2022年10月勒索软件态势分析

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。

2022年10月,全球新增的活跃勒索软件家族有: SexyPhotos、Prestige、Ransom Cartel、Azov等家族。其中SexyPhotos与Azov均为擦除器类勒索软件，他们分别借助色情网站和广告程序进行有针对性的传播和攻击；Ransom Cartel勒索软件则被怀疑是REvil勒索软件家族的最新变种；而Prestige则是较为传统的文件加密行勒索软件，据研究人员分析发现该软件与此前流行一时的HermeticWiper擦除器勒索软件的攻击目标高度重叠。此外OldGremlin黑客组织在本月的攻击中加入了针对Linux系统的勒索软件部署，该组织曾在今年早些时候的攻击活动中向受害者开出了高达1690万美元的高额赎金。

以下是本月值的关注的部分热点：

一、白宫召集第二届国际反勒索攻击峰会，37国共同参与

二、BlackByte勒索软件利用合法驱动程序禁用安全产品

三、勒索软件攻击导致某些德国报纸停刊

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

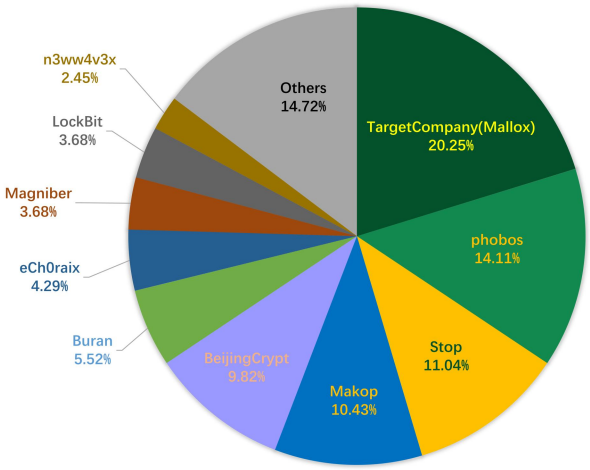
针对本月勒索软件受害者所中勒索软件家族进行统计，TargetCompany(Mallox)家族占比20.25%居首位，其次是占比14.11%的phobos，Stop家族以11.04%位居第三。

前两个月较为流行的TellYouThePass在本月已经销声匿迹，取而代之的则是TargetCompany(Mallox)家族。虽然TargetCompany(Mallox)并没有出现较大规模的爆发，但其流行度的增长势头也需要企业管理员提起重视。

而phobos作为国内老牌勒索家族，流行热度一直比较高，主要通过暴破远程桌面传播。

Stop勒索软件虽然近期传播量有所下降，但始终保持传播热度，再其它家族未有明显攻势情况下，该家族再次进入前三，目前尚属于正常的浮动范围。

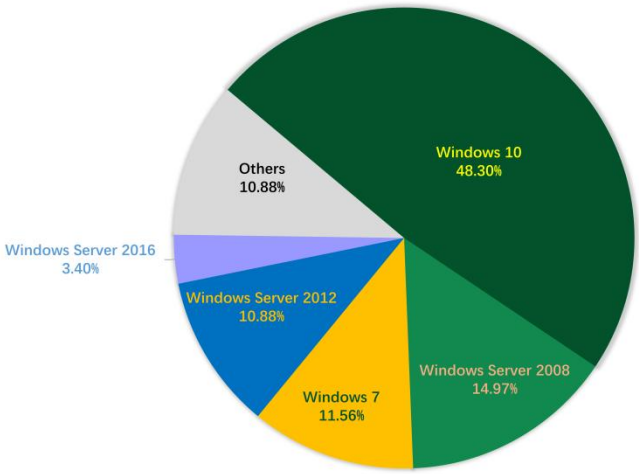
2022年10月反勒索服务处置勒索病毒家族占比



数据来源：360反勒索服务

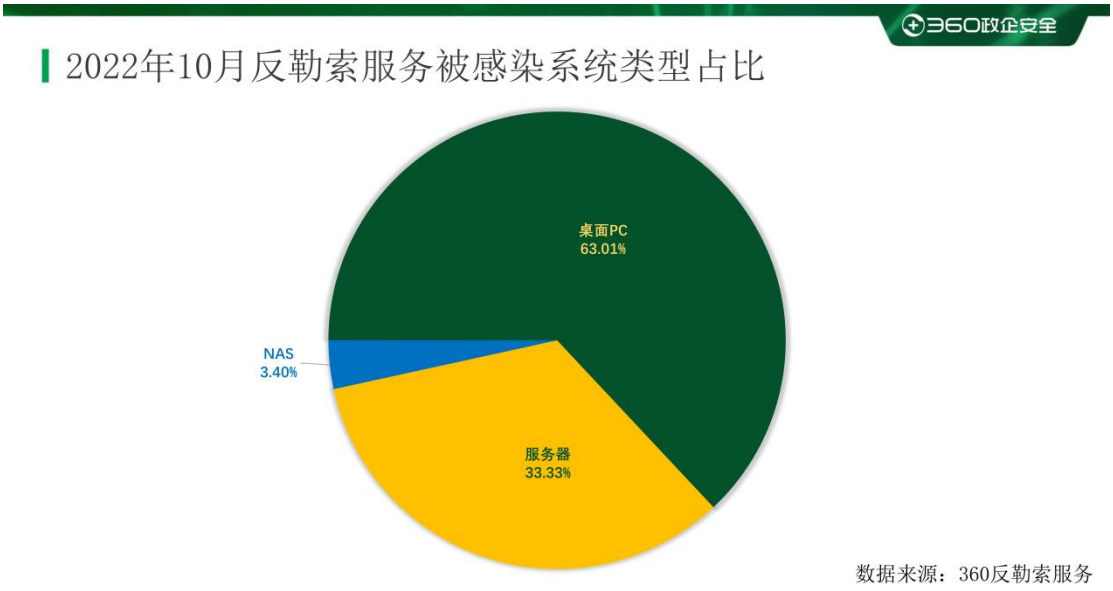
对本月受害者所使用的操作系统进行统计，位居前三的是：Windows 10、Windows Server 2008 以及 Windows 7。

2022年10月受勒索病毒影响操作系统占比



数据来源：360反勒索服务

2022 年 10 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。



数据来源：360反勒索服务

勒索软件疫情分析

白宫召集第二届国际反勒索攻击峰会，37 国共同参与

美国当地时间 10 月 31 日至 11 月 1 日,美国协同其他 36 个国家以及 13 家企业及组织,在华盛顿白宫举行了第二届国际勒索软件倡议（CRI）峰会，以研究如何更好地打击勒索软件攻击。会议再次强调，勒索是一个全球性问题，在信息化之路上，没有一个国家能独善其身。

在会后的联合声明中，成员国共同表示，将提升对勒索威胁的共同抵抗能力，行动包括:

打击勒索相关的虚拟货币及其服务商施行反洗钱和打击资助恐怖主义措施,打击勒索软件攻击者从中获得非法利益，以及制定和实施反洗钱和打击资助恐怖主义加密标准。。

跨国合作，共同打击勒索犯罪，不为勒索攻击者提供庇护。

分享有关勒索的相关情报信息，帮助盟友应对勒索威胁。

BlackByte 勒索软件利用合法驱动程序禁用安全产品

BlackByte 勒索软件团伙正在使用白驱动利用的技术来协助传播，该技术通过正常驱动程序来禁用各种安全软件驱动程序，干扰安全软件运行，以此绕过保护系统。

该组织最近的攻击涉及 MSI Afterburner RTCore64.sys 驱动程序的一个版本，该版本存在 CVE-2019-16098 漏洞的代码执行攻击。利用该安全问题，BlackByte 尝试禁用了数千个安全软件驱动。近期另外两个值得注意的此类攻击案例包括 Lazarus 滥用有漏洞的 Dell 驱动程序和未知黑客滥用 Genshin Impact 游戏的反作弊驱动程序。

勒索软件攻击导致某些德国报纸停刊

德国报纸《Heilbronn Stimme》于 10 月 15 日遭到勒索软件攻击并被破坏了印刷系统后，其以电子版形式发布了后续的期刊。

10 月 16 日，该报发布了一个“紧急”六页版公告，所有原本要发行的报纸均改为线上发布。16、17 日两天，其电话和电子邮件通信均仍处于离线状态。该报纸的发行量约为 75000 份，但由于此次攻击事件引发的印刷问题，其已暂时取消了官网的付费渠道。而其网站每月约有 200 万访问者。

报社主编 Uwe Ralf Heer 表示：此次攻击影响了整个 Stimme Mediengruppe 媒体集团，包括旗下的“Pressedruck”、“Echo”和“RegioMail”等公司。而发行量为 25.4 万份的 Echo 也受到了网络攻击的影响，导致读者在其网站中访问电子文件时出现了问题。不过其在线新闻门户网站 Echo24.de 目前仍在正常运行。

Heer 主编还表示攻击者已经留下了勒索信息，但尚未提出具体的赎金金额。

Dank des sonnigen Sommers fahren Imker eine bessere Honig-Ernte ein als im Vorjahr. Seite 7

Zweimal Buga, viel gemeinsam: Was die Konzepte in Mannheim und Heilbronn verbindet. Seite 22

Im Blickpunkt

Interview: Jörg R. Wingerter über Selbstverteidigung im Wing Tsun. Seite 4

HEILBRONNER STIMME

www.stimme.de

Montag
17. Oktober 2022

Zeitung für die Region
Heilbronn-Franken
Hohenlohe
Kraichgau

Nr. 240 · 2,40 Euro

Bundespräsident empfängt Erntekrone in Hohenlohe

Schöntal Bundespräsident Frank-Walter Steinmeier hat am Sonntag in Kloster Schöntal die Erntekrone in Empfang genommen. Der Deutsche Bauernverband hatte Baden-Württemberg und Hohenlohe für die Übergabe auserkoren, die zum Erntedank in wechselnden Bundesländern stattfindet. Die Hohenloher Kreislandfrauen um Regina Müller (links) hatten die Erntekrone auf dem Bauernhof von Jürgen Maurer in Kupferzell-Feßbach (rechts) gebunden, der Vorsitzender des hiesigen Bauernverbands ist. Foto: Mario Berger/Seite 24

Meinung

Von Michael Schwarz

Oppositionsarbeit ist wichtig, reicht aber in der CDU nicht aus, findet unser Autor.

Erneuerung

Trotz der globalen Krise müssen politische Akteure und die Basis der Parteien motiviert bleiben. Denn wer den Kopf in den Sand steckt, ist politisch handlungsunfähig. Unter dieser Prämisse ist auch der Landesparteitag der Südwest-CDU in Villingen-Schwenningen zu bewerten. Parteichef Friedrich Merz hielt eine gute und für die Delegierten motivierende Rede. Auch Landeschef Thomas Strobl gelang es, trotz Brief-Affäre und Untersuchungsausschuss, die Basis auf die nächsten Monate einzustimmen. Dabei hatten die beiden führenden Köpfe der Partei auf Bundesebene und im Südwesten leichtes Spiel: Der Dauer-Streit in der Berliner Ampelkoalition bietet viel Angriffsfläche.

Allerdings muss die CDU den eigenen Erneuerungsprozess fortsetzen. Denn der ist dringend nötig, im Bund wie im Südwesten, wo Landtagsfraktionschef Manuel Hagel als der Kopf der Zukunft gilt. Ihm ist es gelungen, die CDU-Parlamentarier hinter sich zu einen. Dabei kommt ihm die Brief-Affäre Strobls ungelegen. Denn solange der Heilbronner die Partei in Ruhe führt, kann sich Hagel auf die parlamentarische Arbeit konzentrieren. Käme es zum Rückzug Strobls, müsste Hagel nach dem Parteivorsitz greifen. Doch eine Doppelfunktion in Partei und Fraktion würde den Druck auf den 34-Jährigen immens erhöhen.

@ Ihre Meinung?
michael.schwarz@stimme-mediengruppe.de

Regierung sucht weiter Lösung im Atom-Streit

Grüne Basis bestärkt Minister bei Bundesparteitag

BERLIN/BONN Im Koalitionsstreit der Bundesregierung über die weitere Nutzung von Atomkraftwerken wächst der Zeitdruck, doch eine Lösung zeichnete sich vorerst nicht ab. Die Grünen bestätigten die Position ihrer Parteiführung am Wochenende formal auf einem Parteitag. FDP-Finanzminister Christian Lindner warnte hingegen vor roten Linien. Die SPD hielt sich mit einer eigenen Positionierung weiter zurück. Bundeskanzler Olaf Scholz (SPD), Grünen-Wirtschaftsminister Robert Habeck und Lindner trafen sich am Sonntag, um nach einem Ausweg zu suchen. Nach Informationen der dpa wurde eine Fortsetzung der Gespräche für Montag vorbereitet. SPD-Parlamentsgeschäftsführerin Katja Mast rief zu „gesundem politischen Pragmatismus“ in der kommenden Zeit auf. *dpa* Seite 3

Auswirkungen der Cyber-Attacke

HEILBRONN *Stimme-E-Paper erscheint, Druck noch nicht möglich – Ermittlungen der Polizei laufen*

Von unseren Redakteuren Uwe Ralf Heer und Jürgen Kümmerle

Nach dem Cyber-Angriff auf die *Stimme Mediengruppe* sind die Auswirkungen weiterhin gravierend. Ein Cyber-Interventionsteam arbeitet gemeinsam mit der IT der Mediengruppe an der Wiederherstellung der Systeme. Am Sonntag wurde der Versuch unternommen, ein E-Paper zu erstellen. Der Druck der Tageszeitung war für die Montagsausgabe nicht möglich. Wann wieder eine Zeitung gedruckt werden kann, ist derzeit noch nicht absehbar.

Auch das Verteilen der Freudzeitungen, wie „Süddeutsche Zeitung“ oder „Stuttgarter Zeitung“, musste entfallen. Das *Stimme*-E-Paper ist dagegen für alle Kunden über www.stimme.de frei zugänglich. Nach der Cyber-Attacke am frühen Freitagmorgen sind weite Teile der *Stimme Mediengruppe* lahmgelegt. Neben der Tageszeitung sind auch Regiomail, der Pressedruck sowie das Echo betroffen. Die Online-Angebote auf www.stimme.de und www.echo24.de konnten dagegen von den Reportern und Autoren weiter aktuell bestückt werden. Hier findet sich rund um die Uhr die übliche aktuelle Berichterstattung aus allen Ressorts über alle Geschehnisse. Die Bezahlschranke bei *Stimme.de* ist vorerst ausgesetzt.

Foto: VideoFlow/stock.adobe.com

Notausgabe Am Samstag erschien eine sechsseitige Notausgabe, in der die Öffentlichkeit über die Ereignisse informiert wurde. Diese Notausgabe wurde bei der Brettener Woche produziert, anschließend in Karlsruhe gedruckt und schließlich im Laufe des Samstags an alle Haushalte im Stadt- und Landkreis Heilbronn sowie im Hohenlohekreis verteilt.

Seit dem frühen Freitagmorgen arbeiten Mitarbeiter der IT der *Stimme Mediengruppe* mit einem Sicherheitsunternehmen aus München rund um die Uhr an der Wiederherstellung der Systeme. IT-Experte Florian Oelmaier erklärt: „Der Wiederaufbau einer IT ist kein Sprint, sondern ein Marathon.“

Die Polizei ermittelt, nähere Erkenntnisse liegen bislang noch nicht vor.

Die Redaktion konnte am Sonntag arbeiten und dieses vereinfachte E-Paper produzieren. Eine Aktualisierung – vor allem der abendlichen Sportereignisse – war nicht möglich. Zudem konnten keine unterschiedlichen Lokalteile erstellt werden. Es gibt daher ein 28-seitiges E-Paper mit einheitlichem Lokalteil.

Kurios

1000 Teddys für die Queen

LONDON Königin Elizabeth II. hatte einen besonderen Draht zur Kinderbuchfigur Paddington Bär. Ein Videoclip zu ihrem 70. Thronjubiläum mit dem Bär hat Kultstatus. Nach dem Tod der britischen Königin wurden neben Blumen auch über

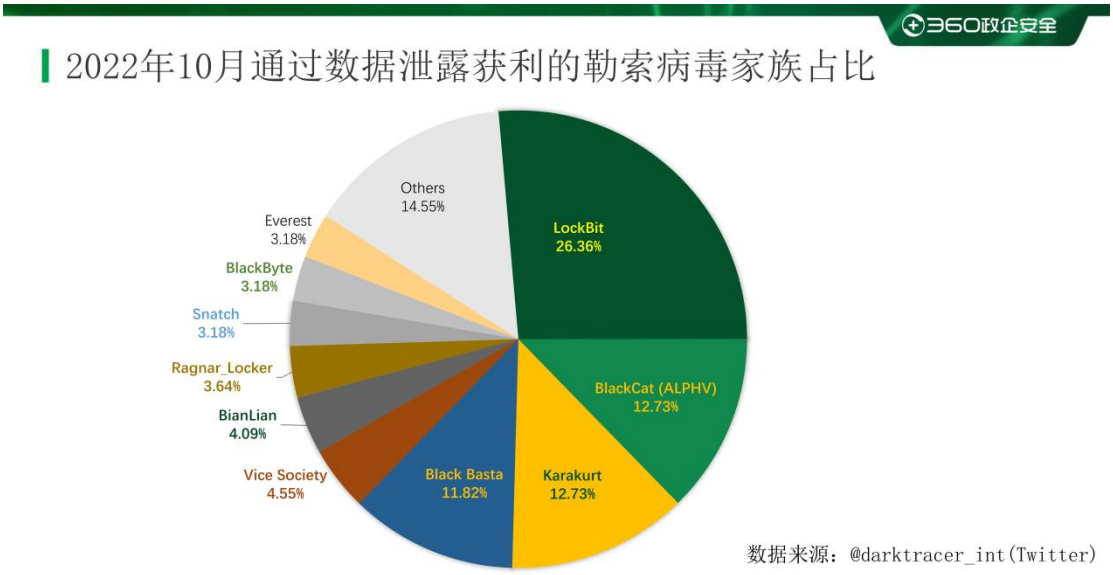
黑客信息披露

以下是本月收集到的黑客邮箱信息：

ryzen@cyberfear.com	MyFile@waifu.club	datanewsok@tutanota.com
elmorenolan@tutanota.com	nergontr96@cyberfear.com	alco2022decoding@onanmal.com
xats@privatemail.com	idemitsu122@cyberfear.com	helprequest@techmail.info
integra2022@tutanota.com	rast@airmail.cc	dupuisangus@aol.com
regyhny@tutanota.com	sikfotrisd@tutanota.com	WrwLx3jZaG@proton.me
decryp@tutanota.com	idemitsu122@cyberfear.com	tomas1991goldberg@cock.li
st3v3njansen@onionmail.org	tugruldams@onionmail.org	idemitsu122@cyberfear.com
dataservice@nigge.rs	datahelp112233@mailfence.com	eonardoboss@onionmail.org
sunhuyvchay@messagesafe.io	backshow@my.com	Backshow@tutanota.com
integra2022@tutanota.com	recoverydata@onionmail.org	ryzen@yberfear.com
hope2honest@aol.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）。



以下是本月被双重勒索软件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 220 个组织/企业遭遇勒索攻击，其中包含中国 5 个组织/企业在本月遭遇了双重勒索/多重勒索。

Genesys Aerosystems	Bitron	Var Group
thalesgroup.com	HENSOLDT France	santimuni.com
coopavegra.fi.cr	will-b.jp	happmobi.com.br
bellettiascensori.it	exco.fr	cacula.com

aaanchorbolt.com	seamlessglobalsolutions.com	close-upinternational.com.uy
macrotel.com.ar	zurifurniture.com	byp-global.com
sociedadbilbaina.com	gruposanford.com	hoosierco.com
lincare.com	railway.gov.tw	saurer.com
Kolas Law Firm	Network Communications Inc	Asahi Group
fvsra.org	greenstamp.co.jp	Kujalleq Municipality
The Bishop of Hereford's Bluecoat School	Rankam	AT&T
R1 Group	Qualified Staffing	Bergamo Metal
Medilife Hastanesi	ipb Baggenstos Montagen	Miracapo pizza company
steelesolutions.com	unipiloto.edu.co	tiffinmetal.com
DURAVIT A.G.	Comando Conjunto de las Fuerzas Armadas Del Ecuador	CCLint
Municipio de Chihuahua	Vercity	Özel GözAkademi Hastanesi
Associated Lighting Representatives	CADEPLOY	sskb.com.au
Ethigen Limited	APECQ	Cromwell Management Inc.
Tata Power	Club Asteria Belek	Davenport Community School
South Jersey Glass & Doors	bfw	pendragonplc.com
Kenosha Unified School District	rjyoung.com	mdaemon technologies
UNE	covisian.com	Lightbank
Diamond Mowers	Pitman Family Farms	LIBERTY PULTRUSIONS
Metroclean	Egyptian Electric Cooperative Association	EDC3
J.M. Rodgers Co.	ALRO	STONE1
Maternite des Bluets	TSC	ESSICKAIR
METASYS	A G Equipment Company	Legend Holdings
KEMET	DIPF-INTERN	Dollmar SpA
Weidmuller	Latitude 37	Rosenblatt Securities
Wes-tec inc.	Cheval Electronic Enclosure	Unimed Belem
Dialogsas	Ville-chaville	BOOTZ
Bilthoven Biologicals	KINSHOFER GmbH	kingfisherinsurance.com
HUSSEY GAY BELL	Murphyfamilyventures	Döhler
tokaisolidtire.com	castemark.tw	kingteam.com.tw
eeckman.eu	Quantumce.com	centurion.com.pl
oomiya.co.jp	groupesavoie.com	eureka-puzzle.eu
Air Defense Solutions company	mk.co.th	tamhash.co.il
heronconstruction.co.nz	villajuris.be	kilvington.vic.edu.au
bankruptcypa.com	API MDC Technical Research Centre Sdn Bhd	Aerotech Precision Manufacturing
Wellington College Hangzhou	Canny Elevator Co Ltd	RecordTV
Jam Filled Entertainment	nelsonautohaus.com	ZIGI NY
www.projectredirectdc.org	CSW GmbH	ALFATECH

AMPORTS	martel.es	Michael Sullivan & Associates
SMART Mechanical Solutions	Quality Telecom Consultants Inc	bigcenters.rs
mtrx.com	Hiersun Jewelry Co Ltd	Infinitum
Energy Transfer Durafin Tubes	Consorci Sanitari Integral & Geseme	Regulatory Authority for Telecommunications and Posts (ARTP)
Municipalidad de belen	TMShipping	HALYVOURGIKI.S.A.
Marist College Ashgrove	Pate's Grammar School	Test Valley School
Mars Area School District	The Hibbert Group	DMCI Holding
marktel.es	Cloud Gaming GeForce | NVIDIA GeForce NOW	tdwood.com
jtchapman.com	polycube.co.th	dmcinet.com
Shiloh Industries	RS.GOV.BR	securityalliancegroup.com
dragages-ports.fr	alliedusa.com	cedemo.com
buydps.com	Município De Loures	ROFA INDUSTRIAL AUTOMATION
ADATA Technology	Severn Glocon Group	Home Dynamix
Deutsche Saatveredelung AG	Notos Com	Electricity company
Bevolution Group	SPERONI S.P.A	Circles of Care
Clarion Communication Management Ltd	Knoll	Pinnacle Incorporated
MERCOLA	ScinoPharm Taiwan	Robert Bernard
Contempo Card	Lojas Torra	EMTELCO
Dialog Information Technology	Rundle Eye Care	MARCELSOLUTION.COM
OPPLE Lighting	Empower Insurance	Unicity
Oil India Limited	Avalon luxury transport	Willemen Group
apunipima.org.au	apunipima.org.au	National Stores Inc.
Batesville Products	APSM Systems	Peter Duffy Ltd
Sunflower Farms Distributors, Inc	Aarti Drugs Ltd	Berg Kaprow Lewis
Feldman, Holtzman & Company, LLC	Läderach	Seanic Ocean Systems
Bartelt	Gate Precast	The UNITED GRINDING Group
Grupo Jaime Camara	ALVAC SA	AudioQuest
Malayan Flour Mills Bhd.	Ferrari	Simex Defence Inc
Aesthetic Dermatology Associates	Almoayed ICT	Swiss American
MultiCare Home Health	CBLSYS.CO.UK	PENDULUM ASSOCIATES
ASSOCIATED RETAILERS LIMITED	ID-ware	NJVC
Midwest Petroleum		

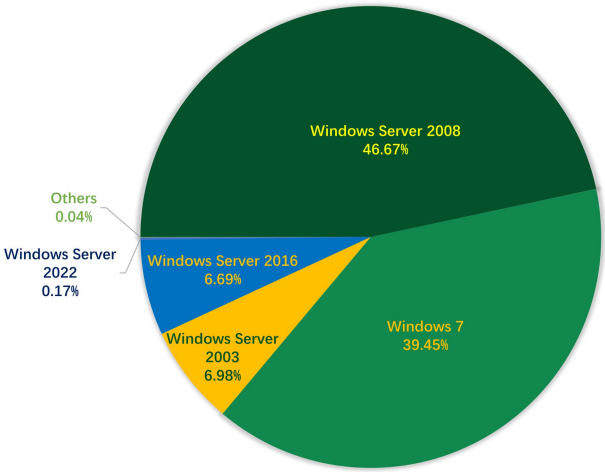
表格 2. 受害组织/企业

系统安全防护数据分析

360 系统安全产品，针对服务器进行全量下发了系统安全防护功能，针对非服务器版本的系统仅在发现被攻击时才下发防护。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。

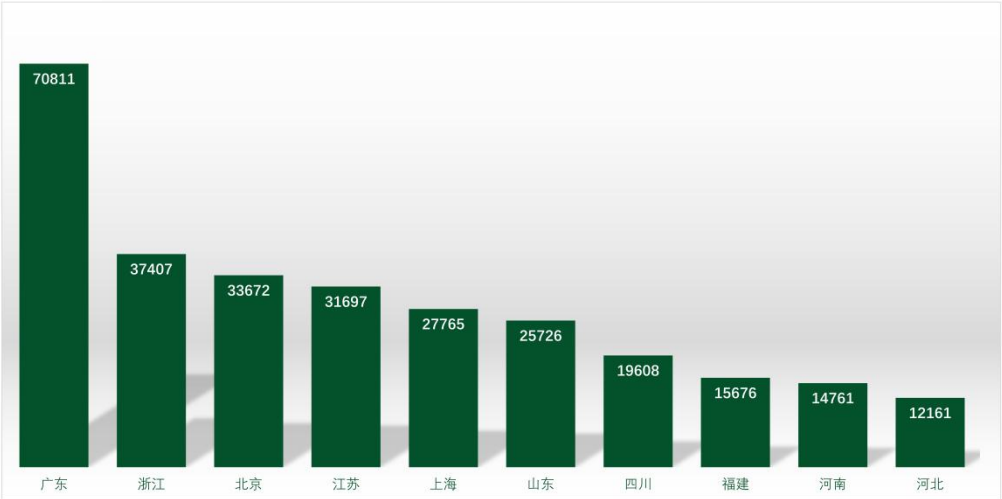
2022年10月弱口令攻击系统占比



数据来源：360反勒索服务

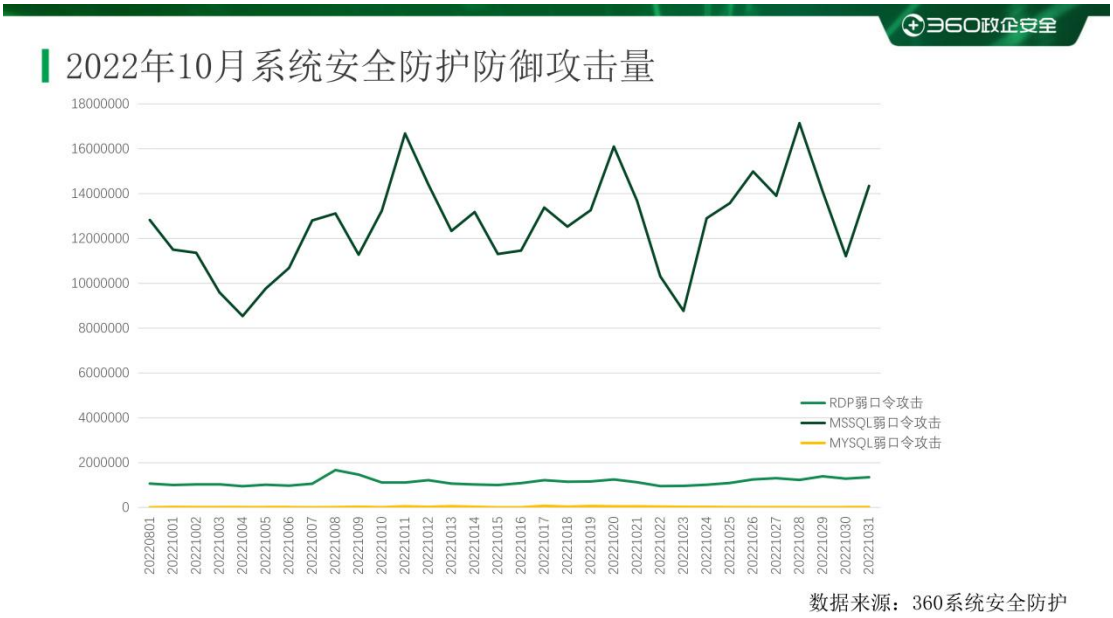
对 2022 年 10 月被攻击系统所属地域统计发现，与之前几个月采集到的数据进行对比，地区排名和占比变化均不大。数字经济发达地区仍是攻击的主要对象。

2022年10月全国被弱口令攻击地区TOP10



数据来源：360系统安全防护

通过观察2022年10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。



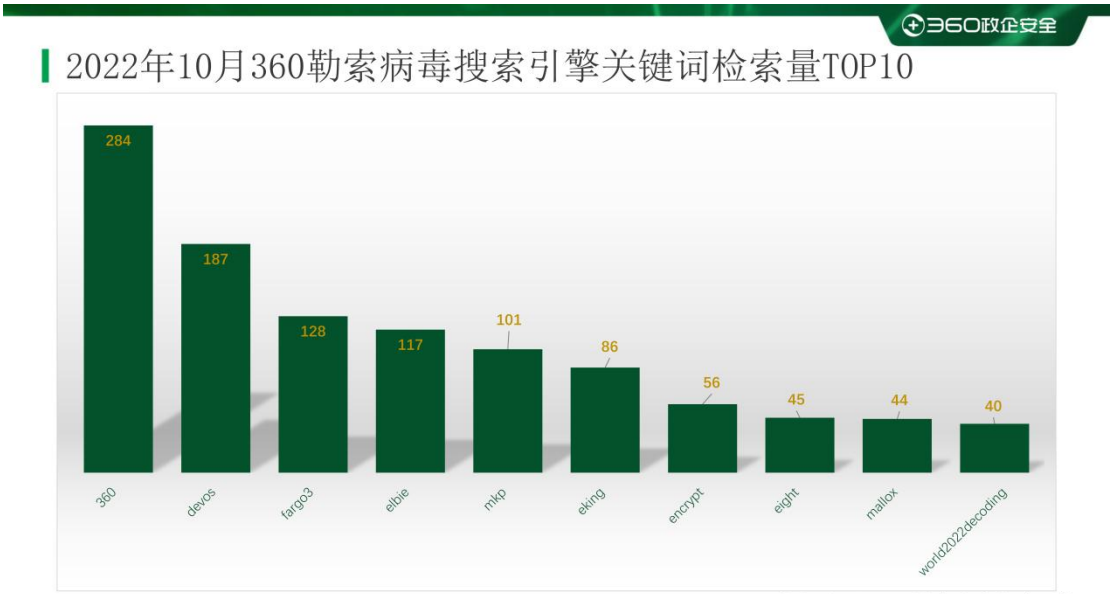
数据来源：360系统安全防护

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。

- 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。
- 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。
- fargo3：属于 TargetCompany(Mallox)勒索软件家族，由于被加密文件后缀会被修改为 fargo3。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和远程桌面弱口令爆破。
- 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。
- elbie：属于 phobos 勒索软件家族，由于被加密文件后缀会被修改为 elbie 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。
- 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。
- eking：同 elbie。
- encrypt：属于 eChOraix 勒索病毒家族，由于被加密文件后缀会被修改为.encrypt 而成为关键词。该家族是一款针对 NAS 设备进行攻击的勒索病毒，主要通过漏洞攻击威联通设备，同时还曾对群辉设备采取桌面弱口令攻击。
- eight：同 elbie。
- 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。
- world2022decoding：属于 Honest 勒索软件家族，由于被加密文件后缀会被修改为

world2022decoding 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。



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 Loki，其次是 Coffee。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(解密文件数较小故未入榜)，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