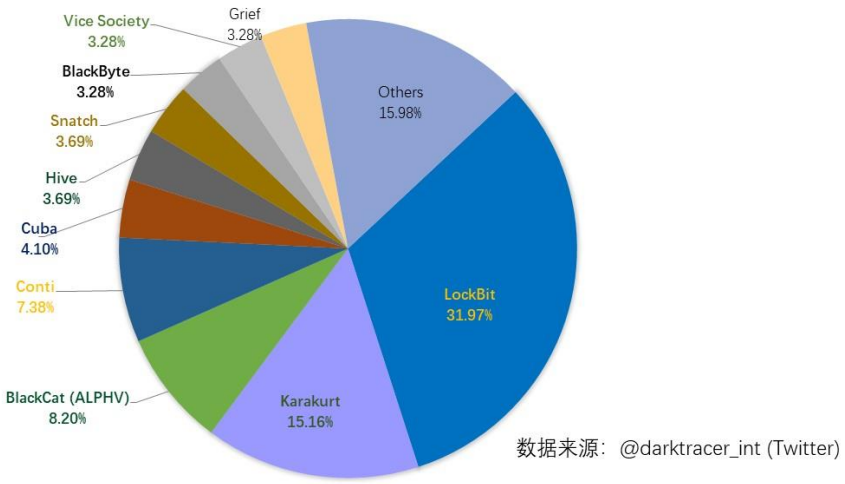
以下是本月收集到的黑客邮箱信息：

writeme@onionmail.org	Wingate@onionmail.org	aLPoint@privatemail.com
raincry@dr.com	restaurera@safeswiss.com	Harman@privatemail.com
back23@vpn.tg	decryptor@cock.lu	Cybell@firemail.cc
xena@airmail.cc	ustedesfil@cock.li	hyperme@tuta.io
robud@ctemplar.com	votredatei@ctemplar.com	suppmkp@msgsafe.io
robud@outlookpro.net	indyan@airmail.cc	suppmkp@tutanota.com
dec0ding@tutanota.com	Kardon@privatemail.com	JohnWilliams1887@gmx.com
decrypt@onionmail.org	Rheinland01@privatemail.com	newexploit@tutanota.com
ljubisupporte@protonmail.com	equalitytrust@disroot.org	ariakei@protonmail.com
LilliBTC@tuta.io	unlocker@onionmail.org	bambam988@tuta.io
mrcrypt2@mailfence.com	unlockersuport@msgsafe.io	china_decr2021@xmpp.jp
mrcrypt@msgsafe.io	kardon@privatemail.com	asistchinadecryption2022@goat.si
ithelp02@decorous.cyou	360recover@mailfence.com	fastwindGlobe@mail.ee
ithelp02@wholeness.business	webweb321@fiermail.cc	restauera@safeswiss.com
wilhelmkox@tutanota.com	kongbang@privatemail.com	unblocker@tuta.io
koxic@protonmail.com	henrystanley1861@gmx.com	bryan1984jackson@pressmail.ch
koxic@cock.li	Bomani@Email.CoM	24recovery@onionmail.org
helpcenter2008@gmail.com	restaurera@runbox.com	Dec_youfile1986@mailfence.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）。

2022年2月通过数据泄露获利的勒索病毒家族占比



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 244 个组织/企业遭遇勒索攻击。

RRD	NZ UNIFORMS	Maple Lodge Farms
XAL	Acorn Media	Northern Contours
Cle	Team Realty	Thomson Broadbent
Edgo	Mediagistic	Bank of Indonesia
DURA	Royal Laser	harrisshelton.com
EDSI	udmercy.edu	centralbankfl.com
Acorn	paybito.com	Mecanico Cairo SL
STIMM	Gardenworks	Heartland Alliance
Subex	bayview.com	Slepoy Corporation
Sanden	Fdcbuilding	COFRAP ESPAÑOLA SA
izo.es	snapmga.com	mitchellmcnutt.com
PLACON	bricofer.it	onlinesalespro.com
HAPOLO	chemtech.net	Hall Cross Academy
Arcese	aludesign.ro	JALEEL TRADERS LLC
Cmmcpas	siamdial.com	fairnessforall.com
joda.de	supersave.ca	Perennials Fabrics
ipec.ro	bernheim.org	Imperial Logistics
RIVADIS	Abdi ibrahim	lee-associates.com
UNICRED	cbibanks.com	The Scion Group LLC
Moncler	NORDFISH SRL	castro-urdiales.net
CSEG.CN	Little Giant	universalwindow.com
48Forty	rightsys.com	huntsville4rent.com
Arc Com	jockeyclub.org.ar	salesiancollege.com
Sectrio	bishopeye.com	kainz-haustechnik.at

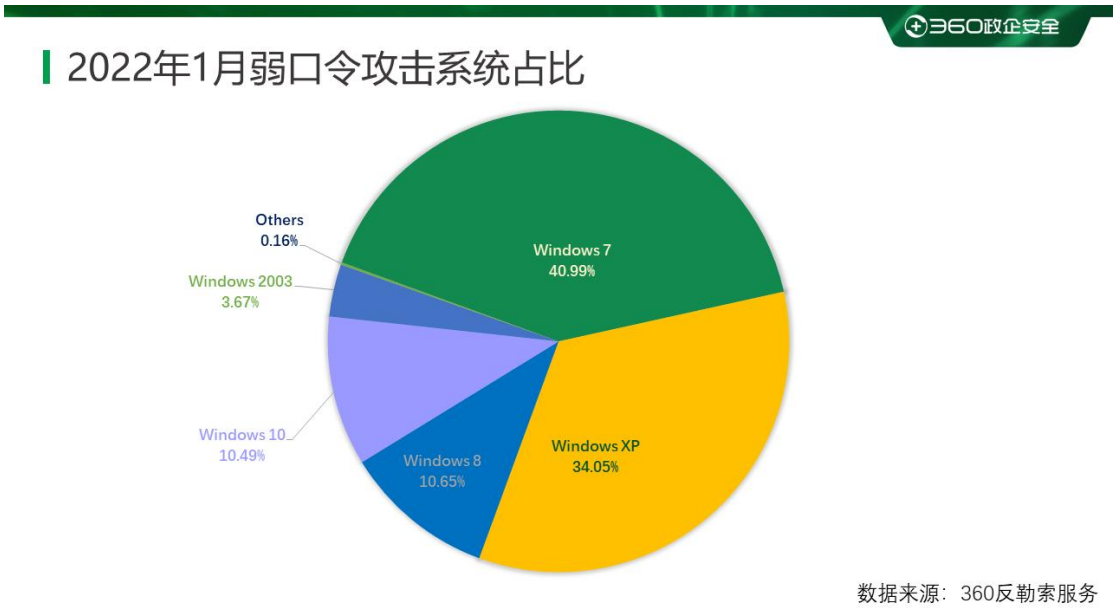
RedGuard	Valle del Sol	ametisfacilities.com
Forterra	tntorello.com	fivestarproducts.com
AMT Corp	sapulpaps.com	themisautomation.com
Optionis	hk-callcentre	Converse Pharma Group
estpm.fr	Argonaut Gold	hancockassociates.com
Mtlcraft	progereal.com	Vehicle Service Group
Redbadge	Shoesforcrews	Lyon-Waugh Auto Group
Hensoldt	SVA Jean Rozé	Lewis & Clark College
Regulvar	elitemate.com	northsideplumbing.com
Aeronamic	elmonterv.com	securiteassurance.com
KP SNACKS	saintcloud.fr	Rector Hayden Realtors
Oliff PLC	ambau-team.de	Eka Software Solutions
HighRoads	optimissa.com	Busch Vacuum Solutions
nfcaa.org	mfkmakina.com	Overseas Travel Agency
Emil Frey	Acuity Brands	Bob`s Carpet & Flooring
Mab Group	Hanon Systems	girlguidinglaser.org.uk
efile.com	amerplumb.com	independentprinting.com
Safeguard	Amaveca Salud	tyresolesdobrasil.com.br
Superfund	FrenchGourmet	A A Zamarro & Associates
TaxNetUSA	Weldco Beales	Westmount Charter School
Delinebox	empireins.com	Butler Community College
Ezz Steel	skandia.com.mx	CIG de la Grande Couronne
Huhtamaki	ARL Bio Pharma	SAVANNAH State University
aquila.ch	CoreNet Global	Bud Griffin and Associates
BainUltra	prefimetal.com	TVS Supply Chain Solutions
CED Group	Claro Colombia	The City of Pembroke Pines
NanoFocus	bannerbuzz.com	東京コンピュータサービス
SEA-invest	Brookson Group	Cree Nation of Waskaganish
dap.gov.tr	khattarlaw.com	Athens Distributing Company
Petrolimex	Detroit Stoker	Eastern Western Motor Group
Huvepharma	mcsmorandi.com	lhotellerie-restauration.fr
Spirit ORD	Summit College	Venture Machine & Tool, Inc.
Assura PLC	Visit Montréal	Altoona Area School District
Division D	Jazeera Airways	PAUL BEUSCHER PUBLICATIONS
bar2.co.uk	hotelcedres.com	Creative Liquid Coatings INC
ukrl.co.uk	botafogo.ind.br	Carthage R-9 School District
dectro.com	mainland.com.hk	Premium Transportation Group
savonia.fi	paramountme.com	Albany Bank and Trust Company
CGT S.p.A.	plainviewmn.com	The Public Safety Credit Union
Keuerleber	Shutterfly inc.	Greenwood Metropolitan District
ibasis.com	Polen Implement	MSH Steuerberatungsgesellschaft
ibasis.net	Info-Excavation	Rafael Advanced Defense Systems
KCA Deutag	thalesgroup.com	ASL Napoli 3 Sud Network Seized

justice.fr	grupomakler.com	Butler County Community College
heubeck.de	The Lovett Group	The Grand Bahama Port Authority
laponte.it	Zamil Industrial	Union County Utilities Authority
vbhlaw.com	hammer-poznan.pl	Consumers Supply Distributing LLC
isnardi.it	Florida lawyer’s	WinningLife International Limited
AFG Canada	Airspan Networks	JAX Spine and Pain Medical Centers
D.F. Chase	kentkonut.com.tr	Prince Jewellery & Watch Co., Ltd.
Strongwell	crossroadshealth	Caribbean Broadcasting Corporation
U.FORM SRL	torann-france.fr	Western Information Management Inc
atsair.com	chervongroup.com	Durham Cathedral Schools Foundation
Division-D	Atlantic Asphalt	UTC Uniformes Town & Country Inc, Les
AKIJ GROUP	aulss6.veneto.it	Rodonaves Transportes E Encomendas Ltda
Iwis Group	Taylor and Martin	Centre D’Odontologia Integrada Miret-Puig
www.paw.eu	ci.hercules.ca.us	NASS USA North American Substation Services
bayer.co.at		

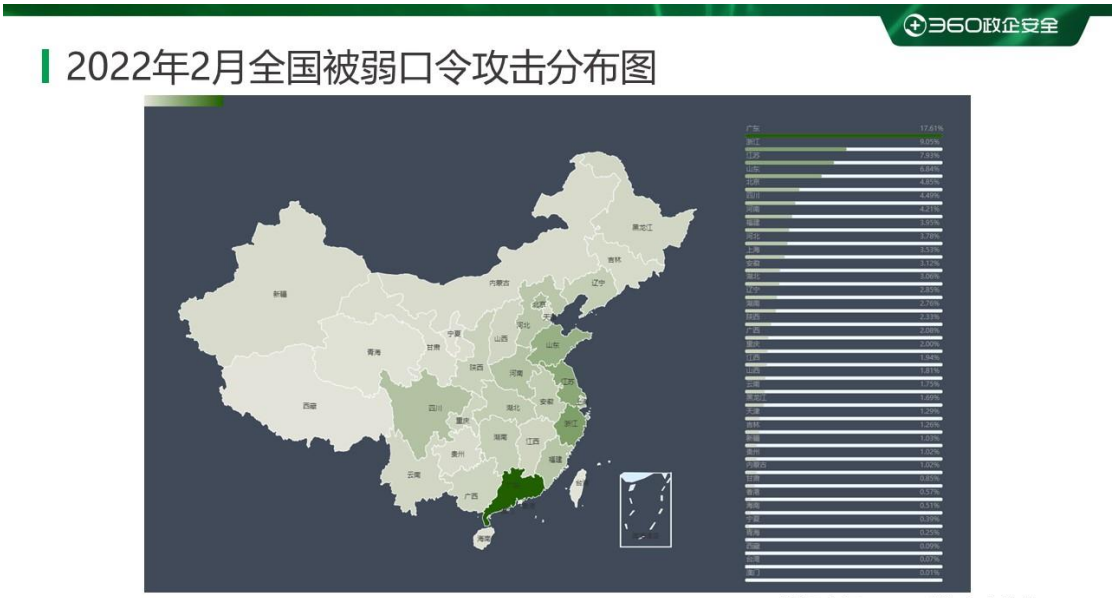
表格 2.受害组织/企业

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。



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。



数据来源：360系统安全防护

通过观察 2022 年 2 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。
- coffee：属于 Coffee 勒索病毒家族，由于被加密文件后缀带有 coffee 而成为关键词。该家族主要传播方式有两种，第一种为通过伪装成具有诱惑性的钓鱼邮件，第二种为蠕虫。

- 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。
- rook:属于 Rook 勒索病毒家族，由于被加密文件后缀会被修改为 rook 而成为关键词。该家族的主要传播方式为：通过匿隐僵尸网络进行传播。本月(2022 年 2 月)受害者大部分是因为到下载网站下载注册机感染的匿隐僵尸网络。
- 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。
- 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。
- rook3:同 rook。
- 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。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。
- 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。
- avast：同 mallox。

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 Coffee，其次是 Sodinokibi。使用解密大师解密文件的用户数量最高的是被 Coffee 家族加密的设备，其次是被 Stop 家族加密的设备。

2022年2月解密大师解密量

数据来源：反勒索服务统计数据