2021 年 11 月勒索病毒态势分析

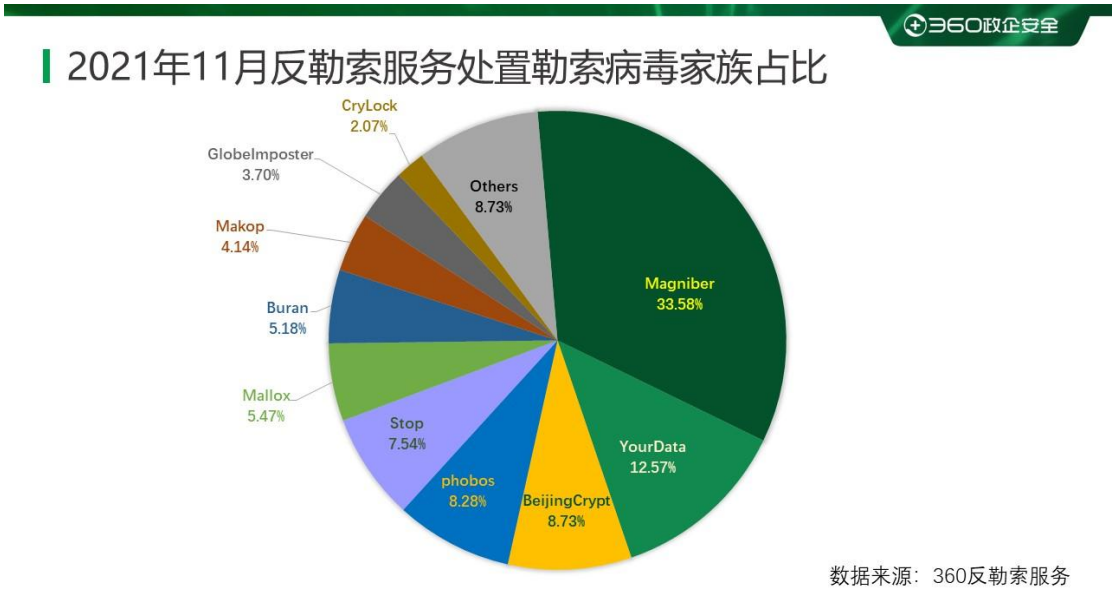
勒索病毒传播至今，360 反勒索服务已累计接收到上万勒索病毒感染求助。随着新型勒索病毒的快速蔓延，企业数据泄露风险不断上升，勒索金额在数百万到近亿美元的勒索案件不断出现。勒索病毒给企业和个人带来的影响范围越来越广，危害性也越来越大。360 安全大脑针对勒索病毒进行了全方位的监控与防御，为需要帮助的用户提供 360 反勒索服务。

2021 年 11 月，全球新增的活跃勒索病毒家族有:Doyuk2、HarpoonLocker、Rozbeh、BlackCocaine、CrytOy、Flowey、54BB47H (Sabbath)、Entropy、ROOK、RobinHood、AvGhost 等勒索病毒家族，其中 54BB47H (Sabbath)、Entropy、ROOK、RobinHood 四个家族为本月新增的双重勒索病毒家族；本月最值得关注的勒索病毒 Magniber，该勒索病毒家族通过网页挂马疯狂传播；老牌勒索家族 Snatch 也开始采用双重勒索模式运营;AvGhost 勒索软件针对服务器进行攻击，虽然受害者联系到黑客后，黑客表示此次攻击只是测试并承诺替用户免费解密文件，但实际结果是受害者仍有大量数据无法恢复。

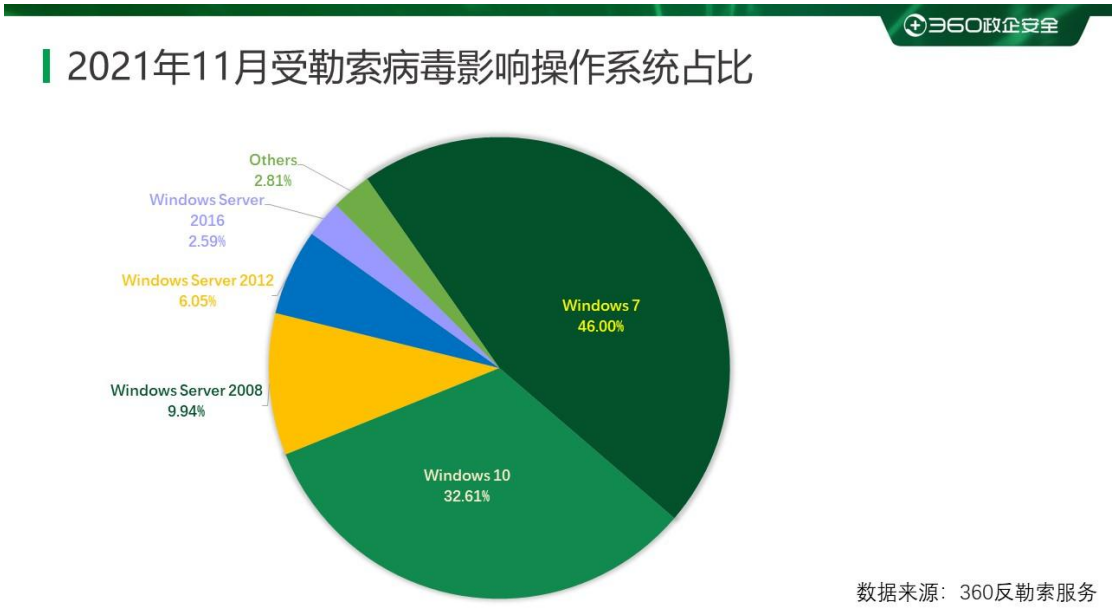
感染数据分析

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 33.58%居首位，其次是占比 12.57%的 YourData，BeijingCrypt 家族以 8.73%位居第三。

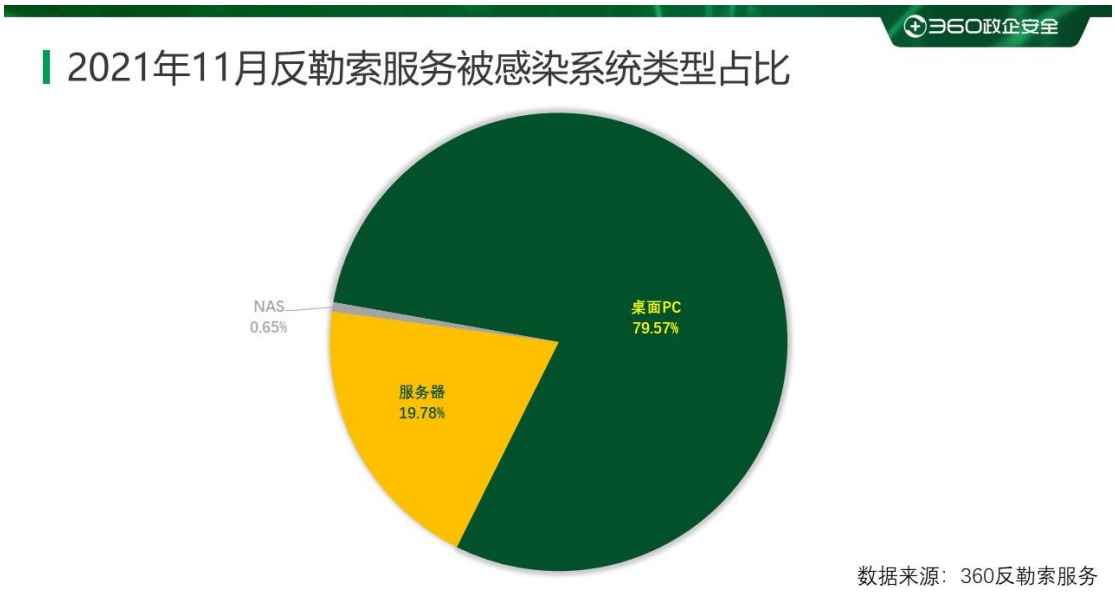
刚做到国内第一的 YourData 勒索病毒仅仅一个月就被 Magniber 取代，究其原因并非是 YourData 传播减弱，而是从 11 月初开始，Magniber 的传播者利用 CVE-2021-40444 漏洞，在网页广告中插入相关利用代码进行传播，在国内的感染量快速提升。



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 11 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。本月被感染的桌面 PC 与 10 月相比占比上涨超过 18 个百分点。这主要因为被 Magniber 勒索病毒攻击的受害者大部分使用的是桌面 PC。

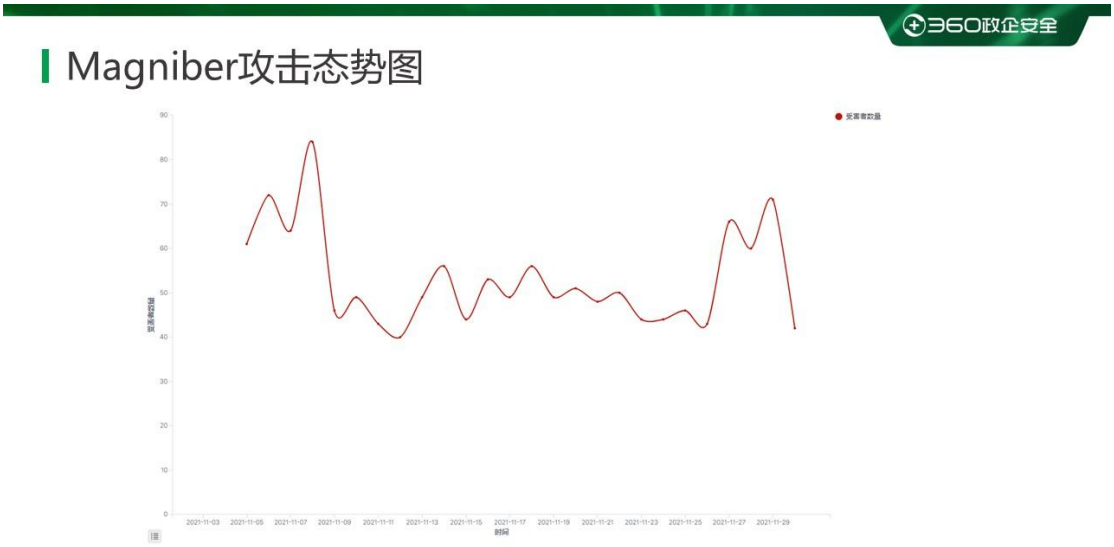


勒索病毒疫情分析

Magniber 勒索软件升级，瞄准国内用户

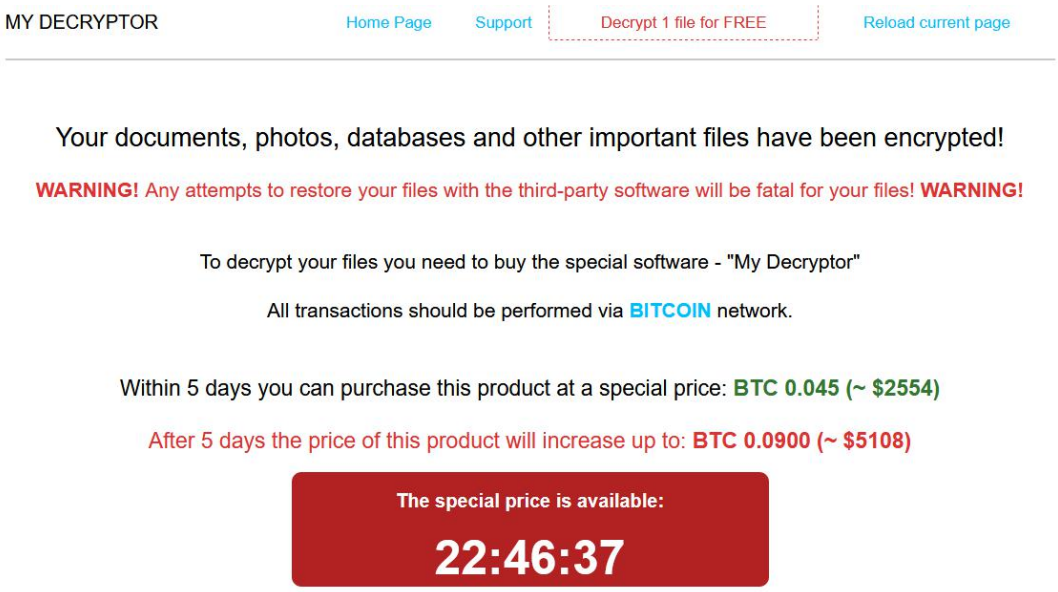
11 月 5 日开始，360 安全大脑检测到 CVE-2021-40444 漏洞攻击拦截量有较明显上涨。经过 360 政企集团高级威胁研究分析中心分析追踪发现，这是一起挂马攻击团伙，利用 CVE-2021-40444 大肆传播勒索病毒的攻击事件，同时病毒在攻击过程中，还使用了 PrintNightmare 漏洞进行提权。该黑客团伙主要通过在色情网站、游戏网站（也存在少部分其它网站）的广告位上，投放植入带有攻击代码的广告，当用户访问到该广告页面时，就

有可能中招，感染勒索病毒。截止当前 360 安全卫士仍能拦截到约 500 次每小时的挂马广告页面访问。而漏洞拦截量，最高单日也已超过 1000 次。



数据来源：360安全大脑

Magniber 勒索软件是基于 Magnitude exploit kit（Magnitude EK）开发套件进行开发，早期还曾传播过 Locky、Cerber 勒索病毒家族。被该勒索加密后，文件后缀将被修改为随机字符串，受害者需向攻击者支付 0.044~0.048 个比特(价格一直在波动,5 天内若未支付，赎金将会翻倍)。



Conti 勒索病毒团伙策划让 Emotet 僵尸网络卷土重来

根据情报公司 Advanced Intelligence 的消息，知名僵尸网络程序 Emotet 将被“复活”。而说服此次复活行动的正式 Conti 勒索病毒团伙的成员。

Emotet 僵尸网络曾于约 10 个月前被关闭，而此次“复活”则会重新对分布官方的受控端开启控制。使其充当恶意软件加载程序，为其他恶意软件提供有价值的受感染系统访问权限。而 Qbot 和 TrickBot 则是 Emotet 僵尸网络的主要客户，这两款软件又会利用获取到的

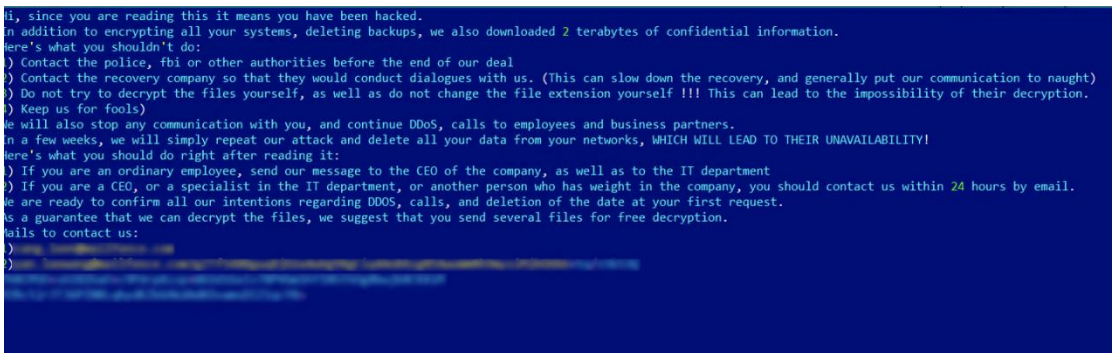
访问权限部署包括 Conti 在内的诸多勒索软件。

在被曝出 Conti 策划重启 Emotet 僵尸网络前，该勒索团伙的支付站点和对应域名则均因被劫持导致关闭，但其数据泄露站点页面及域名仍可以正常工作。

“阎罗王”勒索软件正驶入攻击美国金融部门

近日“阎罗王”勒索病毒的下属机构正在尝试使用 BazarLoader 恶意软件攻击美国金融部门。自从 8 月份以来，“阎罗王”勒索病毒不仅对金融机构发起攻击，还对制造业、IT 服务、咨询及工程领域的公司进行攻击。

该攻击团伙在入侵阶段不仅部署了恶意软件，还尝试从受控设备上收集浏览器保存的登录凭证，例如：Firefox、Chrome、Internet Explorer，以及窃取 KeePass 密码管理器的主密钥等。受害者若不能在规定时间内联系黑客并支付赎金，黑客将对受害者采取 DDOS 攻击以及致电其员工和业务合作伙伴，若几周内仍未支付，黑客将删除其数据。



黑客信息披露

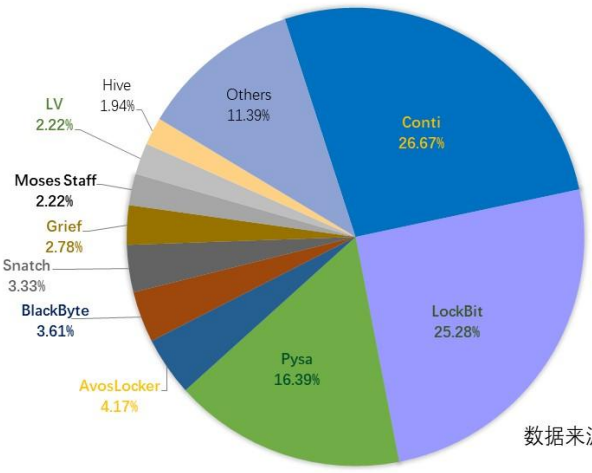
以下是本月收集到的黑客邮箱信息：

Merlen@Dr.Com	ransomware10@yahoo.com	dwaynehogan33@onionmail.org
sazepa@tuta.io	zeppelin_helper@tuta.io	AllenPool1987@onionmail.org
jericoni@pm.me	dr.helper@onionmail.org	Vasco_Alonso@protonmail.com
g.uan_yu@aol.com	mr.helper@onionmail.org	AndryCooper1988@tutanota.com
mak_supp@aol.com	alabacoman@tutanota.com	Mikedillov1986@onionmail.org
Merlen@Keemail.Me	ideapad@privatemail.com	helpdecryptmyfiles@yandex.com
psworm@keemail.me	uSuppor@privatemail.com	jackiesmith176@protonmail.com
zsebas@arimail.cc	zeppelin_decrypt@xmpp.jp	JerseySmith1986@onionmail.org
obamausa7@aol.com	datarecover@ctemplar.com	leonardred1989@protonmail.com
nexyum@zohomail.eu	pecunia0318@tutanota.com	JeremySaylor1987@tutanota.com
kameric@airmail.cc	EndryuRidus@tutanota.com	Rick_Astley_Helper@outlook.com
baseus0906@goat.si	admin@crypteyourdata.com	fionahammers1995@onionmail.org
ransomnow@yandex.ru	chickenwing@onionmail.org	MarkHuntigton1977@tutanota.com
pecunia0318@goat.si	yourfriendz@techmail.info	CharlesSLewis1987@onionmail.org
friend.dec@yandex.ru	Pringls_us@protonmail.com	DavidSchmidt1977@protonmail.com
cnlock@danwin1210.me	cheet0s_de@protonmail.com	JamesHoopkins1988@onionmail.org
pol.aris@tutanota.com	datarecovery@ctemplar.com	ollivergreen1977@protonmail.com
520hard@mailfence.com	jasonchow30@onionmail.org	jeffreyclinton1977@onionmail.org
seawolf@onionmail.org	Kirklord1967@tutanota.com	alberttconner2021@protonmail.com
coronaviryz@gmail.com	VinceGilbert@tutanota.com	DorothyFBrennan1992@tutanota.com
friend.dec@keemail.me	Vasco_Alonso@tutanota.com	noreywaterson1988@protonmail.com
koreadec@tutanota.com	korona@bestkoronavirus.com	rickysmithson1975@protonmail.com
helpservisee@elude.in	parpsrecovery@criptext.com	DerekWillson19878@protonmail.com
RansHelp@tutanota.com	yourrealdecrypt@airmail.cc	steven1973parker@libertymail.net
pol.aris@opentrash.com	Leslydown1988@tutanota.com	richardbrunson1892@protonmail.com
Merlens@Protonmail.com	vilidariobtc12@tutanota.com	ElizabethAntone1961@protonmail.com
coronavirus@exploit.im	zeppelindecrypt@420blaze.it	leticiaparkinson1983@onionmail.org
decryptdelta@gmail.com	harpoonlocker@onionmail.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）。

2021年11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 360 个组织/企业遭遇勒索攻击，其中中国有 10 个组织/企业在本月遭遇了双重勒索/多重勒索。

EHS	reigroup.com	Antal International
SWL	Glamox Group	Garner Dental Group
iPS	tornel.com.mx	Kent County Council
TTC	totalfire.biz	Symonds And Sampson
ION	cilentospa.it	breslowstarling.com
lkma	eberlesrl.com	betsaisonparagot.fr
V-ON	Vision Source	Bruss North America
Hutt	Lucton School	consortiumlegal.com
Otip	Nordic Pharma	Team Computers Ltd.
DAMM	Eileen Fisher	comune.gonzaga.mn.it
AISD	Renault India	morganskenderian.com
AECOM	INTOO Habitat	arrowheadadvance.com
UEMOA	Alco Plastics	waveridernursery.com
Varney	Police Brazil	ARGOS CONNECT ENERGY
socage	cloudpros.com	Family Dental Health
VERBIO	btc-alpha.com	Pitts Baptist Church
CHRYSO	reiss-beck.de	TestOil Oil Analysis
VISTRA	adhhealth.com	Greymouse VA PTY Ltd
INOXPA	apower.com.sg	Gibbs Wire And Steel
Grupo5	Charlie Hebdo	3D imagery of israel
Ishida	Argentina GOV	duncandisability.com
dlb.it	effectual.com	centerspacehomes.com
NOLATO	callay.com.tr	lawrencegroup.net.au
M3 Inc.	Bochane Groep	ardebolassessors.cat
Lantech	Power Plumbing	Burda Sanitärtechnik

PORTALP	benefitexpress	Align Technology, Inc
XacBank	Landmark Builders	The Harrison Law Firm
Ferrara	groweeisen.com	THE METRO GROUP, INC.
Emi Jay	mcmanislaw.com	Diputación de Segovia
Bayonet	nurihiko.co.jp	Capitol Beauty School
Epstein	Stratford Land	Architectural Systems
DUNMORE	Premier Energy	Purifoy Chevrolet Co.
SIRCHIE	The Xssentials	SNR Shopping PUREGOLD
KISTERS	Jonas Software	Volvo Car Corporation
wpdn.net	home.hktdc.com	VIENNA INSURANCE GROUP
Laurenty	daviscrump.com	autolaundrysystems.com
fandi.fr	City of Witten	W A RASIC CONSTRUCTION
eban.com	Visage Imaging	City of Bridgeport, WV
DALLOYAU	mtradeasia.com	Family Dentist Newbury
Burkhart	telepro.com.mx	Woodchurch High School
Jalasoft	Aspen Avionics	Tangent Communications
MPRL E&P	Besson Seguros	peschl-ultraviolet.com
abiom.nl	dtstechnical.ca	Area Energy & Electric
GC Micro	waclighting.com	lenzcontractorsinc.com
EDAN.COM	plumascounty.us	DUNA AUTO az Autovaros
Match MG	David Engineers	Westvale Primary School
Arbitech	ProActive Works	Las Vegas Cancer Center
gaben.cz	Astera Software	Johnson Memorial Health
DEWEtech	Westmont Helena	Cabinet Remy Le Bonnois
Starline	Connect Housing	The Della Toffola Group
Flagship	barfieldinc.com	The Grupo Daniel Alonso
ARM CHINA	The Glass House	Delta Group Electronics
rttax.com	NLB Corporation	Lakeway Publishers, Inc.
EZ Loader	REV Engineering	Enduro Pipeline Services
La Bodega	vicksburgha.org	Florida Heart Associates
itimCloud	Salinen Austria	Schmincke Künstlerfarben
Skatetown	RocTechnologies	evolvedevelopment.com.au
Unit 8200	promo.parker.com	fluidsealingproducts.com
FTI Group	Regence Footwear	DKS Deutsch Kerrigan LLP
alssi.com	besttaxfiler.com	WELLS FARM DAIRY LIMITED
iveqi.com	Agricorp Company	Supernus Pharmaceuticals
inlad.com	Community Brands	Creative Solutions Group
mpusd.net	Emkay Food Sales	ATA National Title Group
San Carlo	ONTEC Automation	QRS Healthcare Solutions
UABL S.A.	thinkcaspian.com	pacificstarnetwork.com.au
gvalue.com	Moneyfacts Group	trueblueenvironmental.com
bdtaid.com	redsrugby.com.au	Rusty Hardin & Associates
ENESCO.COM	Canada West Land	The Skinners Kent Academy

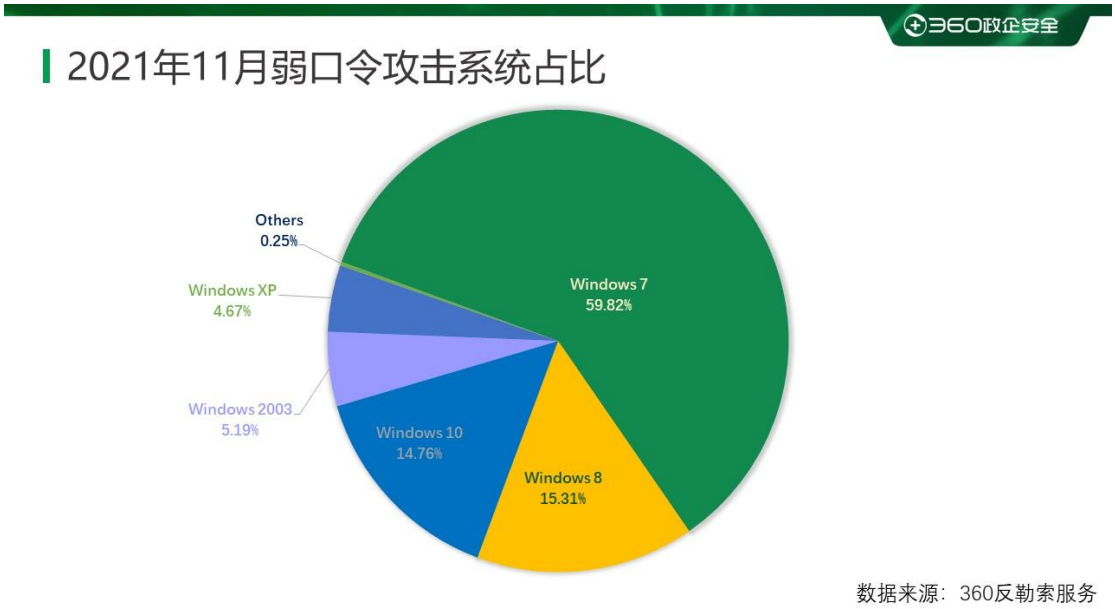
mym.com.pe	Aisha Steel-ASML	Emery Jensen Distribution
rintal.com	scotttesting.com	HELSA Group International
era.org.uk	hanshin-dp.co.jp	hsvgroup.talentnetwork.vn
GPV FRANCE	The Cochran Firm	STAR REFRIGERATION LIMITED
pkf.com.au	telemovil.com.sv	Ehud Leviathan Engineering
royole.com	planters-oil.net	Bryant Industrial Services
ochsnerEFS	nextech-asia.com	Rockbridge and Bath County
siix.co.jp	MCP Services LLC	Dealers Auto Auction Group
wnrllc.com	The Npd Group Inc	Karges-Faulconbridge, Inc.
APR Supply	owenscarolina.com	Comstock Johnson Architects
ALPSRX.COM	optimumdesign.com	Property Damage Restoration
jurelus.de	H.G.M Engineering	Hickory Veterinary Hospital
APG Neuros	Niemi Bil i Luleå	Holy Family RC & CE College
Koltepatil	CarpenterProjects	ASPECT STUDIOS ASIA PTY LTD
kenwal.com	R.E. Pedrotti Co.	MATITIAHU BRUCHIM Law office
JEAN FLOC'H	comfacundi.com.co	Marshall Investigative Group
TRINA SOLAR	ideaitaliausa.com	Virginia Department of Health
Metaenergia	John Sisk and Son	Thunderbird Adventist Academy
Gulfport MS	Lineage Logistics	Eason Horticultural Resources
MVS Mailers	National Material	Williams & Rowe Company, Inc.
abvalve.com	General RV Center	Beaverhead County High School
EQUITY Bank	kankakeetitle.com	Marten Transport (MRTN NASDAQ)
bsg-llp.com	Cadence Aerospace	FLUID COMPONENTS INTERNATIONAL
LOGROS S.A.	Отбасы банк	Law Society of South Australia
VR Souliere	Epple Druckfarben	Eberspächer Group of Companies
evans.co.id	Wolverine freight	Goodwill of Central and Coastal Virginia, Inc.
mecfond.com	Stoningtonschools	HARTMANN FINANCIAL ADVISORS LLC
MENZ&GASSER	Finite Recruitment	Herman & Kittle Properties Inc.
FUND-X S.A.	Southland Holdings	City of Fulton police department
Websites.co.in	Blue Harbor Resort	The Center for Rural Development
Lootah BCGas	Valley Machine Co.	Charley's Greenhouse Supply, LLC
interfor.com	cepimanagement.com	West Virginia Parkways Authority
logistia.com	Pronghorn Controls	Midwest Packaging Solutions, Inc.
INDIAN CREEK	AHEC Tax Solutions	Outdoor Venture Corporation (OVC)
chatrium.com	Raj Transport Inc.	Universitat Autònoma de Barcelona
Royale.co.uk	Alternatives, Inc.	Wisconsin Homes Inc Home Builders
cool-pak.com	The Leschaco Group	Cogan Wire and Metal Products Ltd
Dr Schneider	gunninglafazia.com	Unione dei Comuni Terre di Pianura
Fly Arik Air	Star Island Resort	Bock, Hatch, Lewis & Oppenheim, LLC
Electra Link	Tri Tech Surveying	HUDSON BROTHERS Construction Company
cardigos.com	JAFTEX Corporation	MINISTRY OF ECONOMY AND FINANCE Peru
Axi c orp GMBH	systematicatec.com	Hospitality Furnishings & Design Inc.
Orgill, Inc.	Daylesford Organic	Società Italiana degli Autori ed Editori

mfitexas.com	Amtech Corporation	Pueblo Bonito Pacifica Golf & Spa Resort
transaher.es	SWIRESPO.COM	Società Italiana degli Autori ed Editori
essextec.com	MGA RESEARCH	MOTOR VEHICLE ACCIDENT FUND PENSION FUND
docol.com.br	MCH-GROUP.COM	COMMUNAUTÉ DE COMMUNES PAYS D'APT LUBERON
EL Pruitt Co	PALMER LOGISTICS	The British Columbia Institute Of Technology
immodelaet.be	MUTUAL MATERIALS	ΤΕΧΝΟΛΟΓΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
atlas.ind.br	FRONTIER SOFTWARE	Department of Justice and Constitutional Development
Acne Studios	MUSCHERT-GIERSE.DE	Jet Industries Full Service Design And Construction Services
Alixa Rx LLC	MEYER CORPORATION	Transco Süd Internationale Transporte Gesellschaft mit beschränkter Haftung

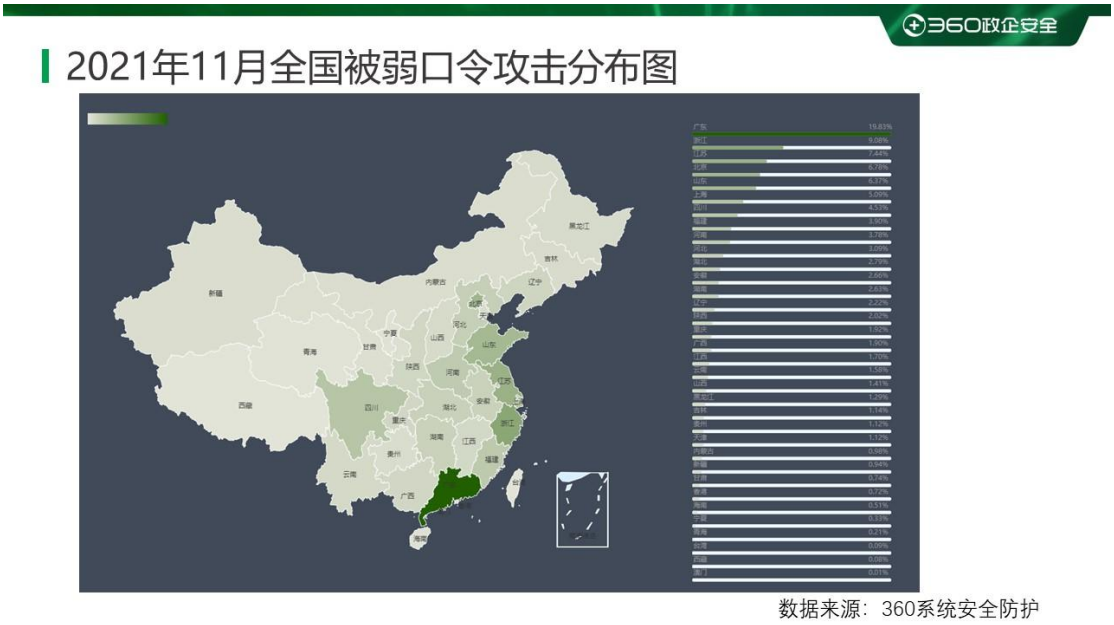
表格 2. 受害组织/企业

系统安全防护数据分析

通过将 2021 年 10 月与 11 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 11 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 11 月弱口令攻击态势发现，RDP 和 MYSQL 弱口令攻击整体无较大波动,MSSQL 的攻击量整体呈下降态势。

数据来源：360系统安全防护

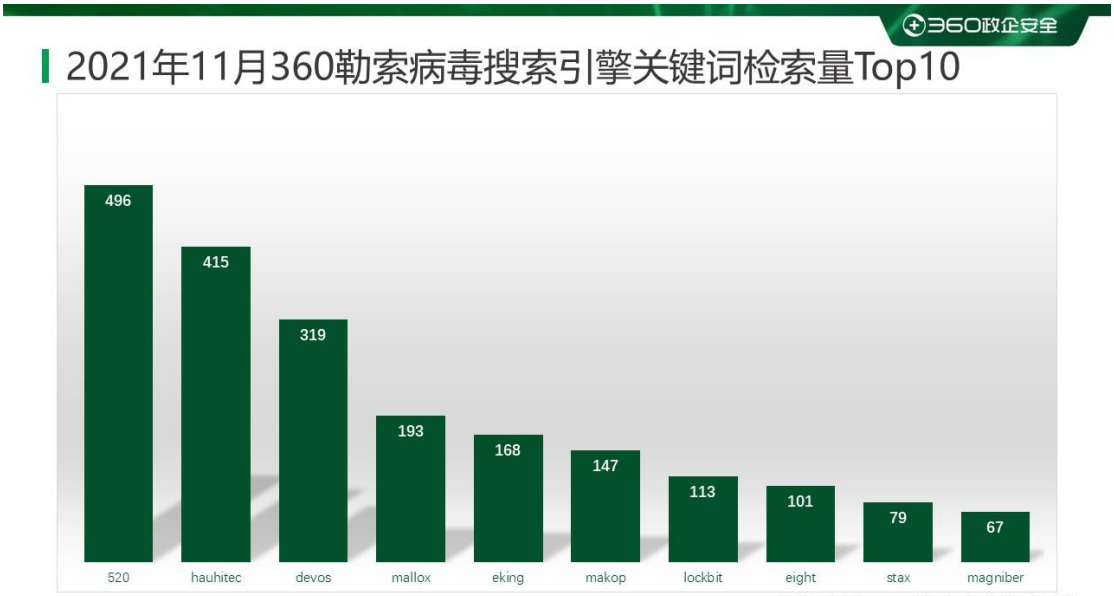
勒索病毒关键词

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。

- 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。
- 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。
- 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。
- 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。
- 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。
- 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。
- eight:同 devos。
- stax：属于 Stop 勒索病毒家族，由于被加密文件后缀会被修改为 stax 而成为关键词。该家族主要的传播方式为：伪装成破解软件或者激活工具进行传播。
- 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。



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 GandCrab，其次是 Crysis。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。

数据来源：反勒索服务统计数据

安全防护建议

面对严峻的勒索病毒威胁态势，360 安全大脑分别为个人用户和企业用户给出有针对性的安全建议。希望能够帮助尽可能多的用户全方位的保护计算机安全，免受勒索病毒感染。

一、 针对个人用户的安全建议

对于普通用户，360 安全大脑给出以下建议，以帮助用户免遭勒索病毒攻击。

(一)养成良好的安全习惯

1) 电脑应当安装具有高级威胁防护能力和主动防御功能的安全软件，不随意退出安全软件或关闭防护功能，对安全软件提示的各类风险行为不要轻易采取放行操作。

2) 可使用安全软件的漏洞修复功能，第一时间为操作系统和浏览器，常用软件打好补丁，以免病毒利用漏洞入侵电脑。

3) 尽量使用安全浏览器，减少遭遇挂马攻击、钓鱼网站的风险。

4) 重要文档、数据应经常做备份，一旦文件损坏或丢失，也可以及时找回。

5) 电脑设置的口令要足够复杂，包括数字、大小写字母、符号且长度至少应该有 8 位，不使用弱口令，以防攻击者破解。

(二)减少危险的上网操作

1) 不要浏览来路不明的色情、赌博等不良信息网站，此类网站经常被用于发起挂马、钓鱼攻击。

2) 不要轻易打开陌生人发来的邮件附件或邮件正文中的网址链接。也不要轻易打开扩展名为 js 、vbs、wsf、bat、cmd、ps1 等脚本文件和 exe、scr、com 等可执行程序，对于陌生人发来的压缩文件包，更应提高警惕，先使用安全软件进行检查

后再打开。

3) 电脑连接移动存储设备（如 U 盘、移动硬盘等），应首先使用安全软件检测其安全性。

4) 对于安全性不确定的文件，可以选择在安全软件的沙箱功能中打开运行，从而避免木马对实际系统的破坏。

(三)采取及时的补救措施

1) 安装 360 安全卫士并开启反勒索服务，一旦电脑被勒索软件感染，可以通过 360 反勒索服务寻求帮助，以尽可能的减小自身损失。

二、针对企业用户的安全建议

(一)企业安全规划建议

对企业信息系统的保护，是一项系统化工程，在企业信息化建设初期就应该加以考虑，建设过程中严格落实，防御勒索病毒也并非难事。对企业网络的安全建设，我们给出下面几方面的建议。

1) 安全规划

- 网络架构，业务、数据、服务分离，不同部门与区域之间通过 VLAN 和子网分离，减少因为单点沦陷造成大范围的网络受到攻击。
- 内外网隔离，合理设置 DMZ 区域，对外提供服务的设备要做严格管控。减少企业被外部攻击的暴露面。
- 安全设备部署，在企业终端和网络关键节点部署安全设备，并日常排查设备告警情况。
- 权限控制，包括业务流程权限与人员账户权限都应该做好控制，如控制共享网络权限，原则上以最小权限提供服务。降低因为单个账户沦陷而造成更大范围影响。
- 数据备份保护，对关键数据和业务系统做备份，如离线备份，异地备份，云备份等，避免因为数据丢失、被加密等造成业务停摆，甚至被迫向攻击者妥协。

2) 安全管理

- 账户口令管理，严格执行账户口令安全管理，重点排查弱口令问题，口令长期不更新问题，账户口令共用问题，内置、默认账户问题。
- 补丁与漏洞扫描，了解企业数字资产情况，将补丁管理做为日常安全维护项目，关注补丁发布情况，及时更新系统、应用系统、硬件产品安全补丁。定期执行漏洞扫描，发现设备中存在的安全问题。
- 权限管控，定期检查账户情况，尤其是新增账户。排查账户权限，及时停用非必要权限，对新增账户应有足够警惕，做好登记管理。

- 内网强化，进行内网主机加固，定期排查未正确进行安全设置，未正确安装安全软件设备，关闭设备中的非必要服务，提升内网设备安全性。

3) 人员管理

- 人员培训，对员工进行安全教育，培养员工安全意识，如识别钓鱼邮件、钓鱼页面等。
- 行为规范，制定工作行为规范，指导员工如何正常处理数据，发布信息，做好个人安全保障。如避免员工将公司网络部署，服务器设置发布到互联网之中。

(二)发现遭受勒索病毒攻击后的处理流程

1) 发现中毒机器应立即关闭其网络和该计算机。关闭网络能阻止勒索病毒在内网横向传播，关闭计算机能及时阻止勒索病毒继续加密文件。

2) 联系安全厂商，对内部网络进行排查处理。

3) 公司内部所有机器口令均应更换，你无法确定黑客掌握了内部多少机器的口令。

(三)遭受勒索病毒攻击后的防护措施

1) 联系安全厂商，对内部网络进行排查处理。

2) 登录口令要有足够的长度和复杂性，并定期更换登录口令

3) 重要资料的共享文件夹应设置访问权限控制，并进行定期备份

4) 定期检测系统和软件中的安全漏洞，及时打上补丁。

a) 是否有新增账户
b) Guest 是否被启用
c) Windows 系统日志是否存在异常
d) 杀毒软件是否存在异常拦截情况

5) 登录口令要有足够的长度和复杂性，并定期更换登录口令

6) 重要资料的共享文件夹应设置访问权限控制，并进行定期备份

7) 定期检测系统和软件中的安全漏洞，及时打上补丁。

三、不建议支付赎金

最后——无论是个人用户还是企业用户，都不建议支付赎金！

支付赎金不仅变相鼓励了勒索攻击行为，而且解密的过程还可能会带来新的安全风险。可以尝试通过备份、数据恢复、数据修复等手段挽回部分损失。比如：部分勒索病毒只加密文件头部数据，对于某些类型的文件（如数据库文件），可以尝试通过数据修复手段来修复被加密文件。如果不得不支付赎金的话，可以尝试和黑客协商来降低赎金价格，同时在协商过程中要避免暴露自己真实身份信息和紧急程度，以免黑客漫天要价。若对方窃取了重要数据并以此为要挟进行勒索，则应立即采取补救措施——修补安全漏洞并调整相关业务，尽可能将数据泄露造成的损失降到最低。