勒索软件流行态势分析

2023 年 1 月

360数字安全

数 字 安 全 的 领 导 者

勒索软件传播至今，360 反勒索服务已累计接收到上万勒索软件感染求助。随着新型勒索软件的快速蔓延，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。勒索软件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 全网安全大脑针对勒索软件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。

2023 年 1 月，全球新增的活跃勒索软件家族有:SUnSafe、Nokoyawa、Mimic、SickFile、Upsilon、BetterCallSaul 等家族。其中 UnSafe 和 Nokoyawa 是本月新增的双重勒索软件，Minic 勒索软件利用合法软件 Everything 来快速过滤需要加密的文件。

以下是本月值的关注的部分热点：

- Lorenz 勒索软件团伙会在入侵后部署后门长达数月。
- BitDefender 免费放出 MegaCortex 勒索软件解密工具，360 解密大师同步跟进。
- Vice Society 勒索软件发动多起勒索攻击。

基于对 360 反勒索数据的分析研判，360 数字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

针对本月勒索软件受害者所中病毒家族进行统计：phobos 家族占比 22.83%居首位，其次是占比 20.29%的 BeijingCrypt，TargetCompany(Mallox)家族以 15.94%位居第三。

Standby 和 RCRU64 虽并非本月新增的勒索家族，但是首次进入月度排行 TOP10。这两个家族目前在国内较为活跃，其传播方式采用了最为常见的暴力破解远程桌面口令成功后手动投毒。

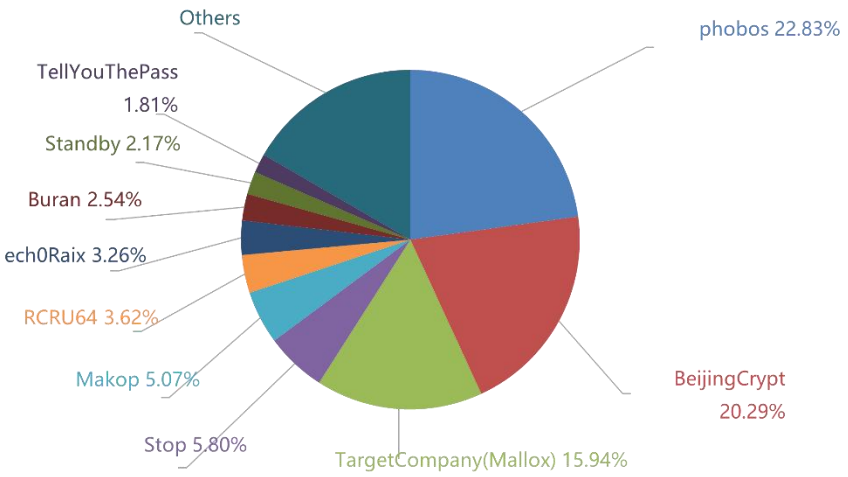

图 1. 本月受害者感染勒索软件所属家族占比

对本月受害者所使用的操作系统进行统计，位居前三的分别是：Windows 10、Windows Server 2008 以及 Windows Server 2012。

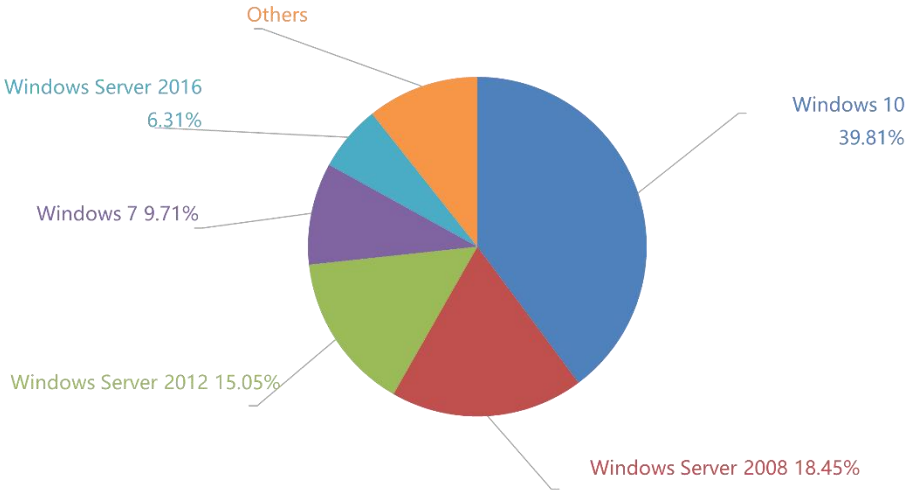

图 2. 本月受害者所使用操作系统占比

2023 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。

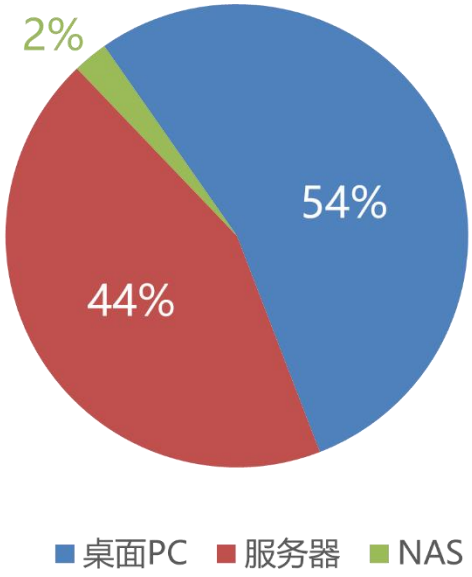

图 3. 本月受害者所使用操作系统类型占比

勒索软件疫情分析

Lorenz 勒索软件团伙会在入侵后部署后门长达数月

安全研究人员警告，在对 Lorenz 勒索软件的攻击事件展开分析研究的过程中发现，黑客在开始横向移动、窃取数据和加密系统之前五个月，就已经侵入了受害者网络。经分析确认，黑客是利用 CVE-2022-29499（Mitel 电话基础设施中的一个重要漏洞，允许远程代码执行）获得了初始访问权限。

研究人员发现，Lorenz 勒索软件的幕后黑客行动非常迅速，在掌握漏洞利用方法后第一时间进行了实际运用。其在受害用户修复漏洞的前一周，便已经成功入侵了其网络系统并安装了 PHP Web Shell 后门。同时，黑客试图隐藏后门，将其命名为“twitter_icon_<勒索字符串>”，并将其放置在系统的合法位置目录中。

而在成功安装后门的五个月后，当黑客准备继续攻击时，他们才启用了该后门并在 48 小时内部署了 Lorenz 勒索软件。

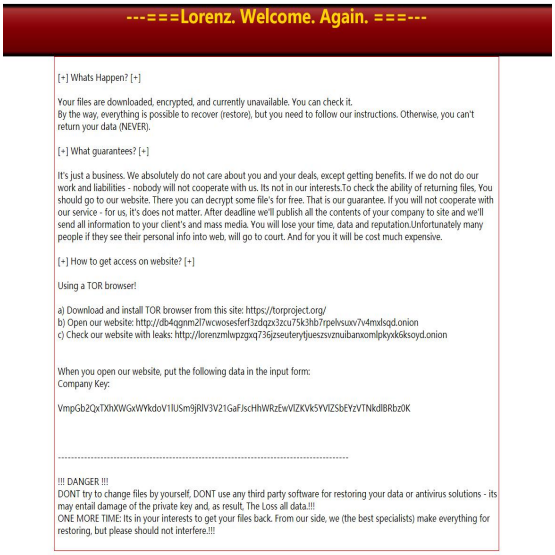

图 4. Lorenz 勒索信息

BitDefender 免费放出 MegaCortex 勒索软件解密工具

反病毒公司 BitDefender 对外发布了 MegaCortex 家族勒索软件的解密工具，使这个“曾经臭名昭著的勒索软件家族”的受害者可以免费恢复他们的数据。

MegaCortex 勒索软件首次被发现于 2019 年 5 月，该家族软件会通过 QBot、Emotet 和 Cobalt Strike 等渠道传播，并针对企业网络发起攻击。2019 年 7 月，MegaCortex 运营者发起了多起攻击，并根据受害者的

企业规模调整赎金要求。2019 年 11 月，MegaCortex 运营者则进一步开始采用双重勒索策略，威胁受害者如果不满足他们的赎金要求，就会公布他们窃取到的数据。

2021 年 10 月，欧洲刑警组织宣布逮捕了 12 名发起勒索软件攻击的人员，其中就包含了 MegaCortex 家族的相关人员。

在该解密公布后，360 解密大师已经第一时间同步添加了对该勒索家族的解密功能。

图 5. 360 解密大师同步加入对 MegaCortex 的解密功能

Vice Society 勒索软件发动多起勒索攻击

据澳大利亚维多利亚州消防救援局（FRV）公布的消息，该局于去年 12 月遭到 Vice Society 勒索软件攻击，对其多台内部服务器及邮件系统造成了影响，直接导致其内部大面积的 IT 系统瘫痪。此外，FRV 还表示，黑客在其内部网络中窃取了多种数据——包括有关现任及前任员工、承包商、借调人员和求职者的信息。

与该攻击类似，Vice Society 自己也公布了去年 11 月时针对德国杜伊斯堡-埃森大学（UDE）的攻击事件。这一攻击迫使该大学重建其 IT 基础设施，截止目前，重建仍未完成。同样的，攻击者还发布了自称是在网络入侵期间从学校设备中窃取到的文件，内容涉及到有关大学运营、学生和人员的敏感细节。受到 IT 基础设施损坏所带来的影响影响，医院已取消了部分手术。此外，据法国卫生与预防部消息，受 IT 基础设施遭勒索软件攻击的影响，法国一些医院被迫取消了部分手术，甚至导致多名患者不得不从这些医院的重症监护室转移到其他医疗机构。

而 UDE 方面已确认收到了攻击且已知晓数据泄露问题。但坚称不会向攻击者支付任何赎金。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

icanrestore2022@onionmail.org	icanrestore2022@tutanota.com	icanrestore2022@protonmail.com
jounypaulo@mail.ee	samercin@tutanota.de	datastore@cyberfear.com
azadi3@keemail.me	azadi3@keemail.me	oceannew_vb@protonmail.com
chines34@protonmail.ch	MonaharDecryption@airmail.cc	drk00on@onionmail.org
drk99@onionmail.org	walterwhite@onionmail.org	ithelp02@decorous.cyou
ithelp02@wholeness.business	Brookslambert@protonmail.com	charlefletcher@onionmail.org
Johnatanielson@protonmail.com	Sheppardarmstrong@tutanota.com	emeraldcrypt@onionmail.org
emeraldcrypt@tutanota.com	kat6.l6st6r@aol.com	embog@firemail.cc
sunjun3412@mailfence	sunjun3416@mailfence.com	shadowghost@skiff.com
lastghost@skiff.com	dark_day@cyberfear.com	midnight@email.tg
gardex_recofast@zohomail.eu	icanrestore2022@onionmail.org	icanrestore@onionmail.org
helipsor2022@proton.me	steven1973douglas@libertymail.net	CryptedData@tfwno.gf
main@paradisenewgenshinimpact.top	fireco@onionmail.com	firecorecoverfiles@msgsafe.io
@firecorecoverfiles	emeraldcrypt@onionmail.org	emeraldcrypt@tutanota.com
cynthia-it@protonmail.com	isannamaria@gmx.com	leonardo@cock.lu
Troll900@tutamail.com	redalert@techmail.info	redalertsupp@airmail.cc
robinhood@countermail.com	ryuhb12@protonmail.com	support24@firemail.cc
ftsbk@protonmail.com	rapidorecovery@protonmail.com	sifremialayim@cock.li
datawarehouse@inbox.ru	unlockm301@cock.li	bitlander@armormail.net
trimak@cock.li	tracks@keemail.me	grander123@tutanota.com
grander123@protonmail.com	eject24h@protonmail.com	donaldmorales@protonmail.com
donaldmorales@airmail.cc	dashboard666@mail.com	recoverycode@protonmail.com
donaldmorales@onionmail.org	donaldmorales@gmx.com	helpyoubus11@tutanota.com
helpyourdesk11@protonmail.com	dataware.house@mail.ru	kodal666@inbox.ru
money112@inbox.ru	dataver666@mail.ru	andorambulance@protonmail.com
andorambulance@tutanota.com	steven1973douglas@libertymail.net	MarlonBrando9256@gmx.com
icanrestore@onionmail.org	torres@proxy.tg	azadi33@smime.ninja
drk00on@onionmail.org	justdoit@onionmail.org	justdoit@msgsafe.io

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软件家族越来越多，勒索软件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软件家族占比，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）。

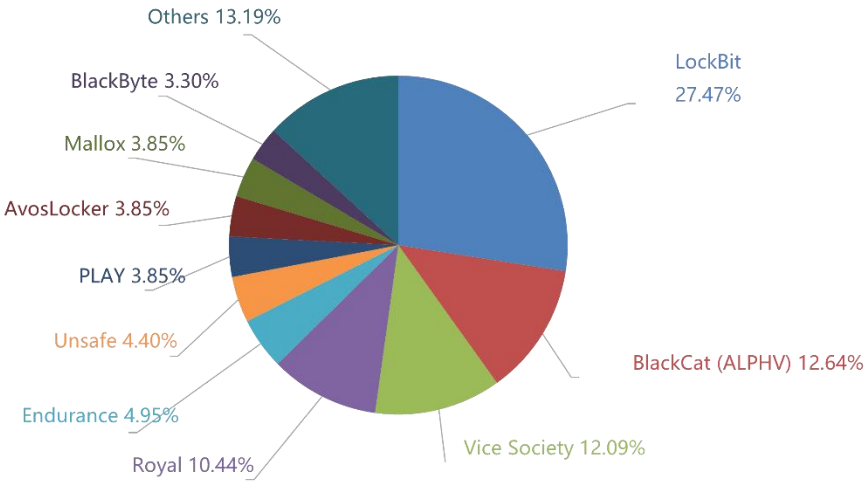

图 6. 本月双重/多重勒索软件家族占比

以下是本月被双重勒索软件家族攻击的企业或个人。未发现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 182 个组织/企业遭遇勒索攻击，其中包含在本月遭遇了双重勒索/多重勒索的 3 个中国组织/企业。此外，有 4 个组织/企业未被标明，因此不在以下表格中。

TechInsights	Societa Italiana Brevetti SpA	geraardsbergen.be
2cara.fr	tcels.or.th	parkavedoors.com
Okanagan College	municipality of Torre del Greco	Scheppersinstituut Wetteren
fujikura.co.jp	wealthwise.com.au	fritsche.eu.com
luacesasesores.es	perenitysoftware.com	thermal.com
cm-vimioso.pt	cplindustries.co.uk	bulldoggroupinc.com
airalbania.com.al	dsavocats.com	itsservicios.com.mx
juvaskin.com	kvie.org	NPTC Group of Colleges
azliver.com	Seguros Equinoccial	ylresin.com
Portnoff Law Associates	Helicar	EGR
Westmont Hospitality Group	Ultrabulk	sdfsdf.dfg
Wesco Turf	Bristol Community College	CDER

SUNY Polytechnic Institute	Travis County Sheriffs Officers Association	ServiceMaster
CHARLES P VONDERHAAR CPA	IOC	SOLAR INDUSTRIES INDIA
Somacis	Crescent Crown Distributing	ADMIRAL Sportwetten
Navnit Group	merlinpcbgroup.com	Copper Mountain
BOMCALCADO	IFPA	First International Food co Ltd
flatironssolutions.com	xlntinc.com	elsan.care
Ucar	CloudCall &emoney Home Loans	ibb-business-team.de
miguelmechanical.com	payroll2u.com	Pillar Resource Services
HRL Technology Group	Barakat Travel Co	A
Cadmet	Guardian Analytics (US)	Monmouth College
Global Mining Products	Buckeye Packaging	NextGen
Fresh Del Monte	Pharmacare	tvk.nl
duomed.com	Alhambra-Eidos	CHARTER COMMUNICATIONS
K Azarosian Costello	Livingston	carinya
R C Stevens Construction	Memtech Acoustical	ARC
Autodelta	Westsächsische Hochschule Zwickau	University of Duisburg-Essen
atcuae.ae	politriz.ind.br	melody.com.tr
Yayla Enerji Uretim Turizm ve Insaat Ticaret	ak.com.sa	fulfilmentmatters.co.uk
Hills Salvage and Recycling	Samuels and Son Seafood	El Seif Development
Holovis	matrixschools.edu.my	Central Texas College
TIMco	K2 Sports	G.W. Becker
fujikura-electronics.co.th	NYCBAR.ORG	EDx.org
Trans Maldivian Airways	Fu Yu Corporation	Air Comm Corporation
IMI Hydronic Engineering	lloyddowson.co.uk	muellergartenbau.ch
lidestrifoodanddrink.com	versteden.com	nuxe.com
russellfinex.com	Physician Partners of America	Ruhrpumpen
Chinery and Douglas	T A Supply	DAYTON PROGRESS
Liebra Permana	TIME TECHNOPLAST LIMITED	Honey Lady
Arnold Clark	circlevillecourt.com	ADIVA CO. LTD
Cambian Group	datair.com	Fire Rescue Victoria
Chestertons Inc.	Thor Specialties, Inc.	Shelco
CARS.com	Aviacode	River City Science Academy
Arizona Labor Force	asianrecorp.com	Koo Wee Rup Secondary College
millennia.pro	Fruttagel	Buffco Production, Inc.
Grupo Estrategas EMM	Pendulum Associates	Duty Free Philippines
Swift Academies	juarez.gob.mx	100x100banco.com
takamiya.co	Park View	Bay Area Rapid Transit
City Lit	LEK / HABO	AT&T

Consulate Health Care	Bevolution Group	PROQUINAL Spradling Group
Sub-drill Supply	LetMeRepair	BOLD
Zety	MyPerfectResume	LiveCareer
LinkedIn	Hayward	Kansas City Homes
Ellison Technologies	DSBJ	Corporate Interiors Inc
CGMLLC.NET	UNISALLE.EDU.CO	CAPMC
Aeronautics company Canada | UTC Aerospace Systems, Bombardier, NASA partners	telarespg.com	Dental One
Nexon Asia Pacific	G.R. Sponaugle	Horwitz Horwitz & Associates
Wings Etc	Dooly County School System	Whatcom County Library System
The Chedi Muscat		

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，目前已加入黑客入侵防护功能。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。

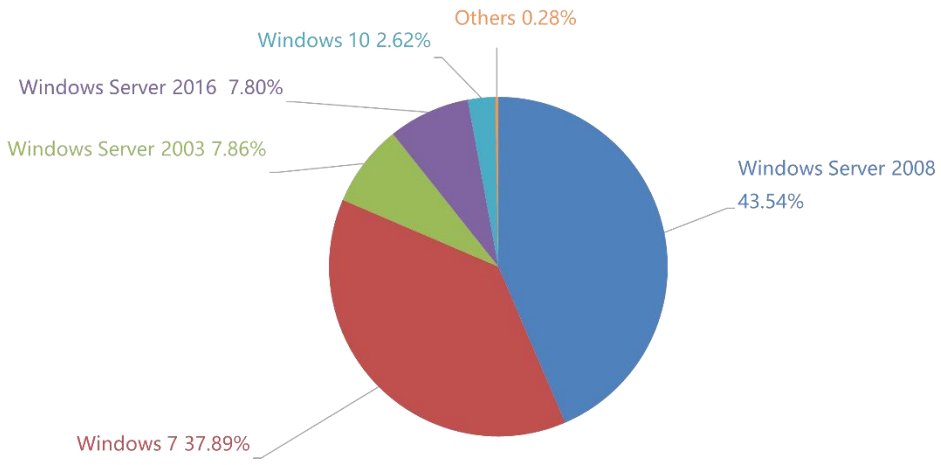

图 7. 本月受攻击操作系统占比

对 2023 年 1 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。

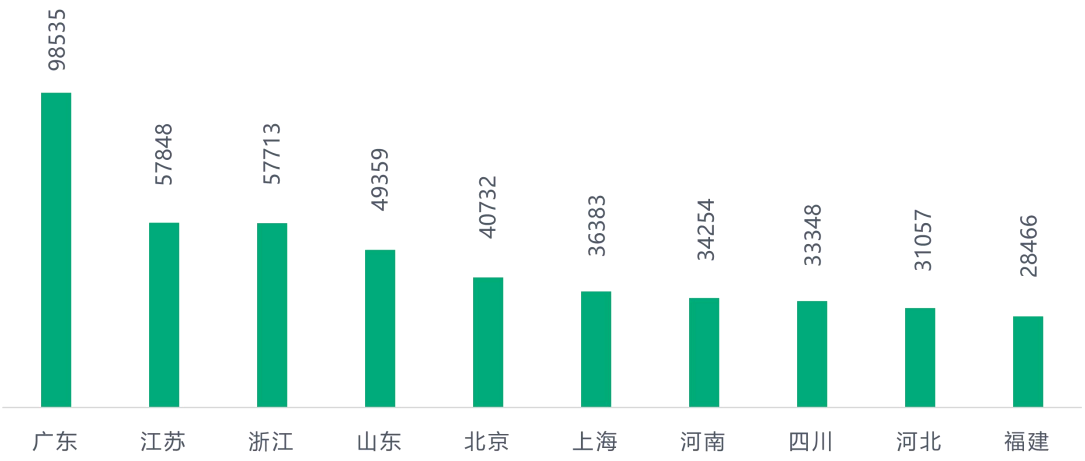

图 8. 本月国内受攻击地区 Top10

通过观察 2023 年 1 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。

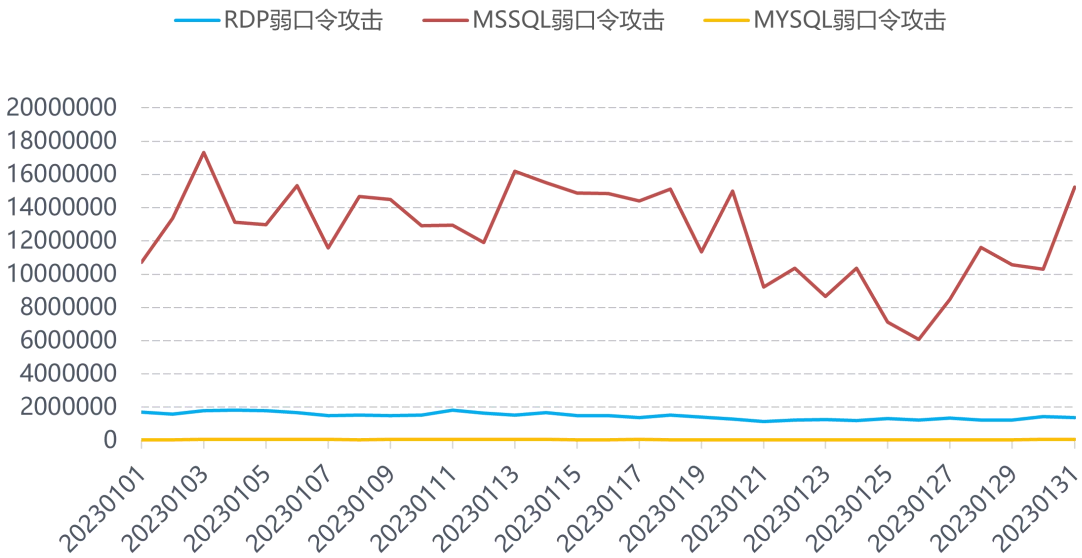

图 9. 本月弱口令攻击量态势

勒索软件关键词

以下是本月上榜活跃勒索软件关键词统计，数据来自 360 勒索软件搜索引擎。

- 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 勒索软件家族，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 勒索软件家族，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 TargetCompany(Mallox)勒索软件家族，由于被加密文件后缀会被修改为 mallox 而成为关键词。主要通过暴力破解远程桌面口令成功后手动投毒和 SQLGlobeImposter 渠道进行传播。此外 360 安全大脑监控到该家族曾通过匿影僵尸网络进行传播。

- mkp：属于 Makop 勒索软件家族，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。

- Encrypt：属于 ech0Raix 勒索软件家族，由于被加密文件后缀会被修改为 encrypt 而成为关键词，该勒索软件家族主要针对 NAS 设备发起勒索攻击，不仅会爆破破解桌面协议还会利用 NAS 设备系统漏洞进行攻击。

- elbie：同 devos。

- eking：同 devos。

- Locked： 属于 TellYouThePass 勒索软件家族，由于被加密文件后缀会被修改为 locked 而成为关键词。该家族主要通过各种软件漏洞、系统漏洞进行传播。

- Xollam：同 mallox。

- milovski：同 mallox。

- faust：同 devos。

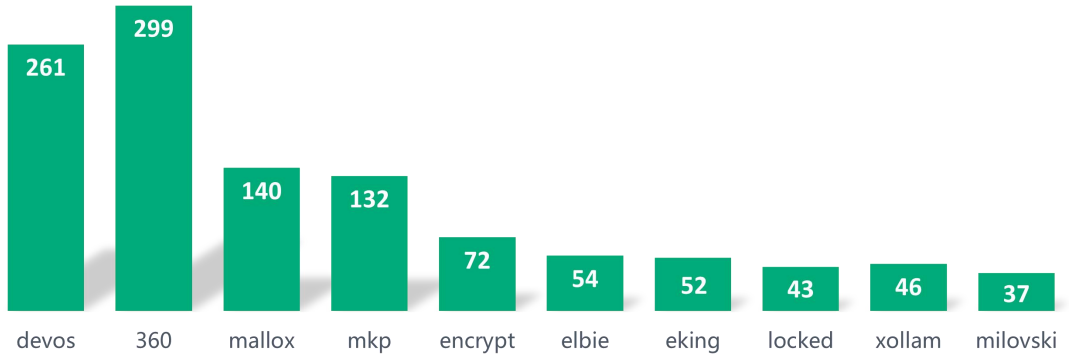

图 10. 360 勒索软件搜索引擎本月搜索量 Top10

解密大师

从解密大师本月解密数据看，解密文件数量最大的是 Sodinokibi，其次是 GandCrab。而从解密的设备量来看，解密最多的是被 Stop 家族加密的设备，排在其后的则是被 Crysis 家族加密的设备。

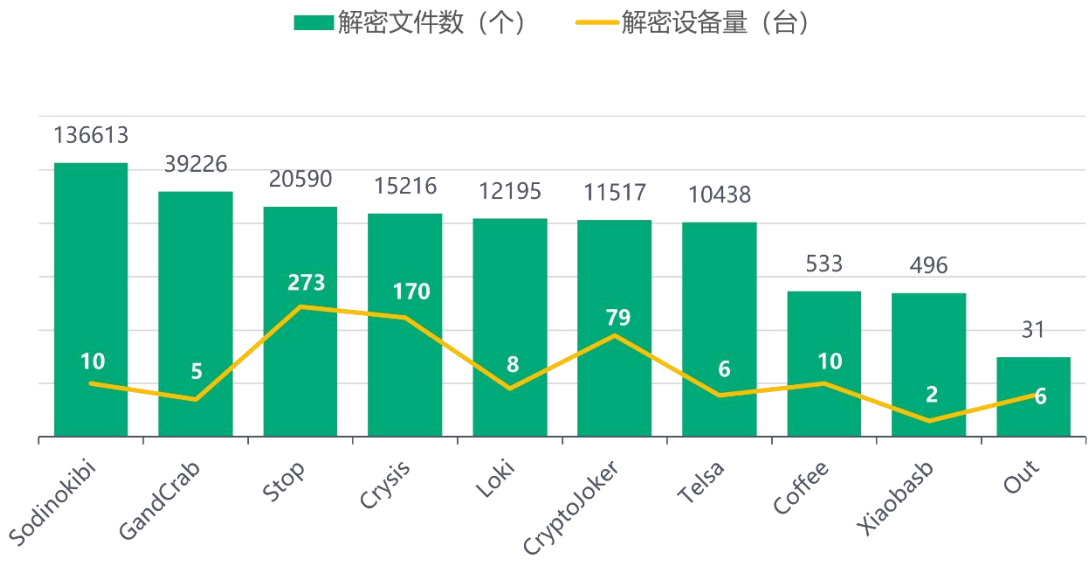

图 11. 360 解密大师本月解密量 Top10

数 字 安 全 的 领 导 者