2022 年 6 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数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，勒索金额高达数百万到近亿美元的勒索案件也不断出现。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测与防御，为需要帮助的用户提供 360 反勒索服务。

2022 年 6 月，全球新增的活跃勒索病毒家族有:BlueSky、Crimson Walrus、SiegedSec、Agenda、Kawaii、DamaCrypt、RedTeam 等家族，其中 Crimson Walrus 和 SiegedSec 均为双重勒索，勒索病毒家族。

本月最值得关注的有三个热点：

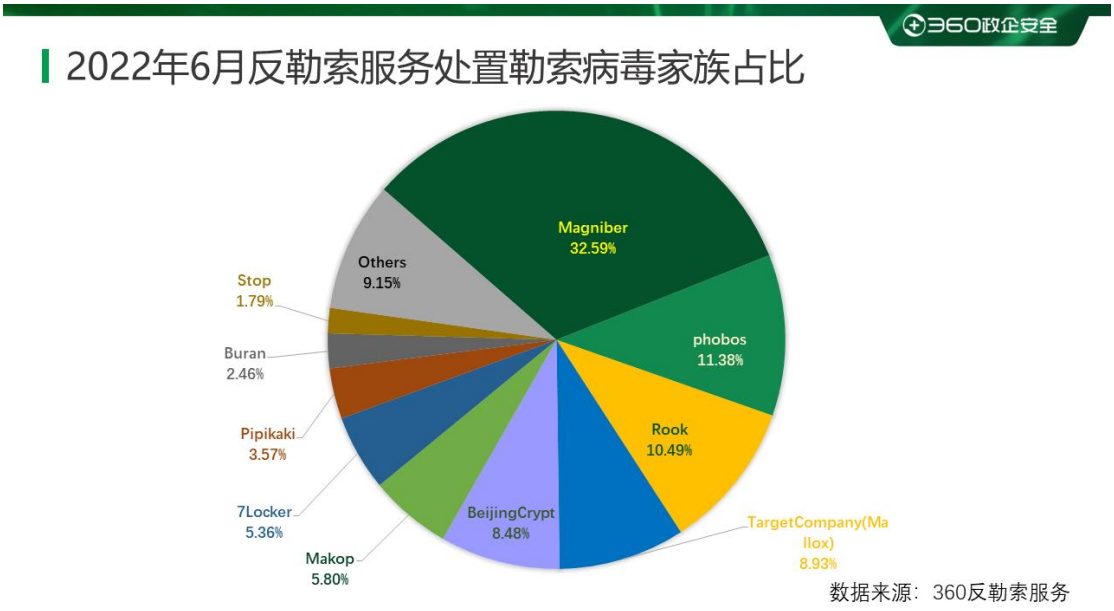
1. LockBit3.0 来袭，首个推出勒索病毒漏洞赏金计划以及首个在数据泄露网站添加对受害组织/企业数据购买/销毁/延期的支付通道。
2. 多款“新型”勒索软件在本月活跃。包括使用全中文勒索提示信息的 Rook，通过 SQLGlobeImposter 渠道传播的 BlueSky 新型勒索病毒以及通过僵尸网络和远程桌面协议进行传播的 Pipikaki 勒索病毒。
3. 针对威联通设备的勒索攻击持续活跃， eChORaix 勒索病毒攻击尚未停止，又新增 DeadBolt 勒索病毒攻击。

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。

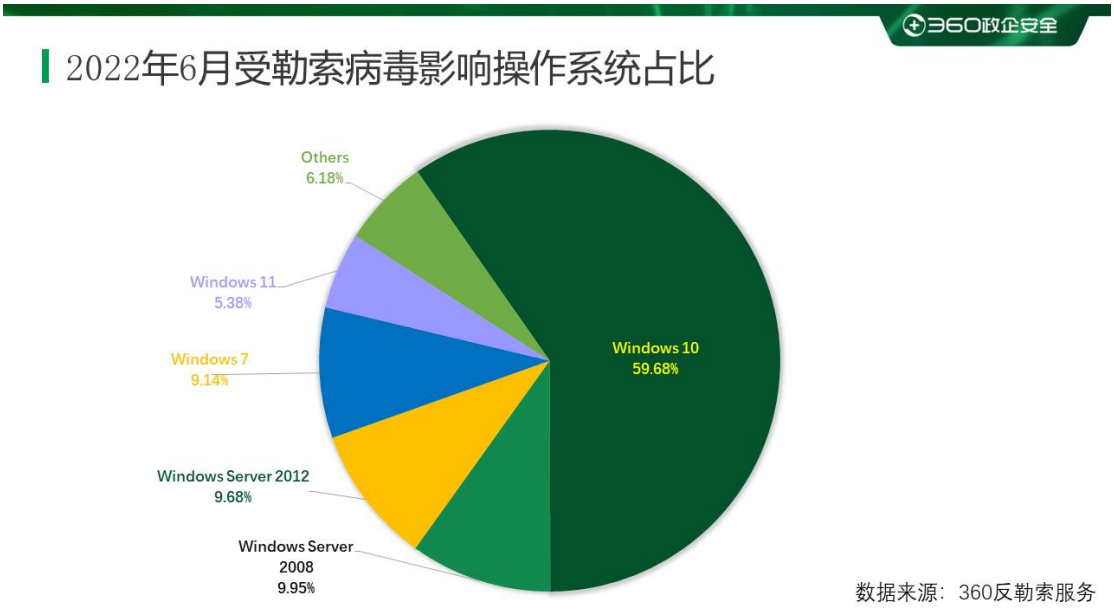
感染数据分析

针对本月勒索病毒受害者所感染勒索病毒家族进行统计，Magniber 家族占比 32.59%居首位，其次是占比 11.38%的 phobos，Rook 家族以 10.49%位居第三。

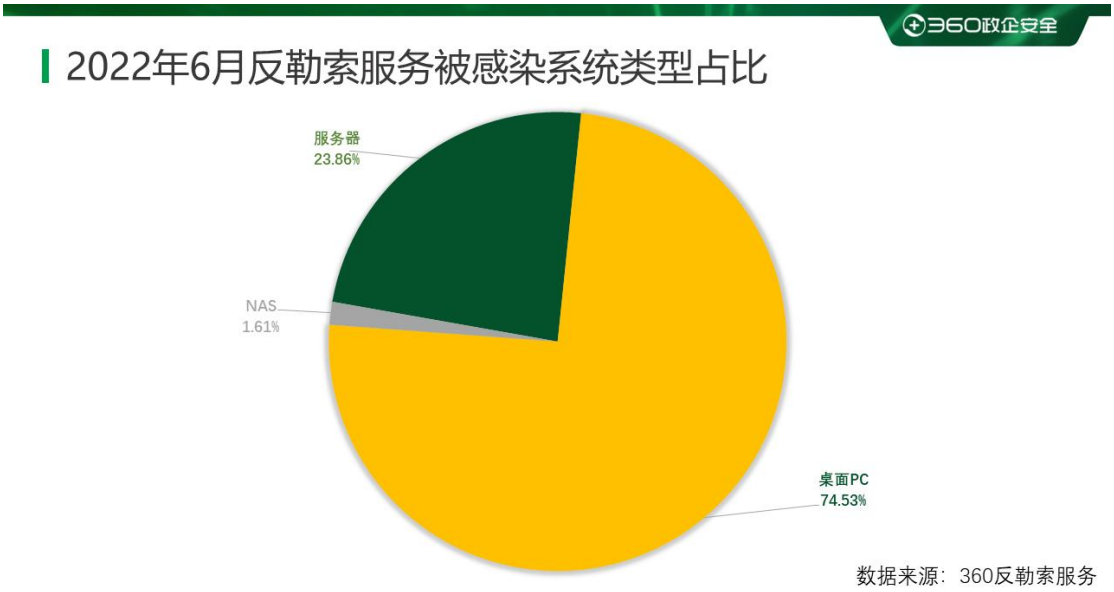
本月上旬消失数月的 Rook 勒索病毒家族，携全新后缀名与勒索提示信息卷土重来，本月下旬利用匿影僵尸网络以及 RDP 暴破进行传播的 Pipikaki 在国内异常活跃。



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 Server 2008、以及 Windows Server 2012。



2022 年 6 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

LockBit 3.0 来袭

本月，Lockbit 勒索病毒团伙正式发布 3.0 版本，并在其数据泄露网站发布公告，邀请全球所有的安全研究员参与该团伙的漏洞赏金计划——根据漏洞的严重程度可换取 1000 至 100 万美元的奖金。

该勒索团伙还在其数据泄露网站发布一篇长文，详细描述该团伙能为病毒运营及投放者

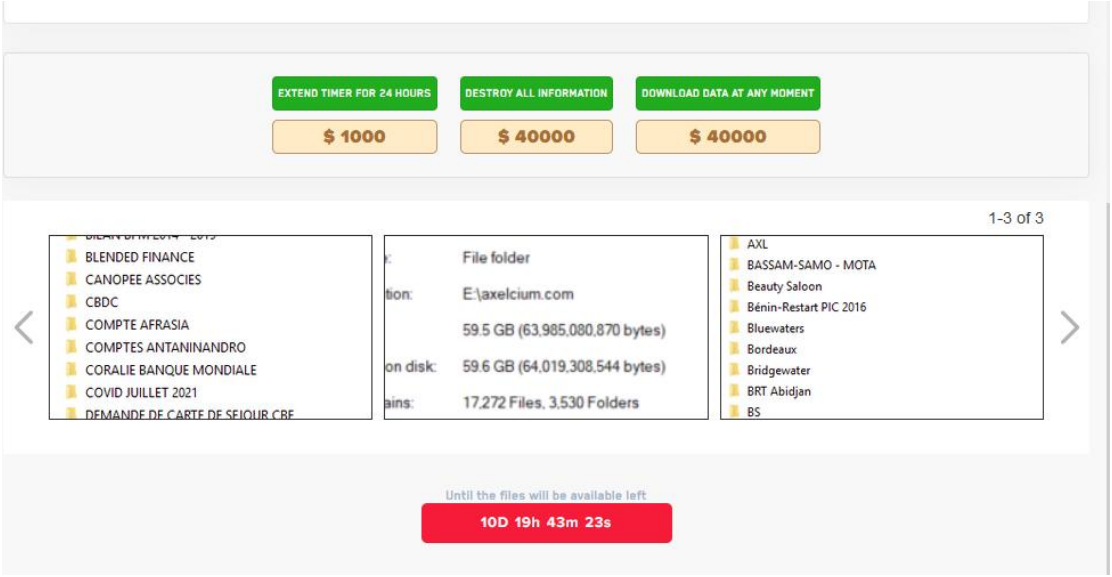
提供的支持，其中包括：安全软件的绕过、网络资源检测、域内自动分发、数据窃取等。同时详细罗列哪些类型的企业不允许实施加密，但可窃取重要数据，例如：核电站、火力发电站、水力发电站等关键基础设施；石油、天然气等能源行业；可能会影响生命的医疗机构等。并鼓励病毒运营及投放者对警察局和任何从事寻找逮捕黑客的执法机构发动攻击。

Categories of targets to attack:
It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.
The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.
It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

It is allowed to attack non-profit organizations. If an organization has computers, it must take care of the security of the corporate network.
It is allowed to attack any educational institutions as long as they are private and have a revenue.
It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex and force to be very careful in Thailand, as well as any other organizations provided that they are private and have rhubarb. It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed. It is allowed to steal data from any medical facilities without encryption, as it may be a medical secret and must be strictly protected in accordance with the law. If you can't pinpoint whether or not a particular medical organization can be attacked, contact the helpdesk.
It is very commendable to attack police stations and any other law enforcement agencies that are engaged in finding and arresting hackers, they do not appreciate our useful work as a pentest with postpaid and consider it a violation of the law, we should show them that a competent computer network setup is very important and write a fine for computer illiteracy.
It is allowed to attack government organizations, only with revenue.

在已被公布受害组织/企业的链接中，能直接看到该团伙索要的赎金金额。目前该团伙为针对被窃取到数据的受害组织/企业提供以下三个选项（黑客会根据受害组织/企业窃取到的数据进行估值，因此每个受害组织/企业被勒索的赎金并不相同，以下为一个受害企业示例）：

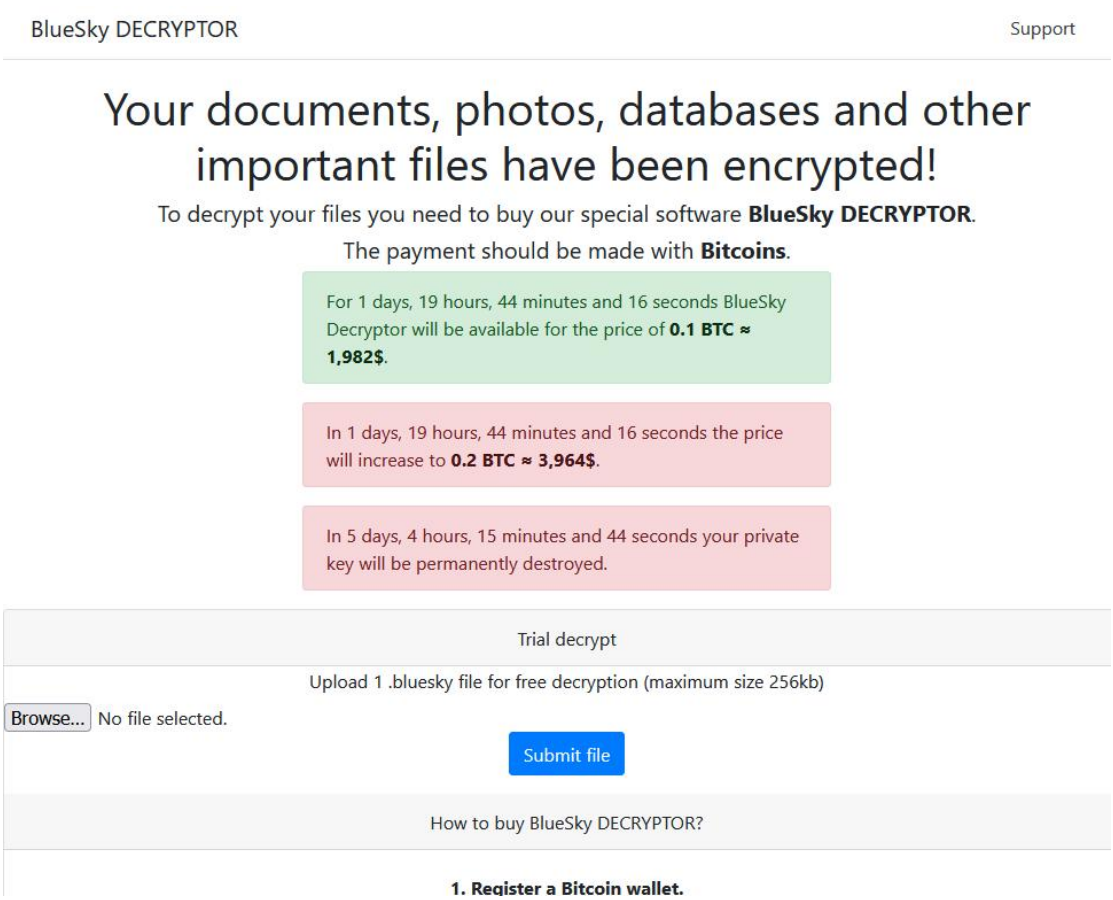
4. 提供 1000 美元对数据泄露倒计时进行 24 小时的延时。
5. 提供 40000 美元赎金对窃取到的数据进行销毁。
6. 提供 40000 万美元的数据对窃取到的数据进行购回。



多款“新型”勒索病毒在本月活跃

360 安全大脑监测到本月有三款勒索病毒异常活跃。其中第一款是在本月上旬消失数月的 Rook 勒索病毒再次回归公众视野。在消失之前，该家族曾短暂想要通过模仿 LockBit 和 BlackCat 两款流行的双重勒索病毒来混淆视听，失败后便销声匿迹。此次回归使用的勒索提示信息采用全中文版，对每个受害者索要价值 4000 人民币的比特币。同时还提醒受害者可通过淘宝和勒索病毒贴吧去获取解密协助。

第二款是在本月中旬出现的一款自称为 BlueSky 的勒索病毒。根据 360 安全大脑监测到的数据分析，该家族通过 SQLGlobeImposter 渠道进行传播（该渠道的传播方式为：黑客通过暴力破解方式获取到数据库密码后向被攻陷设备投放各类型病毒木马）。受害者通常会被索要 0.1 比特币作为赎金（截至报告撰写时，约合人民币 13291 元）。

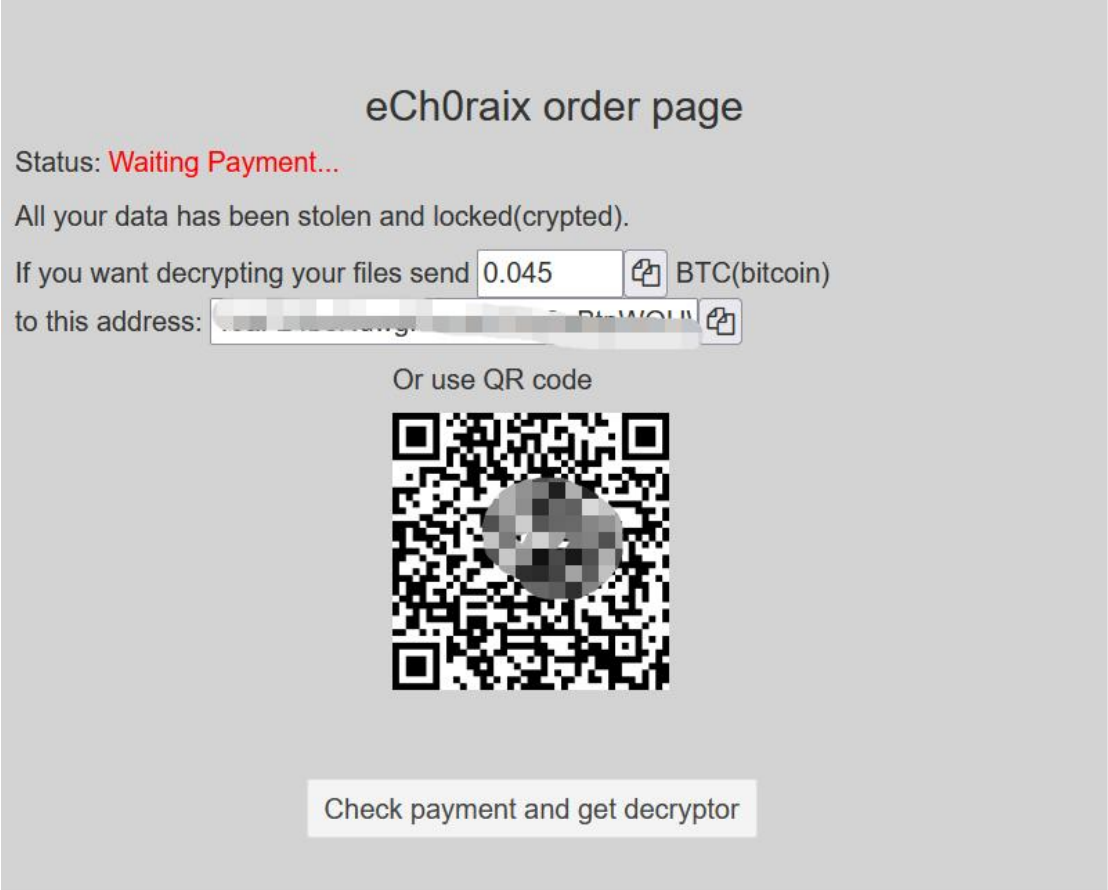


第三款则是本月下旬开始活跃的 Pipikaki 勒索病毒家族。该家族虽然 4 月份已在国外被发现，但本月才开始在国内流行传播。通过 360 安全大脑监控到的数据分析到，该家族不仅利用暴力破解远程桌面弱口令后手动投毒，还通过匿影僵尸网络进行传播。被攻击的设备通常是在收到攻击前运行过 AutoDesk 注册机、CAD 注册机、KMS 注册机等工具软件。而这些程序通常带有恶意代码，会向受害者机器内写入计划任务，定时启动达到长期驻留在受害者系统的目的，而后由僵尸网络控制者决定向其下发什么类型的病毒木马。也正因这种先感染后受控中毒的特性，导致受害者运行这类工具后文件并不会马上被加密，也给事后分析病毒来源带来了一定的难度。

NAS 设备迎来新对手

本月初，有威联通设备遭遇 eCh0raix 勒索病毒攻击。eCh0raix（也称为 QNAPCrypt）从 2019 年夏天开始，便多次大规模对 QNAP 的 NAS 设备发动攻击并成功入侵，直至 2020 年 5 月该家族依然有攻击活动，并于 2021 年 12 月中旬开始针对 NAS 设备发动了新一轮的大量弱口令攻击，而这一波攻势在 2022 年 2 月初才逐步放缓。

此次 eCh0raix 的新一轮攻击出现在 6 月 8 日前后，目前已经捕获到数十个 eCh0raix 的变种样本，预估实际成功攻击量会更高。



此外，QNAP 于 6 月 17 日再次警告其用户要当心他们的设备遭到另一款勒索病毒——DeadBolt 的新一轮攻击。根据威联通产品安全事件响应小组（QNAP PSIRT）的调查，这两次的勒索病毒攻击针对使用 QTS 4.3.6 和 QTS 4.4.1 的 NAS 设备，受影响的机型主要是 TS-x51 系列和 TS-x53 系列。“此次警告是在该公司自 2022 年初以来发布的第四次相关警报信息，所有这些警报都建议用户保持其设备最新状态，且不要将设备其暴露在互联网中。”

黑客信息披露

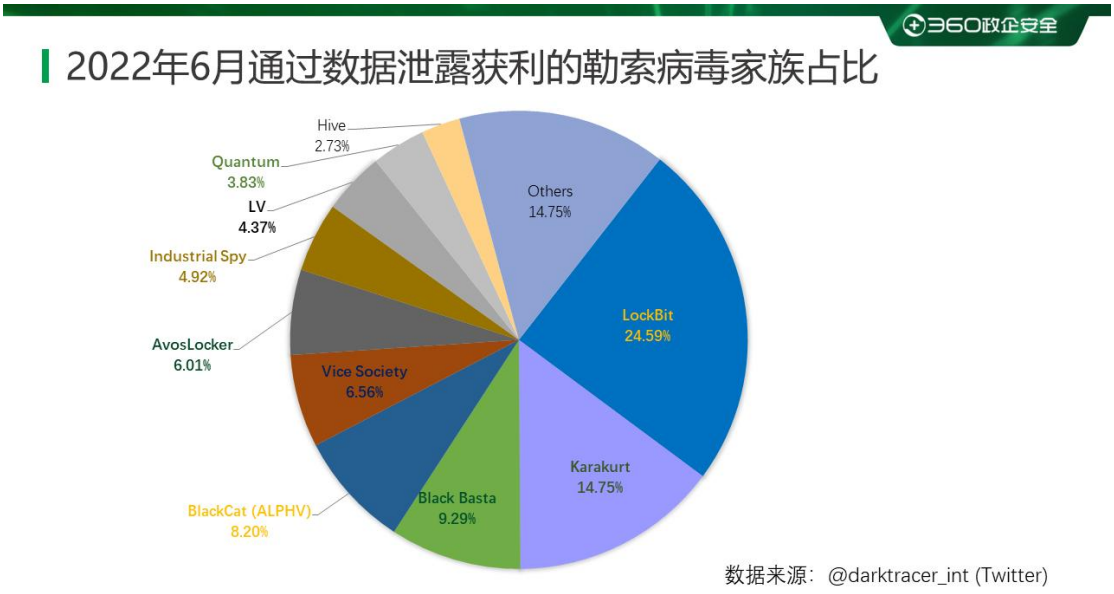
以下是本月收集到的黑客邮箱信息：

return@email.tg	bleepbloopbop@criptext.com	bleepbloopbop@protonmail.com
back23@vpn.tg	for_recovery@privatemail.com	Data_recovery_asia@mailfence.com
recoverservice5@onionmail.org	restaurera@rbox.co	recuper@smime.ninja
blockzsupport@protonmail.com	@PIPIKAKI	pipikaki@onionmail.org
irvesely17@onionmail.org	yourcyanide.help@gmail.com	encoderdecryption@yandex.ru
encoderdecryption@gmail.com	@EAF_SUPPORT_BOT	d3add@privatemail.com
supportx@privatemail.com	yoshihama@privatemail.com	ariakei@protonmail.com
ariakei@protonmail.com	xats@privatemail.com	teamdecrypt@disroot.org
snowbox@tuta.io	helpforyou@gmx.com	@Ransomware_Decrypt
d3add@privatemail.com	tomas1991goldberg@medmail.ch	buybackdate@privatemail.com
r3wuq@tuta.io	Starmoon@my.com	rebackteam@mail.ee

reback01@tutanota.com	bsupport@email.tg	woodpeker@tutanota.com
dealinfrm@cock.li	brendasrivera@tutanota.com	eternalnightmare@tutanota.com
qkhooks0708@protonmail.com	poolhackers@tutanota.com	shadowghosts@tutanota.com
fortihooks@protonmail.com	shadowghosts@tutanota.com	rsaecho@tutanota.com
securityaccounts@tutanota.com	takunoya@tutanota.com	etira@tutanota.com
payorleak@cock.li	JulioErick@tutanota.com	payorleak@cock.li
Just4money@TUTANOTA.COM	bsupport@email.tg	marcosroxana@aol.com
sikfotrisd@tutanota.com	khgurwte@tutanota.com	apolo1000@protonmail.com
sacipaws@tutanota.com	jiminok31@cock.li	for_recovery@privatemail.com
hudsonL@cock.li	pipikaki@privatemail.com	hpsupport@cyberfear.com
for_recovery@privatemail.com	myers@cock.li	trust03@tutanota.com
newSanta@protonmail.com	andreihelp@cyberfear.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 183 个组织/企业遭遇勒索攻击，其中包含中国 7 个组织/企业（含 3 个台湾省组织/企业）在本月遭遇了双重勒索/多重勒索。

Atlantic Dialysis Management Services	fgmarchitects.com	sando.com
diodes.com	Crupi Group	Apex
Avante Health Solutions	New Peoples Bank	Egg Holz Kälin AG
Catalogic Software Inc.	Tolmage, Peskin, Harris & Falick	Paracca Flooring

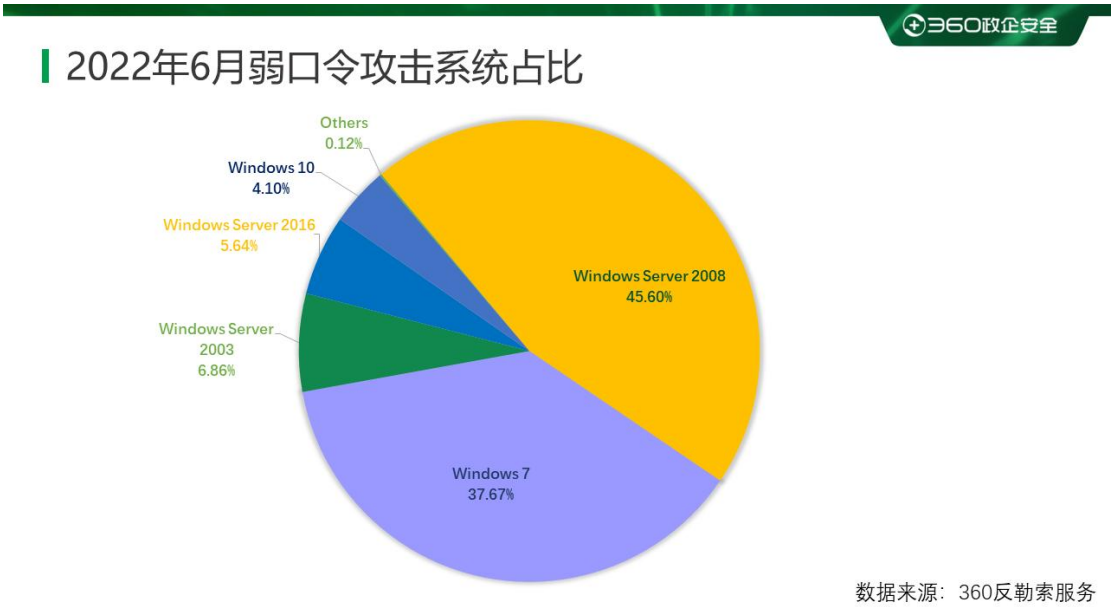
AUTOPAY	TVS Logistics Services	Senior Star Corporate
OKAKI	Century Dental Associates	Tankersley Foodservice
Viora	Lawson Products	KMH Cardiology
Mitcham Industries, Inc	Norwood	Superior Asphalt
CMG Mortgage, Inc.	Forterra PLC	Habasit
FellowShip Warehousing & Logistics	Shields Health Care Group	Hengan International Group
Council of Governments (COG)	Weldco	Trantor
Kamarin	Notaire	SuperAlloy Industrial Co., Ltd.
Diskriter	datalit.it	Ministry of Agriculture Rebublic Indonesia
metroappliancesandmore.com	lonseal.com	Bonneville Collections
Advanced Micro Devices, Inc	R1group	Medical University of Innsbruck
oak-brook.org	Elbit Systems of America	Napa Valley College
Prudential LTG.	Northern Data Systems	Cpl Architects, Engineers
nutis.com	Alphapointe	FAYAT
Arte Radiotelevisivo Argentino (Artear)	ENTEGA.DE	COUNT+CARE
Reed Pope Law	BAHRA ELECTRIC	Electric House
Matco Electric	PT Astra Honda Motor	Pilton Community College
ecos-office.com	coteg-azam.fr	GRUPO mh
Ospedale Macedonio Melloni	Canaropa	Mechanical Systems Company
Crane Carrier Company	PARADOX	farmaciacirici.com
sigma-alimentos.com	agricolaandrea.com	Vinstar
business.gov.om	builditinc.com	rhenus.group
kuwaitairways.com	emprint.com	plagepalace.com
acac.com	ChungHwa Telecom	htijobs.com
hfi-inc.com	SOCOTEC	CR2
Bechstein	Spy Ballon	tb-kawashima.co.jp/en/
lundinroof.com	RG Alliance Group	www.cmz.com
Novelty Group	MOLTOLUCE	vanderpol's
Israeli power companies	RadiciGroup	Magnum
genusplc.com	medcoenergi.com	dgi.gouv.ml
gruppowasteitalia.it	www.kinexia.it	YMCA
Shred Station	M. Green and Company LLP	Medlab Pathology
Purvis Industries	SHOPRITE HOLDINGS LTD	Plainedge Public Schools
SCHIFFMANS	MOTOLUCLE.COM	theallison.com
Bernd Hösele Group	Grand Valley State University	Etron
ptg.com.au	Opal	SDZ Druck und Medien
slgienergy.com	novartis.com/ch-de/	www.planet-biogas.com
The University of Pisa	Metek Plc	eivp-paris.fr
Tiroler Rohre GmbH	Worldwide Flight Services	cargoexperts.eu
vectorinf.com.br	Samson Supplies Co.	Spencer, Daniels & Daniels Law
D.S Financial	Ascension International	kaisoten.co.jp

CAPECODRTA	Palermo	Livingston
Goodman Campbell Brain & Spine	English Construction Company	The O'Regan
Losberger De Boer	equis.com	Yildiz Entegre USA
CMHA National	Chimbusco	VTVCAB
mandiant.com	IBRCN.COM	sesver.gob.mx
patralogistik.com	hyatts.com	linmark.com
kansashighwaypatrol.org	bestattung-walzer.at	vainieritrasporti.com
SilTerra	colonail.com	wik-group.com
specpharm.co.za	ora.com	familyclinicbridgeport.com
Northeastern Technical College	Sierra Packaging	TPI Corporation
Public Employees Credit Union	CPA Mutual Insurance Company	BLUME GLOBAL INC
CHRISTUS Health	St Paul	Acorn Recruitment
The De Montfort School	land karnten	Alexandria. (LA)
closetheloopeu.com	Novartis.com	sattse.com
Nelsonslaw LLP	CICIS.COM	Jonathan Adler
NewsVoir	AMS-Gruppe	JBS TEXTILE GROUP

表格 2. 受害组织/企业

系统安全防护数据分析

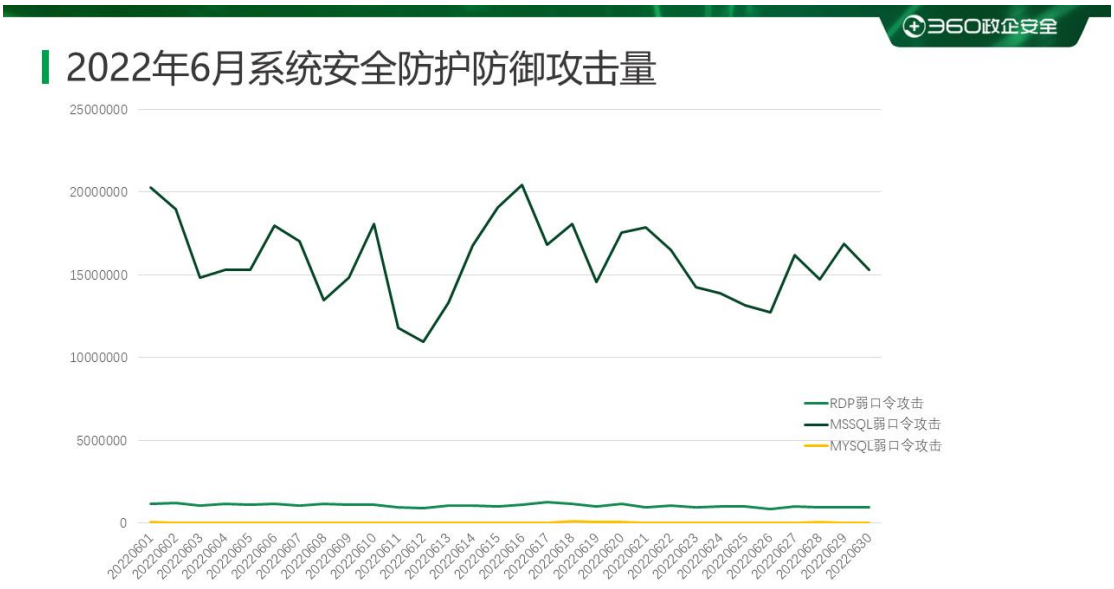
在本月被攻击的系统版本中，排行前三的依次为 Windows Server 2008 、Windows 7 以及 Windows Server 2003。



对 2022 年 6 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。

数据来源：360系统安全防护

通过观察 2022 年 6 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。



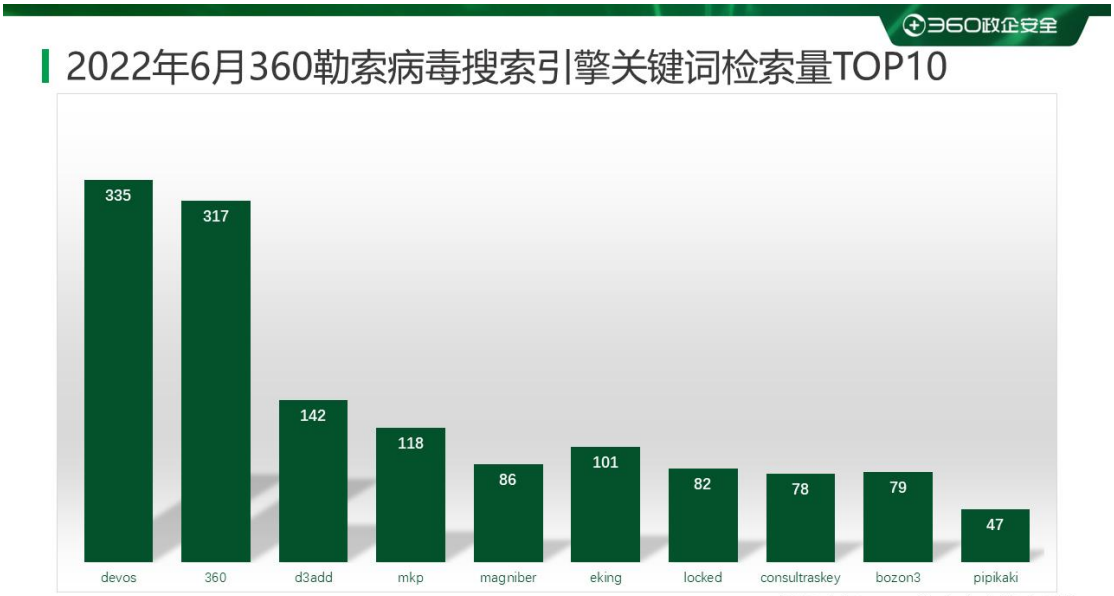
数据来源：360系统安全防护

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。

- 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。

- d3add：属于 Rook 勒索病毒家族，由于被加密文件后缀会被修改为 d3add 而成为关键词。该家族的主要通过匿隐僵尸网络进行传播
- 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。
- Magniber:勒索病毒 Magniber 家族，主要通过伪装成 Win10/win11 的补丁/升级包进行传播。
- 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。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。
- 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。
- 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 而成为关键词。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。本月新增通过入侵 Web 应用进行传播。
- bozon3:同 consultraskey。
- pipikaki:属于 Pipikaki 勒索病毒家族，由于被加密文件后缀会被修改为@pipikaki 而成为关键词，该家族主要通过匿影僵尸网络以及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 Coffee。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 GandCrab 家族加密的设备。

数据来源：反勒索服务统计数据

2022 年上半年勒索病毒发展回顾

2022 年上半年，勒索病毒攻击势头不减，继续引领全球网络安全热点，360 政企安全集团高级威胁研究分析中心对国内外勒索病毒攻击态势进行了分析，总结了如下一些新的攻击特点：

1. 勒索病毒成为网络战争首选武器

现代国际冲中，突越来越多的出现“热战”之前网络战先行的趋势。勒索病毒做为低成本、高效率的网络破坏性武器，也越来越受到攻击者的青睐，假借商业勒索病毒之名发起的“假旗”攻击更是层出不穷。

在今年上半年俄乌冲突中，勒索病毒就成为多方使用的网络武器之一。在过去几年的攻击中，也出现了以 NotPetya 为代表的网络武器。使用勒索病毒发起破坏攻击，可以掩盖攻击的真实意图，让受害者放松警惕，以为仅仅是常规的商业攻击事件。而今年早些时候，HermeticWiper、WhisperGate 等多种 wiper 类擦除器，对多个关键基础设施造成了广泛破坏，也再次展示了此类攻击的威力。

数字时代下网络战将成任何形式冲突中的首选攻击方案。网络战攻击不仅仅是为了窃取情报，还可以对交通、能源、金融等基础设施造成破坏。而网络中任何一个设备节点都可能成为攻击跳板，牵一发而动全身引发严重后果，为此必须要意识到网络战的严峻形势，正视网络战。

2. 国内传播多元化、变种多样传播更趋本土化

以 Log4j2 漏洞为代表的一批高危安全漏洞，拉开了本年度网络攻击事件的序幕。年初 TellYouThePass 勒索家族先后使用 Log4j2 漏洞、Spring 漏洞和向日葵漏洞等多个 Nday 漏洞大肆传播。之后 Magniber 不甘示弱，开始伪装系统升级，利用网页挂马传播，并迅速占领国内第一的位置。随后而来的，还有 Rook 利用携带恶意代码的第三方软件进行传播；TargetCompany(Mallox)勒索病毒使用 Web 应用入侵渠道传播等等。

可以看出，国内勒索病毒的传播越来越多元化，竞争也愈加激烈。勒索病毒的趋势不再由少数几个头部家族说掌控，而其传播方式也越来越“接地气”——不管是越来越多的漏洞攻击，还是 Magniber 这类有本土特色的传播方法。攻击方法无孔不入，也加速了勒索病毒对普通用户和中小企业的侵扰。

另一方面，针对 NAS、Linux 系统、MacOS 的攻击也显著增加，过去大众一般认为“安全”的设备，其实并不安全，也无法豁免于勒索病毒的攻击中。

3. 病毒团伙内讧、被捕与地缘政治

年初 Conti 团伙的内讧，其内部数据的公开给安全研究人员一个很好的视角研究勒索病毒攻击问题。泄露的内部数据可以看出：Conti 是一个复杂的组织，成员分工明确且复杂和多个黑产组织如 TrickBot 和 Emotet 有密切往来。公开的内容还包括大量攻击方法、教程、工具、勒索病毒源码等，并且很快就出现了使用公开源码编写的变种勒索病毒。

同一时间，臭名昭著的勒索团伙 REvil 多为成员被捕。据官方报道：联邦安全局（FSB）宣布已经逮捕了 14 名与网络犯罪团伙 REvil 相关的人员，并没收了超过 4.26 亿卢布的财产。加上此前被逮捕的成员，至少有 20 多个隶属于该团伙的成员被逮捕。

由于俄乌冲突，多个黑客团伙也选边站队，多个知名黑客组织声称要发起大规模网络攻击。上半年黑产团伙活跃而混乱。

4. 支付方式多样化

自从去年 DarkSide 勒索美国燃油管道公司的比特币被追缴以来，勒索攻击者对比特币的信任度在不断降低，越来越多的攻击者开始选择门罗币、零币、达世币等做为替代手段支付方案——这一趋势在今年更加明显。这也表明，脱离监管的支付工具是这类黑产的重要依赖手段。越来越多的匿名支付工具以及更好的匿名性也给勒索病毒犯罪的打击，带来了很大挑战。