勒索软件流行态势分析

2023 年 2 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 2 月，全球新增的活跃勒索软件家族有:Masons、DoDo、Vendetta、Medusa 等家族。其中 Vendetta 和 Medusa 是本月新增的双重勒索软件。Medusa 勒索软件本月在暗网公布的受害者数量已多达 19 个，主要针对能源，金融、医疗和交通运输等基础设施行业发起勒索攻击。

以下是本月值的关注的部分热点：

1. 数十家企业中招！360 发布 Paradise 勒索软件预警。

2. ESXiArgs 勒索软件针对全球 VMware ESXi 服务器发动大规模攻击。

3. Lockbit 勒索软件团伙声称对“皇家邮件”发动网络攻击。

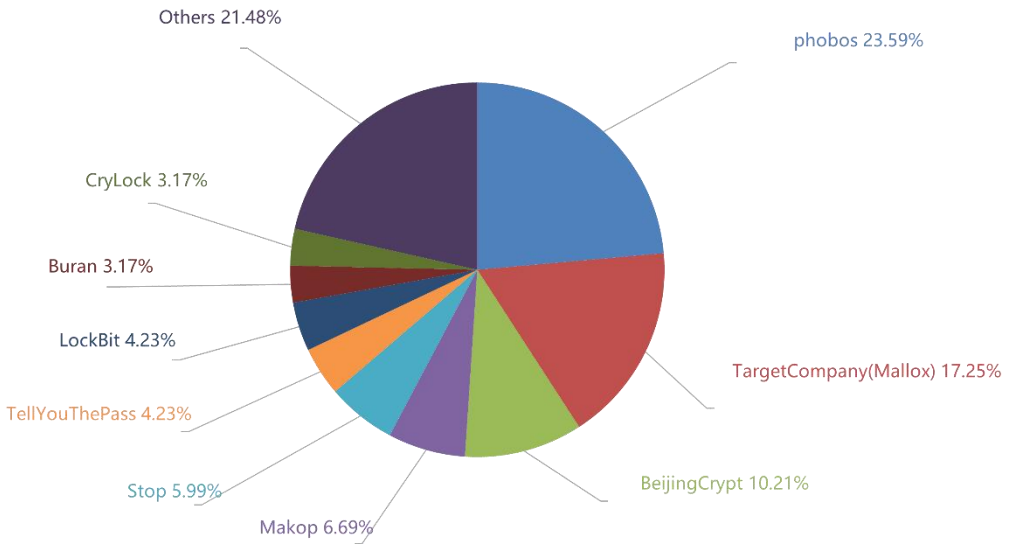
4. HardBit 要求受害者提供保单详情以指定最佳勒索金额。

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。

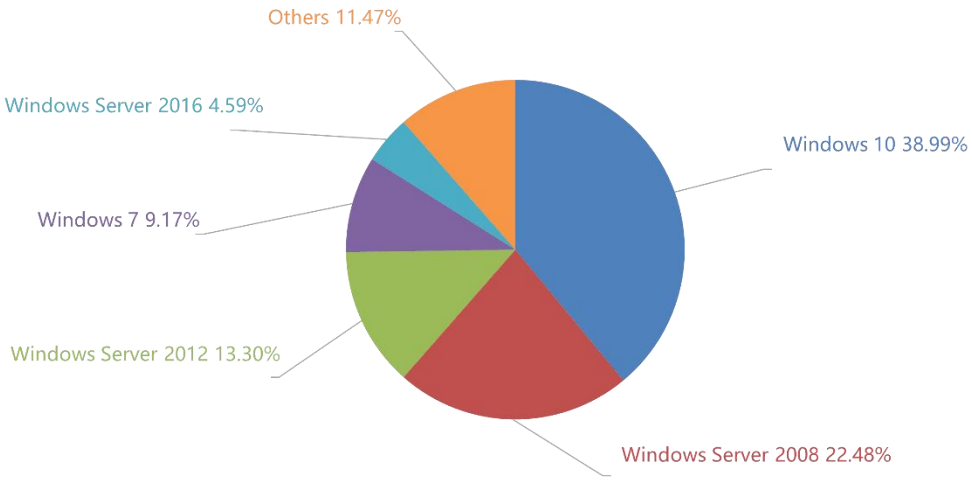
感染数据分析

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 23.59%居首位，其次是占比 17.25%的 TargetCompany(Mallox)，BeijingCrypt 家族以 10.21%位居第三。前三大家族占比超 50%，均为过往的流行家族。

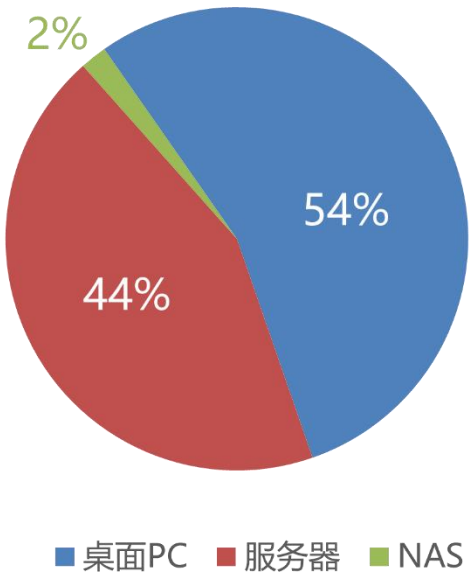
在本月初，Paradise 勒索软件家族通过老版本向日葵软件漏洞下发攻击。



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。



2023 年 2 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。



勒索软件情况分析

数十家企业中招！360 发布 Paradise 勒索软件预警

360 安全大脑监测到，有黑客团伙正在利用向日葵远程控制软件漏洞 CNVD-2022-10270 发起攻击，向目标机器投递 Paradise 勒索病毒。

此次攻击最早发生于 2023 年 1 月 30 日，目前仍在持续，根据 360 安全大脑的监测数据，攻击者对网络中暴露的向日葵远程控制软件进行大范围扫描，并对存在漏洞的向日葵远程控制软件发起攻击，目前已经有数十个目标被攻破并被投递勒索病毒。

受害用户的向日葵远程控制软件日志显示，攻击 IP：45.77.29[.]56 对目标发起攻击，利用漏洞尝试执行多种恶意命令，这些恶意命令用于下载执行 Paradise 勒索病毒并将其写入启动项。此外，攻击者还会向机器投递“永恒之蓝”漏洞利用工具，尝试使用该工具在内网横向移动。

此次攻击所使用的勒索病毒和黑客工具均部署在域名 upload.paradisenewgenshinimpact[.]top 下。

受害用户向日葵远程控制软件日志

攻击发生时进程树

ESXiArgs 勒索软件针对全球 VMware ESXi 服务器发动大规模攻击

近期，大量攻击者对 VMware ESXi 服务器发起攻击，利用两年前被公布的 ESXi 远程代码执行漏洞来部署新的 ESXiArgs 勒索软件，此外新型勒索软件 Royal 也加入到了这一轮针对 ESXi 服务器的攻击当中。本轮攻击所利用的漏洞为 CVE-221-21974，该漏洞因 OpenSLP 服务中的堆溢出现问题而引起，未经验证的攻击者可以轻松利用该漏洞进入用户的服务器系统。

受此漏洞影响的 ESXi 版本为：

ESXi versions 7.x prior to ESXi70U1c-17325551

ESXi versions 6.7.x prior to ESXi670-202102401-SG

ESXi versions 6.5.x prior to ESXi650-202102101-SG

因此，VMware 公司向其客户发出安全警告，提醒用户安装最新的安全更新，并禁用 OpenSLP 服务。此外，VMware 公司还补充说明此次攻击并没有利用未知的 0day 漏洞，而 2021 之后发布的 ESXi 软件版本则已经默认禁用了 OpenSLP 服务。

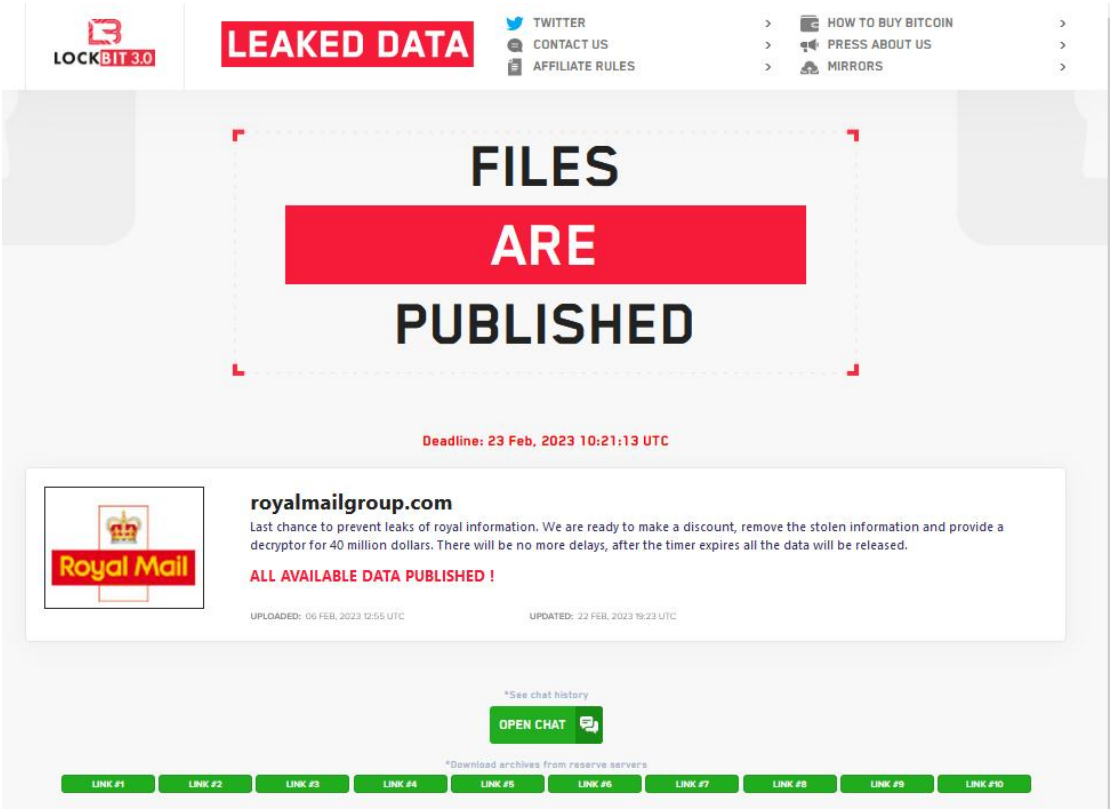
另外，美国网络安全和基础设施安全局（CISA）也公布了针对此次攻击的修复脚本，用于修复被破坏的 ESXi 虚拟机环境。

Lockbit 勒索软件团伙声称对“皇家邮件”发动网络攻击

LockBit 勒索软件组织近期声称对英国的邮件递送服务公司 Royal Mail 受到的网络攻击负责。受害公司也表示因“严重服务中断”而被迫停止其国际航运服务。

此前，该 LockBit 勒索软件团伙曾声称其并没有攻击 Royal Mail。相反，他们将攻击行动归咎于其他团伙使用了其 2022 年 9 月在 Twitter 上泄露的 LockBit 3.0 勒索软件生成器所自行生成的勒索软件。

但近期 LockBitSupp 却又在一个俄语黑客论坛上发布帖子确认，LockBit 确实是此次攻击的幕后黑手——是他们的一个分支机构在 Royal Mail 的系统上部署了该团伙的勒索软件。此外该团伙代表还补充说，他们只会提供一个解密器，并在支付赎金后删除从 Royal Mail 网络窃取的数据。



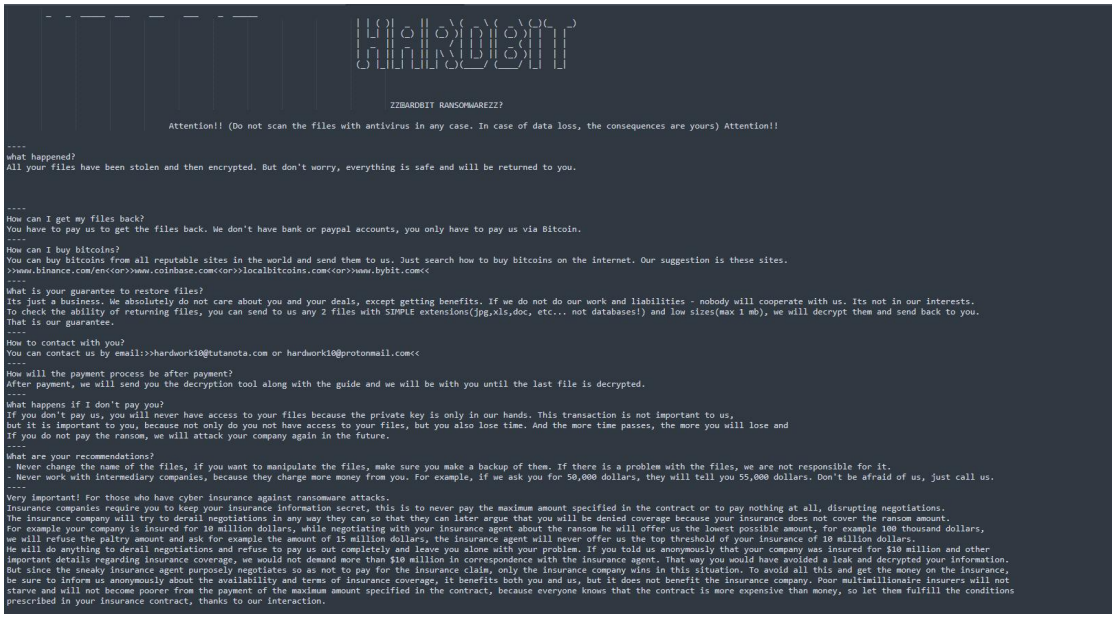
HardBit 要求受害者提供保单详情以指定最佳勒索金额

HardBit 家族勒索软件 2.0 版运营者将其勒索思路从直接勒索受害者转换为从受害者的保险公司获得勒索赎金。

具体方案是：攻击者试图说服受害者告知其为数据或设备所购买的保险详情，并以此为依据来调整他们的赎金要求，以便让保险公司来承担所有赎金费用。

根据分析，HardBit 勒索家族最早被捕获于 2022 年 10 月，而其 2.0 版则于 2022 年 11 月推出，该版本目前仍处于活跃状态。而与现下主流的勒索软件家族不同的是，目前尚未发现 HardBit 的数据泄露站点——尽管其运营团队曾声称窃取了受害者数据并威胁要将这些数据泄露。

而该家族的攻击者则建议受害者不要与中间商合作以徒增支付成本。但对于购买了网络攻击相关保险的受害者，黑客则会有针对性地引导他们披露其所购买的保险金额。更重要的是，黑客还试图将保险公司描绘成阻碍恢复数据的坏人，同时让受害者认为分享保单内容对自身更为有利。



黑客信息披露

以下是本月收集到的黑客邮箱信息：

CryptedData@tfwno.gf	damavand@cock.li	unusualsituation@tutanota.com
torres@proxy.tg	guan_yu@jabber.systemli.org	guan.yu@xmpp.jp
samsamsa@tuta.io	pm24@tuta.io	idostuff@protonmail.com
hardwork10@protonmail.com	Cyber@tfwno.gf	hardwork10@tutanota.com
fireco@onionmail.com	leljicok@gmail.com	kkizuko@yandex.com
RootOpen@airmail.cc	firecorecoverfiles@msgsafe.io	@firecorecoverfiles
Restdb@tutanota.com	RESTDB@my.com	@AresDatabase
mantis1991@onionmail.org	emeraldcrypt@tutanota.com	emeraldcrypt@onionmail.org
angry_war@protonmail.ch	mantis1991@tuta.io	gameovercreation@cock.li
allisonmartin813@cock.li	msupport2019@protonmail.com	sunhuyvchay@tutanota.com
brittonucgm147@gmail.com	allisonmartin813@yahoo.com	friendendfriend@cock.li
yashinkov007@tuta.io	msupport@elude.in	decryptyourfiles007@cock.li
crioso@protonmail.com	regina4hgoregler@gmx.com	pansymarquis@yahoo.com
anygrishevich@yandex.ru	wiruxa@airmail.cc	yongloun@tutanota.com
trustdatanswer@tutanota.com	kassmaster@danwin1210.me	kassmaster@tutanota.com
avarious@protonmail.com	willettamoffat@yahoo.com	uspex1@cock.li
filescrp@yandex.ru	uspex2@cock.li	filescrp@420blaze.it
kd8eby0@onionmail.org	udacha123@mail2tor.com	kd8eby0@nuke.africa
conkichinmodl@conkichinmodl.com	kd8eby0@inboxhub.net	russellveeh@yahoo.com
sendr@onionmail.org	conkichinmodl@gmx.com	@udacha123yes
nergontr96@cyberfear.com	mail4restore@swismail.com	hrol@tutanota.com

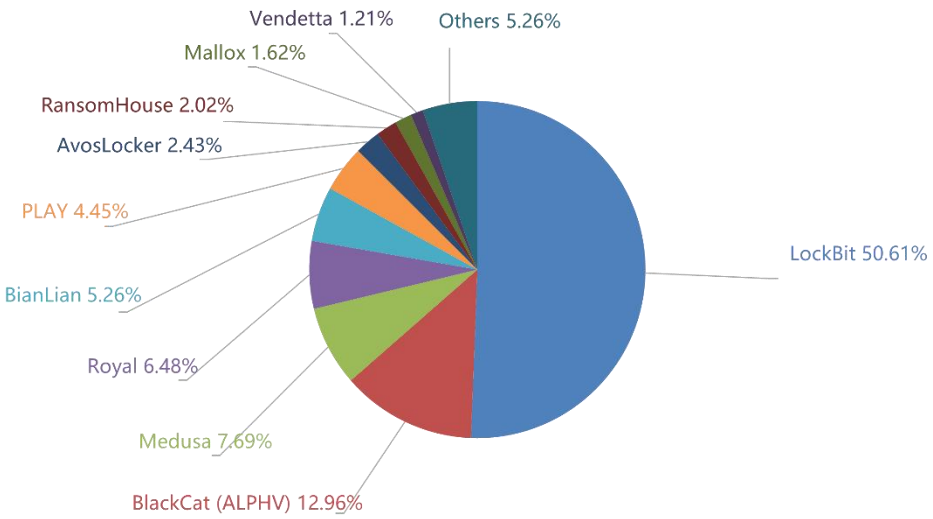
Sunjun3412@onionmail.org	info@fobosone	killhackfiles@cock.li
LeakHub@Keemail.me	tracklus@tfwno.gf	ineedatool@rape.lol
pizhon@torbox3uiot6wchz.onion	hensaxxx12@tuta.io	Sunjun3416@zohomail.com
wyattpettigrew8922555@mail.com	LeakHub@Mailfence.com	farusbig@tutanota.com
AbbsChevis@protonmail.com	MayarChenot@protonmail.com	aperywsqaroci@o2.pl
AxidOruraep1999@o2.pl	SayanWalsworth96@protonmail.com	cottleakela@protonmail.com
couwetizotofo@o2.pl	IjuqodiSunovib98@o2.pl	dutyuenugev89@o2.pl
phanthavongsaneveyah@protonmail.com	asuxidoruraep1999@o2.pl	qyavauzehyco1994@o2.pl
qicifomuejijika@o2.pl	dharmaparrack@protonmail.com	schreibereleonora@protonmail.com
romanchukeyla@protonmail.com	rezawyreedipi1998@o2.pl	MayarChenot@protonmail.com
suzumcpherson@protonmail.com	SuzuMcpherson@protonmail.com	AxidOruraep1999@o2.pl
QicifomuEjijika@o2.pl	wyattpettigrew8922555@mail.com	AbbsChevis@protonmail.com
DharmaParrack@protonmail.com	CottleAkela@pavatonmail.com	Qy1922555@mail.com
IjuqodiSunovib98@o2.pl	YpilokOmoadae1994@o2.pl	rddata@aol.com
JinMaglaya@protonmail.com	equalitytrust@disroot.org	anderssperry6654818@mail.com
founder@tfwno.gf	ThomassenVallen1999@mail.com	@dimaestr0
MckinnisKamariyah91@mail.com	shawhart1542925@mail.com	Update2020@airmail.cc
redacted@redacted.com	dimaestro@tutanota.com	support@freshmail.top
dimaestro@cyberfear.com	lazandelone@onionmail.org	rainbowforever@skiff.com
lazandelone@tutanota.com	helprecovery@gnu.gr	Mikel@cyberfear.com
smbppt@tutanota.com	back2up@swismail.com	Apoyo@msgsafe.io
aegisbackupz@gmail.com	datahelp321@nigge.rs	@sorry_bro_bivaet
datahelp321@onionmail.org	Mikelsupport1@msgsafe.io	NIGER1253@COCK.LI
Mikel@onionmail.com	spaceit@techmail.info	venolockdate1@rape.lol
spaceit@keemail.me	doctorSune@protonmail.com	annawong@onionmail.org
mail@domain.tld	RansomwareRecoveryExperts@tutanota.com	mrdrinkins@msgsafe.io
remarkpaul77@cock.li	gardex_recofast@zohomail.eu	dunkanmaznik1988@proton.me
herbtc@lenta.ru	meganbrons@protonmail.com	ziziclimber1989@tutanota.com
rast@airmail.cc	helpmemegan@tuta.io	lucifer.elbie@gmail.com
hensaxxx12@tutanota.com	hensa12@cock.li	leonherrero@protonmail.com
return_the_job@privatemail.com	asmodeus.elbie@gmail.com	satana@keemail.me
virtuoz1556@tutanota.com	adamstarkowsky@tutanota.com	samercin@tutanota.de
slyevil@keemail.me	xdenimx@lenta.ru	myfile@waifu.club
icanrestore@onionmail.org	icanrestore2022@onionmail.org	monahardecryption@airmail.cc
cinzzz@cock.li	recoverydata@onionmail.org	use_harrd@protonmail.com

warning@cyberfear.com	hashtreep@waifu.club	saraconor@gmx.com
rastcorp@securetalks.biz	teodorbutler1841@gmx.com	gelbertwatson1979@gmx.com
bill.g@onionmail.org	g.buttery@aol.com	helpfiles102030@inboxhub.net
jamesstevenson1799@tutanota.com	loopermiit@protonmail.com	padget_stewart@aol.com
hamsikdepay@tutanota.com	lettointago@onionmail.org	claraschumann1819@gmx.com
info@fobos.one	helpfiles@onionmail.org	icanrestore2022@protonmail.com
marlonbrando9256@gmx.com	calvingreen1957@tutanota.com	ritasventop32@protonmail.com
tsai_shen@zohomail.eu	tsai_shen@tutanota.com	palvaradobrendale@keemail.me
mark_willson94@tutanota.com	icanrestore2022@tutanota.com	fasthelper@gmx.com
bobywillsonteam@gmx.com	bobywillson@gmx.com	recovery2021@onionmail.org
claredrinkall@aol.com	susanbroderic@aol.com	bill.gteam@gmx.com
henrystanley1861@gmx.com	markzober1987@gmx.com	johnwilliams1887@gmx.com
benfestomser@tutanota.com	albertmatews1972@tutanota.com	bramwell.i@aol.com
recovery2021@inboxhub.net	bill.g@gmx.com	100returnguarantee@keemail.me
hughclapperton1877@gmx.com	bernhardriemann1901@tutanota.com	foxbox@airmail.cc
samuelwhite1821@tutanota.com	louisvega@tutanota.com	2020x0@protonmail.com
g.uan_yu@aol.com	guan_yu@tutanota.com	shelfit@airmail.cc
useHHard@cock.li	nopain555@protonmail.com	robertwels@airmail.cc
vivanger123@tutanota.com	ICQ@VIRTUALHORSE	ezequielanthon@aol.com
bondy.weinholt@aol.com	fidelako@int.pl	mccreight.ellery@tutanota.com
bertylarwayorstoner@jabb.im	ICQ@HONESTHORSE	foxbox@xmpp.cz
sorysorysory@cock.li	helprecoveryfiles@cock.li	patiscaje@airmail.cc
xsupportx@countermail.com	messi_tr_2020@protonmail.com	Bk_Data@protonmail.com
verious1@cock.li	willi.stroud@aol.com	decrypt2021@elude.in
hershel_houghton@aol.com	jewkeswilmer@aol.com	emerson.parkerdd@aol.com
decryptfilesonlinebuy@pm.me	mrdizzy@onionmail.org	lyontrevor@aol.com
Petya20@tuta.io	SupportC4@elude.in	bhattarwarmajuthani@420blaze.it
wang_team888@aol.com	barnabas_simpson@aol.com	cornellmclearey@aol.com
brandon_draven@protonmail.com	erich_northman@protonmail.com	verilerimialmakistiyorum@mail.ru
mccandlessronald@aol.com	AaronKennedy74@cock.li	s.boultons@aol.com
brokenbrow.teodorico@aol.com	deraksmauzi@gmx.com	chocolate_muffin@tutanota.com
zoiberghelp@onionmail.org	ximenezpickup@aol.com	frankfbagnale@cock.li
sookie.stackhouse@gmx.com	dupuisangus@aol.com	zoiberghelp@techmail.info
blair_lockyer@aol.com	murryu@aol.com	martinwilhelm1978@cock.li
frankfbagnale@gmail.com	michaelwayne1973@tutanota.com	recoveryufiles@tutamail.com

victorlustig@gmx.com	elfbash@protonmil.com	coxbarthel@aol.com
alexei.v@aol.com	eppinger.adams@aol.com	benwell_jonathan@aol.com
fredmoneco@tutanota.com	andreashart1834@cock.li	bernard.bunyan@aol.com
cheston_windham@aol.com	augusto.ruby@aol.com	dalgliesh.aaron@aol.com
tsai.shen@mailfence.com	frankmoffit@aol.com	geraldpotish1980@tutanota.com
onlybtcp@tutanota.com	herbivorous@keemail.me	serhio.vale@tutanota.com
dillon.dabzac@aol.com	sofiabecker21@cock.li	131845@cock.li
cullan_cash@aol.com	decode@criptext.com	kalimenok@gmx.com
normanbaker1929@gmx.com	howtodecrypt2@cock.li	johannesjokinen1977@gmx.com
totalsupportcom@cock.lim	aa1b2c3cc@protonmail.com	ryanmackin83@gmx.com
paynotanotherway@tutanota.com	bill.g@msgsafe.io	bossdata@protonmail.com
clausmeyer070@cock.li	angus_frankland@aol.com	sorryneedbtc@gmx.com
liamwake714@tutanota.com	matheuscosta0194@gmx.com	barenukles@tutanota.com
spacerecovery@tutanota.com	bossdata@keemail.me	greenbookbtc@gmx.com
bothelper@mailfence.com	albertpattisson1981@protonmail.com	recoveryufiles@gmx.com
getdata@gmx.com	ferdinandcohn1828@gmx.com	jamesgadsden1788@gmx.com
assistance@onionmail.org	cashanddash@tutanota.com	albertwesker1998@tutanota.com
greenbookbtc@protonmail.com	louispasteur1824@gmx.com	joshuabernandead@gmx.com
williamdampier1651@gmx.com	guan_yu@mailfence.com	someunusualsituation@protonmail.com
helpermail@onionmail.org	helperfiles@gmx.com	mrparts@mailfence.com
guan_yu@zohomail.com	firstaidfiles@protonmail.com	firstaidfiles@gmx.com
helpforyou@gmx.com	senderreport@gmx.com	tsai.shen@xmpp.jp
wannacry@cock.li		

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。尚未发现存在数据泄露风险情况的企业或个人也请第一时间自查，做好数据被泄露的准备，以便及时采取补救措施。

本月总共有 247 个组织/企业遭遇勒索攻击，其中包含来自中国的 8 个组织/企业在本月遭遇了双重勒索/多重勒索。另有 8 个组织/企业未被标明，因此不再以下表格中。

indigo.ca	hafele.com	thinkwelty.com
INDIKA ENERGY GLOBAL	Coole Bevis Solicitors	haeco.com
nokair.com	princepalace.co.th	globalcommunities.org
cobcreditunion.com	wmich.edu	georgeleslie.co.uk
df.senac.br	lsa-international.com	Ingenico
MSX International	hyosung.jp	rosenbauer.com
pcproductsinter.com	carveraero.com	bocca-sacs.com
wcso.us	moci.gov.kw	wsisd.com
Chowtaifook	ilfsindia.com	cotteeparker.com.au
G&G Electronics	McEwan Fraser Legal	MESSER CUTTING SYSTEMS
ZURCAL	ispace.com	InPro electric
Schwartz Hautmont Port Shop	Smarter Capital	The Keen Group
PRESTIGE MAINTENANCE	Kendall Hunt Publishing	Empresa Distribuidora de Electricidad del Este
Glovers Solicitors LLP	FICCI	AESCULAPIUS Farmaceutici
Bond It	Stone and Electrical Contractors	Moose, Martin, Haynes & Lundy
RAYAB Consulting Engineers	BULOG	AASP
nougat-carlier.be	siqueiracastro.com.br	fosterfarms.com
skylinetrisource.com	La Filipina	Markas
Summit Brands	FUTURE BUILDINGS	City of Lakewood
EncinoEnergy	vuu.edu	beacontech.net
treves-group.com	lyonhealy.com	lasegunda.com.ar

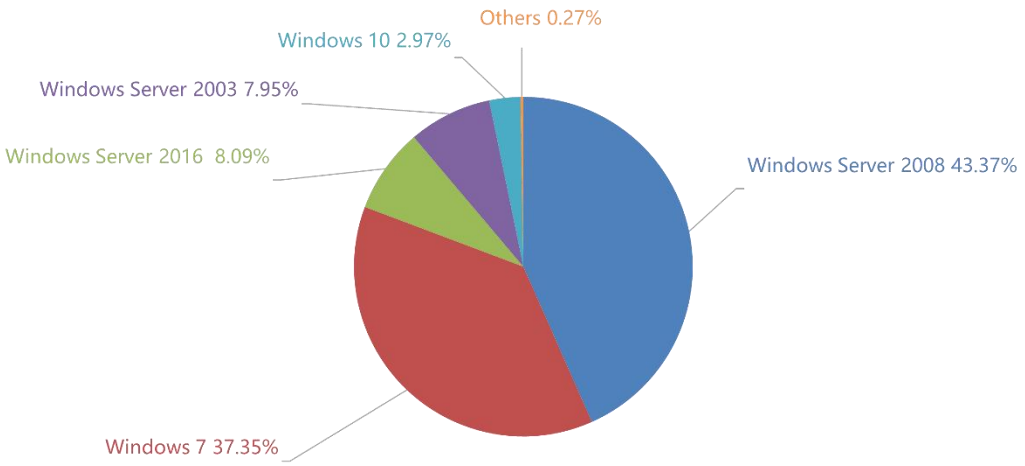
Highwealth		Hopsteiner
UNIS	DALLAS SCHOOL DISTRICT	Ancora - Sistemas de Fixacao
carlocksystems.com	International Center of Photography	elliotthomes.com
anthonymartin.be	BakerMechanicalInc.com	jetboxcargo.com
servicesfinanciersjdf.com	laremo.de	Hengmei Optoelectronics Co.,Ltd.
Cansew	Wawasee Community School Corporation	SINGLESOURCE
championfp.com	sandycove.org	isosteo.fr
diavaz.com	aguasdoporto.pt	inowai.com
primorossi.com.br	piercetransit.org	innophaseinc.com
hotdesk.me	alliedtools.com	NESG
Fibertec	Suburban Laboratories	cordfinancial.com
fikes.com	newbridge.org	AP Emissions Technologies
vissan.com.vn	myerspower.com	ziapueblo.org
royallepage.ca	vitrox.com	Evans Consoles
coreautomation.com	Mitchell Lewis Staver	California Northstate University
Hydrofit Alliance Ltd	Gallier Orléans	Mecaro Co., Ltd
blackandwhitecabs.com.au	trudi.it	Foamtec International
semsinc.net	vipar.com	nationallocums.co.uk
richardsind.com	montibello.com	AMADA WELD TECH
Eureka Casino Resort	PetroChina Indonesia	Vitas
Banco Sol	Leal Group	gruppobeltrame.com
Microgame SpA	Energie Pool Schweiz	Alexandercity
Delallo	cefcostores.com	albanesi.com.ar
srf.com	Hospital Service SpA	cassaragionieri.it
Reventics	vanderkaay.com	dana-group.com
mangalagroup.com	nonson.com.vn	hidalgocounty.us
tucsoneyecare.com	chempartner.com	laganscg.com
mdstrucking.com	greekpeak.net	Elim Clinic
PFA Systems	EnCom	Grace Church International
Integerity Tax	Aglobis	Diethelm Keller Aviation Pte Ltd
EightPixelsSquare	Tonga Communications	Bank of Africa
European Window	Elektro Richter	albouyassociesconsult
olsenlawgroup.com	wilsonart.co.th	ppinvestors.com
mhstech.com	lhermite-agri.com	Inland Group
covermeinsurance.com	mrkpc.com	maysecc.com
interpaving.com	Cork Institute of Technology	Munster Technological University
Thompson Safety	HAK Grazbachgasse	Aviacode (GeBBS)
B&G Foods (CA, US)	Tucson Unified School District	Jeffries Morris
Luna Innovations	iongroup.com	arcessex.org
phihong.com.tw	Mount Saint Mary College	ACS
A10	Cave Beblenheim	Trendsetter Engineering

Menken Orlando	JReynolds	Kerber, Eck & Braeckel LLP
transports-feuillet.fr	Penn Power Group	royalmailgroup.com
Ultralife Corporation	Hamilton Parker	The DGCX
pharmagestao.com.br	Casa Ley	MWI Animal Health
AmerisourceBergen/Censora	teleapps.com	Woodmeister Master Builders, Inc.
TK Elevator	ANXA	Advance2000
hkri.com	medellin.gov.co	etbrick.com
jams.edu.jo	INNOVATION COLLABORATION SYNERGY	nicklaus.com
prlabs.com	wcinet.com	crispinvalve.com
El-Mohandes	Schandy	Finaport
bplawyers.co.id	Five Guys Enterprises, LLC	nexuspoint.com
virtuosgames.com	urmgroup.com.au	Point Dedicated Services
redfordpd.com	jjdentistry.com	CannonDesign
guardiananalytics.com	sakrgroup.net	crystalcreamery.com
tonoli.com	scandia.ro	bethrivkah.edu
fabricatedpipe.com	kostika.co.il	seelllc.com
biosonicsinc.com	nlsmichigan.org	plasmasurgical.com
avantetextil.com.mx	byte.gr	transportsn.com

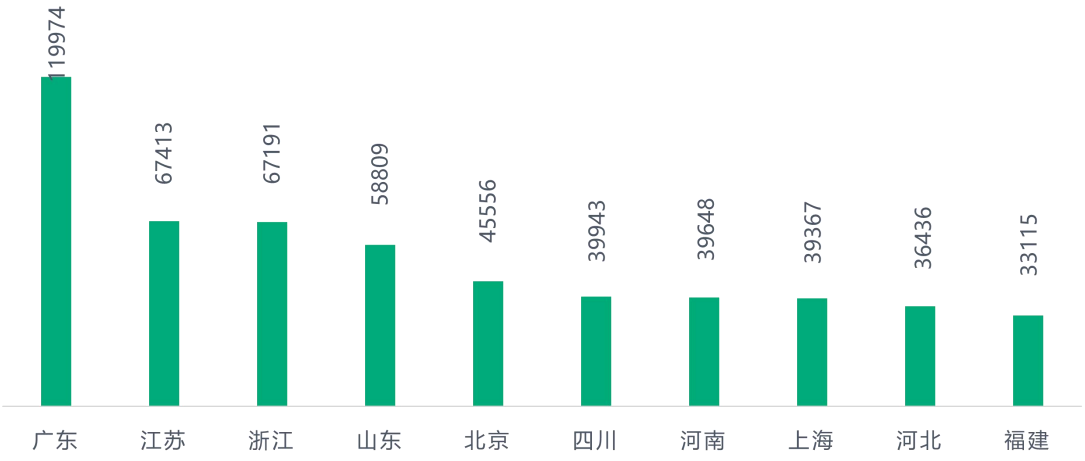
受害组织/企业

系统安全防护数据分析

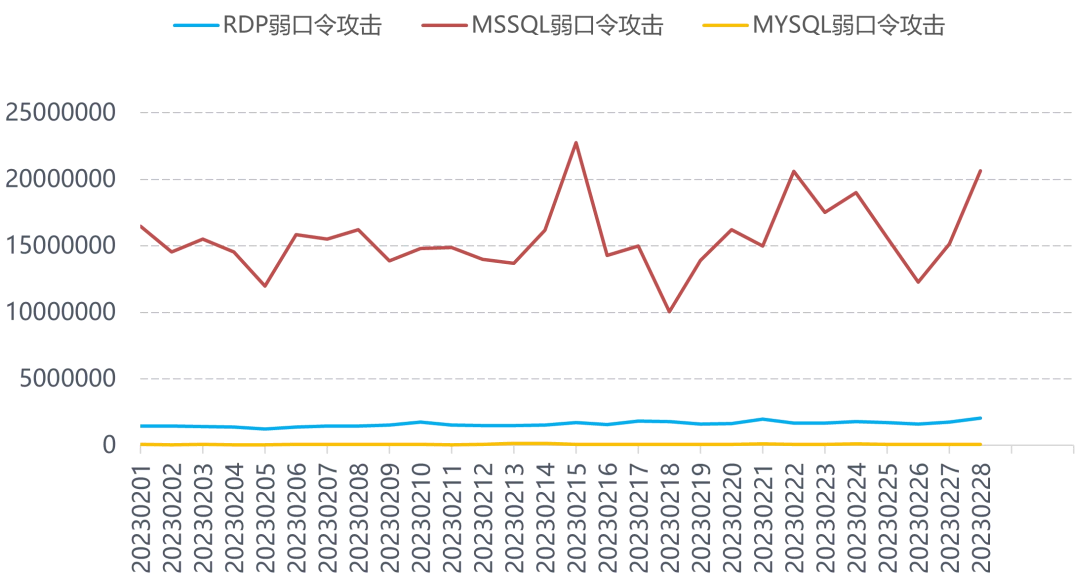
360 系统安全产品，目前已加入黑客入侵防护功能。在本月被攻击的系统版本中，排行前三的依次为 Windows Server 2008 、Windows 7 以及 Windows Server 2016。



统计 2023 年 2 月被攻击系统所属地域发现，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 2 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。

- 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。

- 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。

- Halo：同 360。

- 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。

- xollam:同 mallox。
- eking：同 devos。
- elbie：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。
- zfx:同 mkp。