

勒索软件流行态势分析

2025 年 9 月



三六零数字安全科技集团 | 高级威胁研究分析中心

勒索软件传播至今，360 反勒索服务已累计接收到数万次勒索软件感染求助。随着新型勒索软件的快速蔓延，企业数据泄漏风险不断上升，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，为需要帮助用户提供 360 反勒索服务。

2025 年 9 月，全球新增的双重勒索软件有 The Gentlemen、Coinbase Cartel、ShinyHunters 等多个家族，传统勒索软件家族新增 SnowSoul、HybridPetya、Monrans 等多个家族。其中，SnowSoul 在中国境内有传播痕迹，HybridPetya 绕过 UEFI 启动。

本月 Weaxor 勒索家族在注入系统进程后轮询加载的漏洞驱动列表中，新增 CVE-2025-52915 漏洞驱动、安在远控漏洞驱动。该勒索家族持续跟踪开源情报中的漏洞驱动信息，并迅速将尚未被大多数安全厂商识别或拦截的漏洞驱动用于攻击，以致盲并规避安全防护。我们的产品第一时间检测并成功拦截了这些用于致盲安全防护的恶意行为。

以下是本月值得关注的部分热点：

- 1** 新型 HybridPetya 勒索软件可以绕过 UEFI 安全启动
- 2** 捷豹路虎在网络攻击后将关闭时间延长一周
- 3** 巴拿马经济部披露 INC 勒索软件的攻击事件

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设备所中病毒家族进行统计：Weaxor 家族占比 46.24%居首位，第二的是 Wmansvcs 占比 10.22%，LockBit 家族以 9.68%占比位居第三。

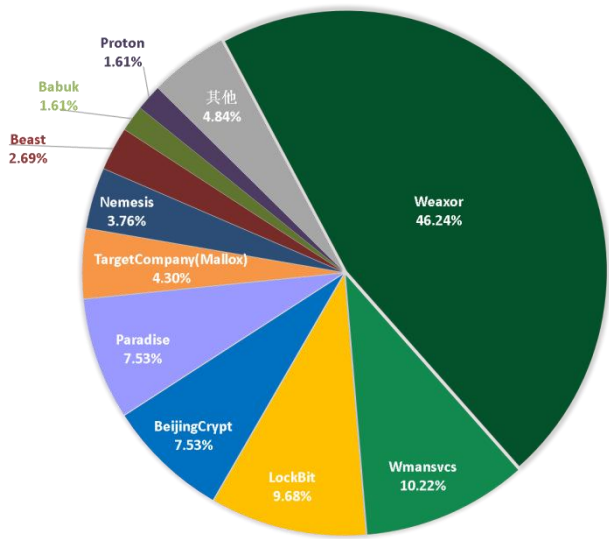


图 1. 2025 年 9 月勒索软件家族占比

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

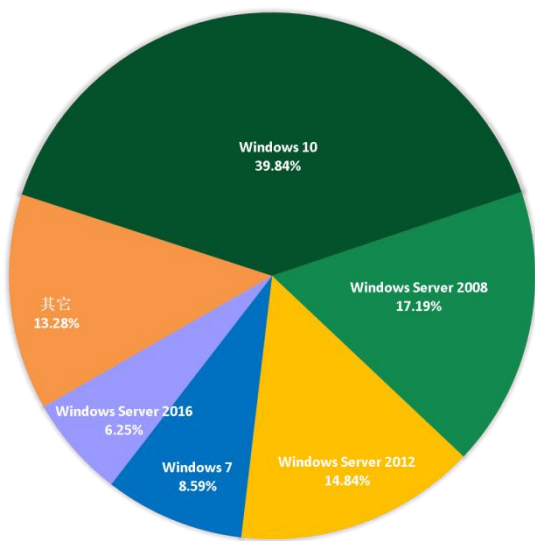


图 2. 2025 年 9 月勒索软件入侵操作系统占比

2025 年 9 月被感染的系统中桌面系统和服务器系统占比显示,受攻击的系统类型桌面 PC 小幅领先服务器。

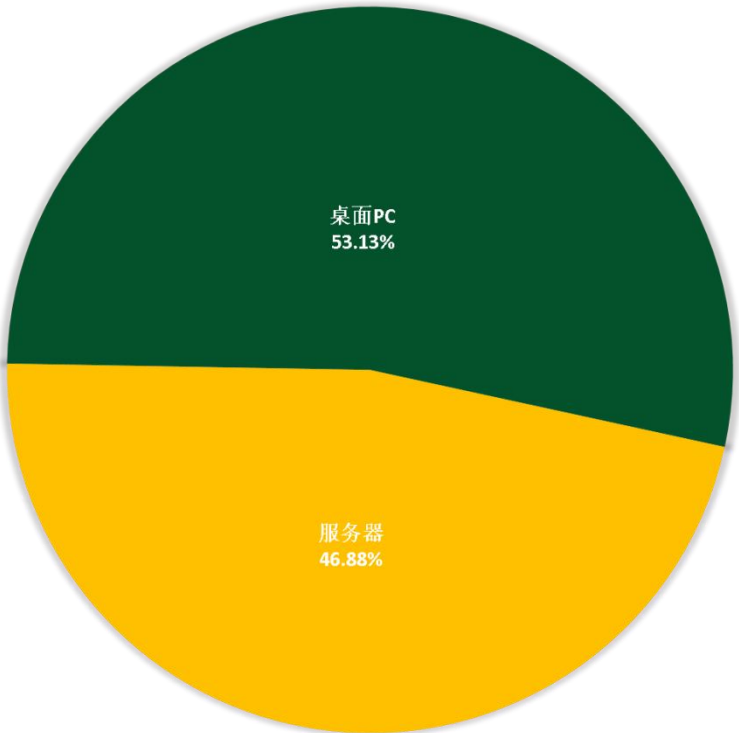


图 3. 2025 年 9 月勒索软件入侵操作系统类型占比

勒索软件热点事件

新型 HybridPetya 勒索软件可以绕过 UEFI 安全启动

最近发现的名为 HybridPetya 的勒索软件，可以绕过 UEFI 安全引导功能，在 EFI 系统分区上安装恶意应用程序。该款 HybridPetya 似乎受到早期知名勒索软件 Petya 及 NotPetya 的启发，这两款勒索软件在 2016 年至 2017 年间颇为活跃，其会加密计算机并阻止 Windows 在攻击中启动，但并不提供恢复选项。

安全研究人员表示，目前发现的 HybridPetya 可能是一个仍在有限范围内测试的早期版本。尽管如此，其具有 Secure Bypass 功能的 UEFI bootkit 模块仍是一个实实在在的威胁。

HybridPetya 融合了 Petya 和 NotPetya 的特征，包括这些旧恶意软件的视觉风格和攻击链特征。但在其感染的 EFI 系统分区中添加了新的东西，例如，利用 CVE-2024-7344 漏洞绕过安全启动。HybridPetya 会在启动后确定主机是否使用带有 GPT 分区的 UEFI，并将恶意引导套件放入由多个文件组成的 EFI 系统分区中，其中包括配置和验证文件、修改的引导加载程序、后备 UEFI 引导加载程序、漏洞利用有效载荷容器以及跟踪加密进度的状态文件。

目前已发现的 HybridPetya 变种中使用的文件有：

- \EFI\Microsoft\Boot\config（加密标志+键+nonce+受害者 ID）
- \EFI\Microsoft\Boot\verify（用于验证正确的解密密钥）
- \EFI\Microsoft\Boot\counter（用于加密群集的进度跟踪器）
- \EFI\Microsoft\Boot\bootmgfw.efi.old（原始引导加载程序的备份）
- \EFI\Microsoft\Boot\cloak.dat（包含安全引导旁路变种中的 X0Red bootkit）

此外，恶意软件将 \EFI\Microsoft\Boot\bootmgfw.efi 替换为易受攻击的

“reloader.efi”，并删除了\EFI\Boot\boot\bootx64.efi 文件。原始的 Windows 引导加载程序也被保存下来，在成功恢复的情况下被用于激活，这意味着受害者支付赎金后勒索软件提供了相应的恢复机制。一旦加密完成，系统将被引导进行重新启动，并在系统启动期间向受害者索要赎金——勒索金额为价值 1000 美元的比特币。

虽然目前并未发现 HybridPetya 的任何实际在野攻击案例，但类似的项目可能会选择将 PoC 武器化，并随时将其用于对未修补的 Windows 系统的攻击。

捷豹路虎在网络攻击后将关闭时间延长一周

捷豹路虎（JLR）在 9 月 16 日宣布，在 8 月底发生毁灭性的网络攻击影响其系统之后，停产时间将再延长一周。该汽车制造商自 9 月 2 日披露遭到网络攻击以来，一直在努力恢复运营，并称其生产受到严重干扰。9 月初，捷豹路虎还证实攻击者在攻击期间窃取了“一些数据”并指示工作人员不要报告工作。而在 9 月 16 日早些时候，这家汽车巨头宣布仍在努力重启运营，要到下周才会恢复生产。

捷豹路虎方面目前尚未回复媒体关于该事件及其对客户潜在影响的置评请求。虽然该制造商证实攻击者从其网络中窃取了信息，但尚未将攻击行为归因于某个特定的网络犯罪集团。然而，一个名为“Scattered Lapsus\$ Hunters”的网络犯罪组织已宣称对网络攻击负责，该网络犯罪组织在 Telegram 频道上发布了 JLR 内部的 SAP 系统截屏，并表示他们还在该公司的受损系统上部署了勒索软件。

该网络犯罪组织称，其是由 Scattered Spider、Lapsus\$ 以及 ShinyHunters 勒索团伙相关的网络犯罪分子组成，并对最近的 Salesforce 数据盗窃攻击负责。在这些攻击中，他们使用社会工程学攻击方式入侵了 Salesloft Drift OAuth 令牌，以窃取众多知名公司的数据，包括 Google、Cloudflare、Palo Alto Networks、Tenable 及 Proofpoint 等。

巴拿马经济部披露 INC 勒索软件的攻击事件

巴拿马经济和财政部（MEF）透露，其内部一些计算机可能在网络攻击中受到损害。政府指出，他们已启动了应对的安全排查程序，并指出该事件已被控制并且没有影响到对其运营至关重要的核心系统。

MEF 表示，个人和机构数据均是安全的，所有相关的预案措施都已到位，以防止未来发生事故。

然而，INC 勒索软件团伙上周在其数据泄露网站上的一篇文章中声称，对 MEF 进行了攻击。黑客称他们从 MEF 的系统中窃取了超过 1.5TB 的数据，包括电子邮件、财务文件、预算细节等。该组织于 9 月 5 日将 MEF 添加到其暗网上的受害者名单中，并以内部文件形式泄露数据样本，作为其入侵行为的证据。

有媒体联系了 MEF 并询问 INC 勒索软件攻击的真实性，但 MEF 尚未对此进行回复。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

troyal@tutamail.com	Temp@E.mail	milford@usa.com
troyal@mail2tor.co	hackerk4@proton.me	suppcarter@uymail.com
theroyal@onionmail.org	Helpadmin@mail.ee	murrock@consultant.com
help@x-mail.pro	RESTDB@my.com	amavalon@myself.com
mrromber@cock.li	Restdb@tutanota.com	taps@tuta.com
mrromber@tutanota.com	LeakHub@Keemail.me	Hulk67888@outlook.com
alt.rl-2xuldec@yopmail.com	wanhedaa@zohomail.eu	hivetech@protonmail.com
Decrypt.fast18@gmail.com	Backonline@cock.li	file@asia.com
Decrypt.jackson18@gmail.com	Backonline@cyberfear.com	ranshype@gmail.com
taro666@jitjat.org	Vertalic@Tuta.io	ranshype@tuta.io
taro@reddithub.com	cryhelp45@gmail.com	cybsupport1@onionmail.com
joedecryption@gmail.com	lockbitasafhsdfh@mailum.com	Elons1890@cyberfear.com
samuelymarry@tuta.com	lohikol22@gmail.com	mikel@onionmail.org
tenebris_silvam@aol.com	lohikol@cyberfear.com	mikel@cyberfear.com
ddhizxvh@onionmail.org	Srvhelp@mail.ee	enzo2003@mailum.com
598954663666452@exploit.im	srvhelp@skiff.com	enzo2003@cyberfear.com
365473292355268@thesecure.biz	HedaSupport@firemail.cc	greenoffer1@aol.com
minstreski@1337.baby	Dec.717team@gmail.com	yamag@onionmail.org
xingfiles@zohomail.eu	Decrypt77team@gmail.com	yamag@tuta.io
bluetooth001@onionmail.org	Qetsiyah@zohomail.com	kcvy@doj.one
troyall@tutamail.com	ketsia@airmail.cc	Merlin@aolonline.top
support1@keysupport.lol	Decvvv110@gmail.com	avantisit@zohomail.eu
r24ecover@cock.li	dicript@tutanota.com	hacker@protonmail.com
recover@atomicmail.io	wowsmith999999@proton.me	forinquiries@cyberfear.com
recover@onionmail.org	wowsmith1234567@proton.me	encryption_help@mailum.com
chivas@aolonline.top	BQTlock@tutanmail.com	edatex@airmail.cc
horsefucker@aolonline.top	datatheft@tuta.io	kqgeo@mailum.com
BackupDATA@tutamail.com	datatheft@cyberfear.com	guram24@proton.me
backupdata@atomicmail.io	rod.dat@tutamail.com	KdnEjwhQnxzbS763@mailum.com
Backfilees2023@Gmail.com	asxianx@proton.me	info@whitelock.xyz
unlockingrdp3@gmail.com		

表 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)。

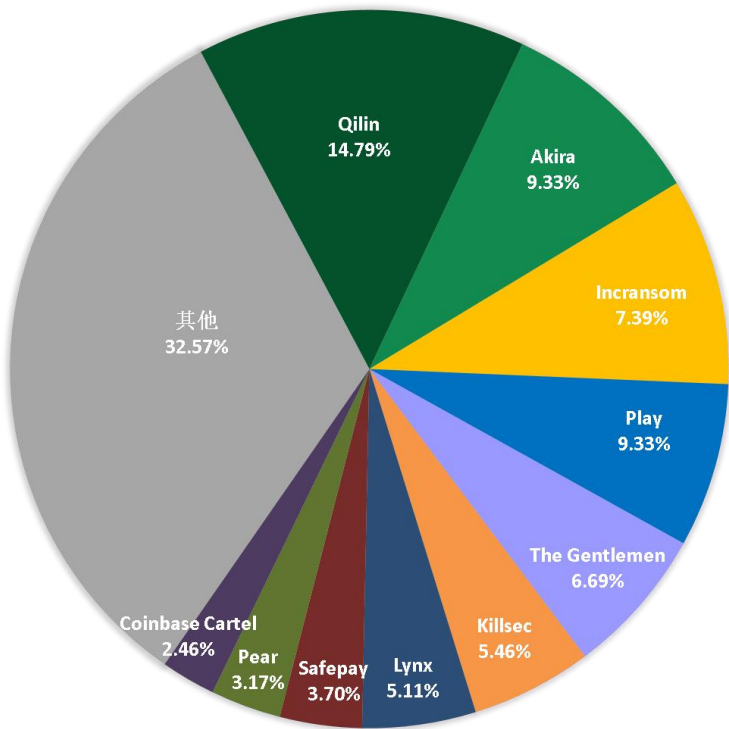


图 4. 2025 年 9 月通过数据泄露获利的勒索软件家族占比

以下是本月被双重勒索软件家族攻击的企业或个人。若未发现数据存在泄漏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 568 个组织/企业遭遇双重勒索/多重勒索攻击，其中包含中国 7 个组织/企业在本月遭遇了双重勒索/多重勒索。其中有 7 个组织/企业未被标明，因此不在以下表格中。

Greenville Legal	Legend Senior Living	Docklyne
multi-media systeme AG (mmsag.de)	ACRO Automation Systems	Northland Auto Solutions
C Well	City Wide	Accelerated Academy
Foremost Asset Management	heidelberggc.com.au/Australia/26.4GB	www.melenco.com
Rectory School	Dubroff, Easley & Lovell, LLP	Coastal Pacific Xpress
TRAUM Investment Co.	Tri-Century Eye Care	Commercial Casework
Petraville Asset Management	Broad High Asset Management	Venezia
The L B	United Pharma	Ben-Mor Inc.
Storage King	ST Asset Management Co	Wouters France

Cascade Pacific Pulp	Orum Asset management	HD Media Systems
Komar Industries	EOS Asset management	Mayors Machine Works
CCMC	www.independentpaperboard.com	JIT Energy Services
Comcast	Dblock Asset Management Co	Anderson Aluminum
Organon	Generali Group	Royal Machine & Tool
Insightin Health	klinglnberg.in	Reliable Roofing
Future Generali	altas.com.tr	Celtic Engineering
Priester Aviation	cardinal-services.com	GDZ Computer Services
Sinco	SUNIQUE Asset Management Co	Cool Wind Ventilation
Pawling	Saebom Asset Management	Rising Star Hydraulics
Tom Duffy Company	Zebra Asset Management Co	Edwards Interiors
Midwest Industries, Inc	grupogid.com	GL Veneer
Turf Care Store	Thomas Safran & Associates	Allegis Group
Bugnard	lindenlaw.com	Aupaircare and Intraxinc
Sueba USA	spartanburgcounty	E&S Food
Von Paris Moving	browneco.com	Fusion Homes
Apex CoVantage	alliancesteelco.com	Republica De Panama
Burke Contracting	slusarski.com	Plan B Die Fachanwaltskanzlei
MCBS, LLC	drcloudemr.com	Cervantes
www.wrapex.ca	venetianassociates.com	Ceres
AZpro Group (azprogroup.com)	armourhome.co.uk	BIOLAP Soluciones Médicas
Mobidic Asset Management	biosorthopedics.com	Proplastics
Dodd-group-ltd	gosheating.co.uk	Kandeo
Pangea Travel Store	Prime Asset Fund	Ransomware Recover Indonesia
Caresoft Global caresoftglobal.com	ARMONIA MEDICAL S. A. S.	JN Aceros
Universite de Pau et du Pays de l'Adour	BMW	Flexofast Indonesia
Al-Babtain Power & Telecommunication	www.vdyne.com	Del Campo Supreme
Petro-Diamond (petrodiamond.com) – subsidiary of Mitsubishi Corporation	RAC Consultoria	Cremona Inoxidable
Peavey Electronics Corporation	Pieffe Auto Group	Grupo Halcon
Bader Gruppe	IAD GmbH	JIEI (Thailand) Co., Ltd
lakehaven.org	Kwg	Wharton Independent
Manjarrez Impresores	Pfullendorfer Tor-Systeme	Kuwait Portland Cement
J. E. Stacey & Co. Ltd (jestacey.com)	Instituto Socio-Económico Comunitario (INSEC)	Amv International Development
raimore.com	Humax Holdings	Liceo Francés Antoine y Consuelo de Saint-Exupéry
Virtual Projects (virtualprojects.build)	https://www.cnh.com/	Dolidol
www.braswellsvc.com	Grup Gestio	AB Mauri Private
busaba.com	Tunad	InjectSense
www.chicagobotanic.org	Accflex ERP	Algorithmica Research
r3consulting.com	grupozeta.com &	Sigma

	www.grupozetajalisco.com	
ncgllc.com	thepropertybusiness.com	PC Chandra Jewellers
sacada.org	ekonomipoolen.se	Shifa Oman
www.sonoshowmoveis.com.br	bmsi.org	Oriental de Seguros
General Directorate of Taxes and Estates	JAFICA Telecomunicaciones	Venezuela Re
heparks.org	Concord New Energy Group	J.V.D.B. & Associates Inc
phi.ca	Medpeds	Laboratorio Clinico Santa Rita
MSB	F1-Generation	Narumi (Thailand) Co.,Ltd.
Naftali Group	Allure Clinics	Ophtazon
Bignault & Carter	Jansenfurniture.com	Surtel Technologies Pvt
The DM Burr Group	chroma.com.tw	Saelen/Heizomat
Belleville International	ferus-smit.home	LOCATION PEINTURES PRESTATIONS (LPP)
WaltersMorgan Construction	jubileelife.com	noblecorp.net
Punctual Abstract	kmssa.net	Miesa
Dorrell Fabrics	webville.net	AVA Senior Connect
Crane Production Systems	elssurveying.com	Energy Fishing
Queens Center For Change	medkar.com	BDE Computer Services
WalletKu Indompet Indonesia	SV-Büro Ing. Schulz GmbH	Promark Partners
XChief / ForexChief	News-Press & Gazette Co.	Melwood
PTR Asset Management	www.shimaogroup.com	Bounds Gillespie Killebrew Tushek Architects
BAM	VirMedice	EPLS: Entreprise d'Installations électriques Courant Fort
BW-RF	SK Telecom	okan.ru
FysioRoadmap	Desjardins Banking/Group	General Converting
Amelia Overhead Doors	AdScale	RBJ Escrow Software
Pangborn	Dreyfuss Williams & Associates Co , LPA	nubox.com & sumasaas.com
ComTec Systems	Focus R Technologies Pvt	runaces.com
Earthadelic	NTT Data/Vectorform	Keller Laser AG
Steve Basso Plumbing Heating	Plug Power	Vardeco
Atlas Pressed Metals	Volt	www.thepromisenig.com
Amos Spacecom	Wakefield & Associates	Easy Credit
Yooshin Engineering Corporation	Ceva Logistics	Engineered Advantage
Phillips Feldman Group	RGR Sportswear	https://gazomet.pl & https://cgas.pl
Asserson	Lake Book Manufacturing	rose-acre-farms-inc
Thai Future Inc. PCL	Eau Palm Beach Resort & Spa	Nathan
thomasmhughes.com	Energenecs	Purwana Group
Rothmann Immobilien	Garrison Architects	Taiwan Flex Electronics
FTCS Forage	McCarter Electrical	Rad-Solutions, LLC
Memphis Millwork	Pathfinder	TuftsMedicine
Cardinal Machinery	General Control Systems	GPS Trackit

ComTec Systems	RFI	Archer Health
SOP. Sistema Odontológico Privado	Crestone Group	Gordon Rees Scully Mansukhani LLP
Podo Asset Management	TerranearPMC	Mechatronics
AV Services Barcelona	Rochester Optical	BinBaires
WEST Inc.	CyberData	OftalTech Solutions oftaltech.com
XCAssociates	CAS EXhibition Partners	Suiza Lab
HUB ASSET MANAGEMENT Co	Venlogistics	eMedicoERP
Summit Asset Management	Technology Assurance Group	GoTelemedicina
Trustar Capital Management Co	jsgroup	MedicSolution+
oconnorcp.com	Volumex Lease	schuler-service-group.de
waxhaw.com	Trucchi's Supermarkets, Inc.	www.midcity.lk
smpeurope.com	volinc.com	RelationMedia A/S
regalmold.com	trchealthcare.com	Indo-MIM
sperispa.com	HappyTenant	Michigan Sugar
grupobocel.com	CBL-SRL	Rulmaksan Makina
halemakua.org	Baum Precision Machining	The Fixing Company
Study Gate	VANCHOR Asset Management	HeavenlyDental
Fattore Cosméticos Ltda	APEX Asset Management	Plazadental
MACMA Werbeartikel oHG	Majesty Asset Management Co.	WZV Warndt
pactchangeslives.com	Melon Asset Management Co.	MeamarGroup
lwginc.net	Taurus Investment & Securities Co	Elite Trailers
VIR	LX Asset Management	Ekmanian Tax & Accounting
awo-ka-land.de	Klarman Asset Management	Osaki Medical
amsfulfillment.com	Human and Bridge Asset Management	CI Engineering
Valufinder Group	Awesome Asset Management Co	www.sixgunsllc.com
www.officepro.cl	Pollex Asset Management Co.	www.simmonsboardman.com
www.mpmimports.com.cy	www.roscovision.com	elektro-buder.at
TLD Law.com	http://www.hiec.com/	www.ziegler-design.de
The Maryland Department of Transportation	https://heritagegrowth.com/	firstlight.net
www.cr-installers.com	MFO ITALIA	Spokane Produce
www.chinup.com.tw	Key 4 Energy Srl	cphcorp.com
www.apm-finance.de	Studio Legale Tisot Iuris	denraytire.com
www.meduane-habitat.fr	Professional Trust Company	www.medwayplastics.com
FAI Aviation Group (fai.ag) - The biggest leak ever	usenergy	highdoc.de
Madison Healthcare Services	Groupe Clarins	pesadoconstruction
Pyramid Global Hospitality	Eagle Excavation	www.onahotels.com
Mavis Tire Supply	olarra	www.primax.com
KIPP DC	bio3g.com	bemac-merivale
Sapp Bros	opso.us	volanno.com
Washington Prime Group Inc	Office Of The Registrar Of Political Parties	city-of-batavia

www.margaritavilleatsea.com	Conception Reproductive Associates Colorado	www.metrotech.edu
www.milkagro.sk/Slovakia/335GB	Black Butte Coal	Carus
Cadisa	Vicon	https://ipathpr.com
Paul Rossi Law Offices	Ramar & Paradiso	Rivertown Surgey Center
siball.net	West Chester	flamgard.co.uk
Speed Art Museum	Catholic Charities of the Diocese of Albany	sandg.local
Alexander Bürkle	Homsey Law Center	omegabiotek.com
P&P Industries	Cheyney University	CANDhenterprises.com
Thermofin	Rescue Mission Alliance	Moore & Van Allen
Edro Real Estate	Cullen, Haskins, Nicholson & Menchetti	Master System Inc
Takeuchi US	Beaumont Bone & Joint Institute	musinmas.com
DHM Properties	US Graphite	UNIDEL Ventures Pvt
Vcinity	Expert MRI	The Bank of Romney
GammaTech	Next Level Solutions	Jack Resnick & Sons
APG	Reynolds & Reynolds	promisedland.com.tw
Roth & Scholl	Cleveland City School District	www.pure-chemical.com
New England Waterproofing	DBK Partners	stthom.edu
Combined Services HVAC	Hanzestrohm	blytheco.com
PTR	BRIGHT SYSTEM JAPAN CO., LTD	Risen Energy Co.
Agility CIS	Miljödata	camaradealmeria.com
Hilldun	Cariri	Commission scolaire des Appalaches
Ronco Safety	halbarstainless.com	CESCONSULT
Markowitz Ringel Trusty & Hartog	TimHaahs	TSI Accessory Group, Stanley Creations Inc, iStar Jewelry, Roman & Sunstone.
cegconstruction.com	cityofmiddletown.org	NPIAV
Rainwalk Technology	osdcourtkts.org	Samwha Capacitor Group
Fractalite	denali-industrial.com	Monterey Mushrooms
BEHCA	Heffner Toyota & Lexus	www.dimarcogroup.com
VTK Legal	Aluf Plastics	identic.be
AX CAPITAL	PYATOK	Bartek Ingredients
FDB Collections	Brownstone Agency	TEAM GROUP
MortDash	Mazza Recycling Services	Artists&Clients
Scanbo	Survival Flight Inc	Pooler Enterprises
UwayApply	Meskan Foundry	Natare
Top4Fans	TAKwest	GCC of America, inc.
Cadorim	Northwest Medical Specialties	Cordeiro Guerra & Associati
optimumdesign.com	CARTONAJES BERNABEU SAU www.cartonajesbernabeu.com serviced by IT company Verne Group www....	Pittsburgh Gastroenterology Associates
Batesky Law Office (BLO)	STANDARD IRON & WIREWORKS (Helgesen	bthcpa.com

	Industries)	
Miami Management	Fluxergy	kclub.ie
ZEF	Molod Spitz & DeSantis	usai.io
Pennsylvania Office of Attorney General	TDK Technologies	wilsonatl1aw.com
goodcents.com	Compagnie des Guides de Chamonix	scottschiff.com
NV ELMAR	Namibia Epia Financial Services Windhoek	mdneal.com
Klinglnberg india pvt ltd	Menten Truck Service N.V., Hoeselt, Belgium	ellison-mills.com
Promociones Luis Barros	BlockBets Casino	SISTRAN Consultores
usadebusk.com	Communicare Inc.	umweltprofis.at
United Machine	Insurance Office of America	waterfordsurgicalcenter.com
Alan Shintani, Inc	Gagosian	oiwky.com
Jones Soda (Stock Symbol: JSDA)	moinian.com	Genmark Automation
About Ross, Brittain& Schonberg Co., Lpa	deerfield.com / singulargenomics.com	Automated Business Solutions
EAST Design Architect Sdn. Bhd	Encore Leisure Group	Caprez Ingenieure AG
Espectral	Spectra Logic	TAK Communications, Inc
KCI Telecommunications	transnova-ruf.de	mffood.com
EUM Asset Management	Ekotrade	gmpc.com
cardiofocus.com	waverlychildcare.org	oakland-museum-of-california
Gurney's Resorts	RG ELECTRIC COMPANY INC	PathoQuest-Biotechnology Research
Hood Technology	ROBERT G. DASHIELL, JR., P.E., INC	Construseñales S.A.
Ronald A/S	Principes Credit Systems Limited	Arboris
Cook Brown	BusOnlineTicket Thailand	Juggernaut
MMI Direct	1 ACT Driving Schools	Vanderpool Construction
Intellect Systems	M8 Group	All States Materials Group
Wargo French	BFLI	LEVEL

表 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 10。

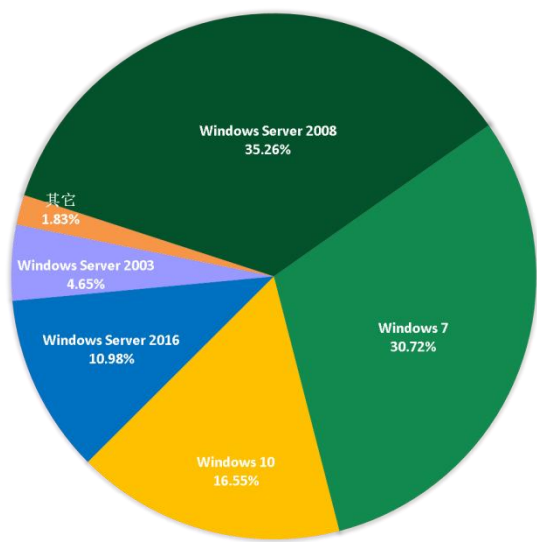


图 5. 2025 年 9 月受攻击系统占比

对 2025 年 9 月被攻击系统所属地域进行统计，并与前几个月采集的数据进行对比发现，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。

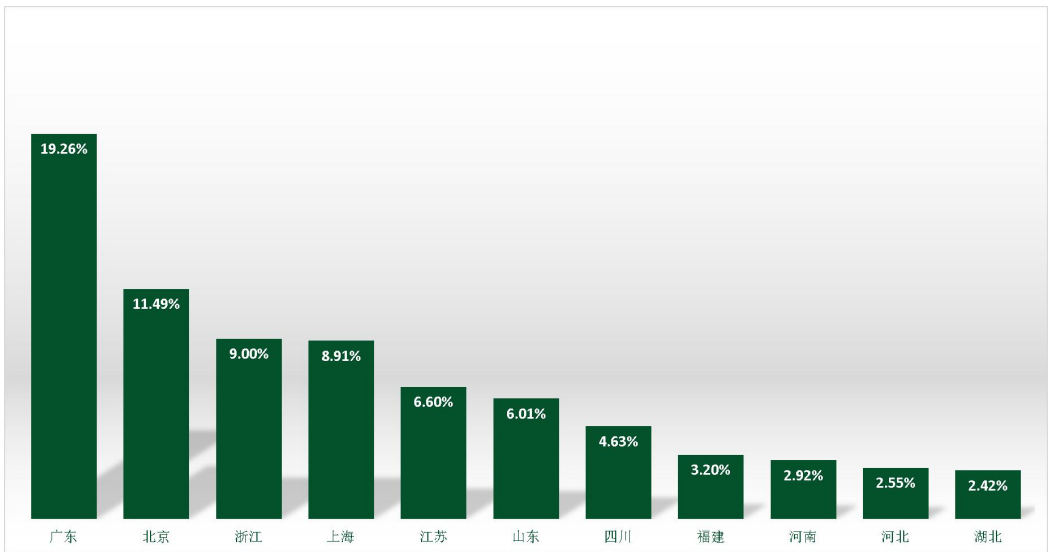


图 6. 2025 年 9 月国内受攻击地区占比排名

通过观察 2025 年 9 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。

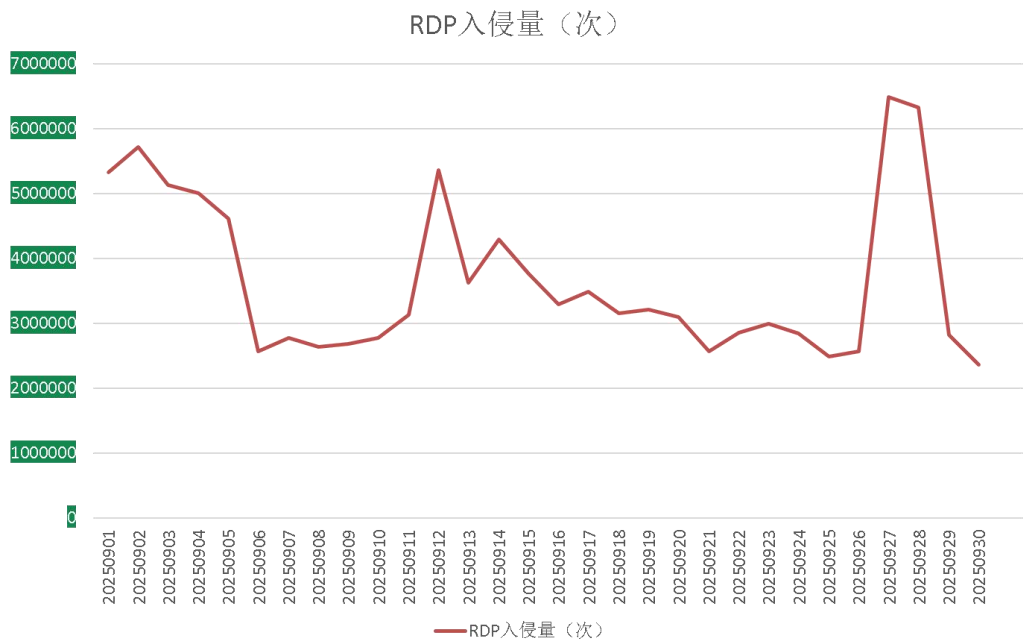


图 7. 2025 年 9 月监控到的 RDP 入侵量

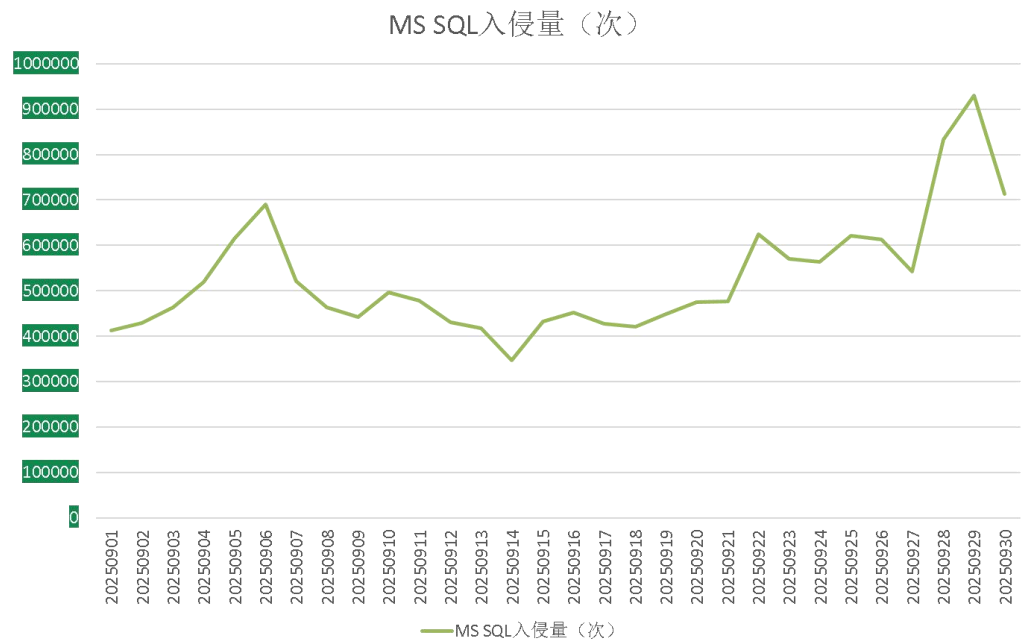


图 8. 2025 年 9 月监控到的 MS SQL 入侵量

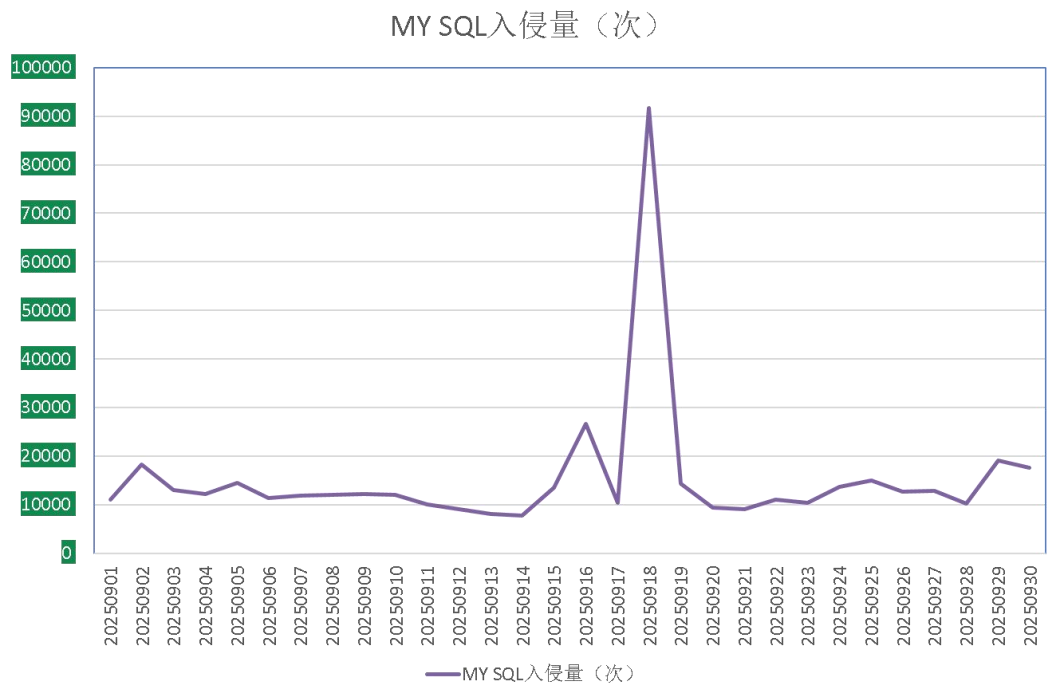


图 9. 2025 年 9 月监控到的 MYSQL 入侵量

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。

- ✧ roxaew: 属于 Weaxor 勒索软件家族，该家族目前的主要传播方式为：利用各类软件漏洞进行投毒，通过 powershell 加载攻击载荷并注入系统进程，多轮加载不同的漏洞驱动与安全软件进行内核对抗。
- ✧ peng: 属于 Wmansvcs 家族，高度模仿 phobos 家族并使用 Rust 语言编译，目前仅在国内传播。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。
- ✧ 888: 属于 Nemesis2024 家族，以勒索信中的 Nemesis 家族字段命名。该家族的主要传播方式为：通过暴力破解远程桌面口令与数据库口令，成功后手动投毒。
- ✧ baxia: 属于 BeijingCrypt 勒索软件家族，由于被加密文件后缀会被修改为 beijing 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与数据库弱口令成功后手动投毒。
- ✧ bixi: 同 baxia。
- ✧ spmodvf: 目前此扩展名反馈的用户均未提供溯源信息，暂未研判家族归属与攻击方式。
- ✧ taps: 属于 Paradise 勒索软件家族，该家族目前的主要传播方式为：通过暴力破解远程桌面口令与数据库弱口令成功后手动投毒。
- ✧ weaxor: 同 roxaew。
- ✧ 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，后来增加了漏洞利用的传播方式。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。

✧ devicdata: 同 mallox

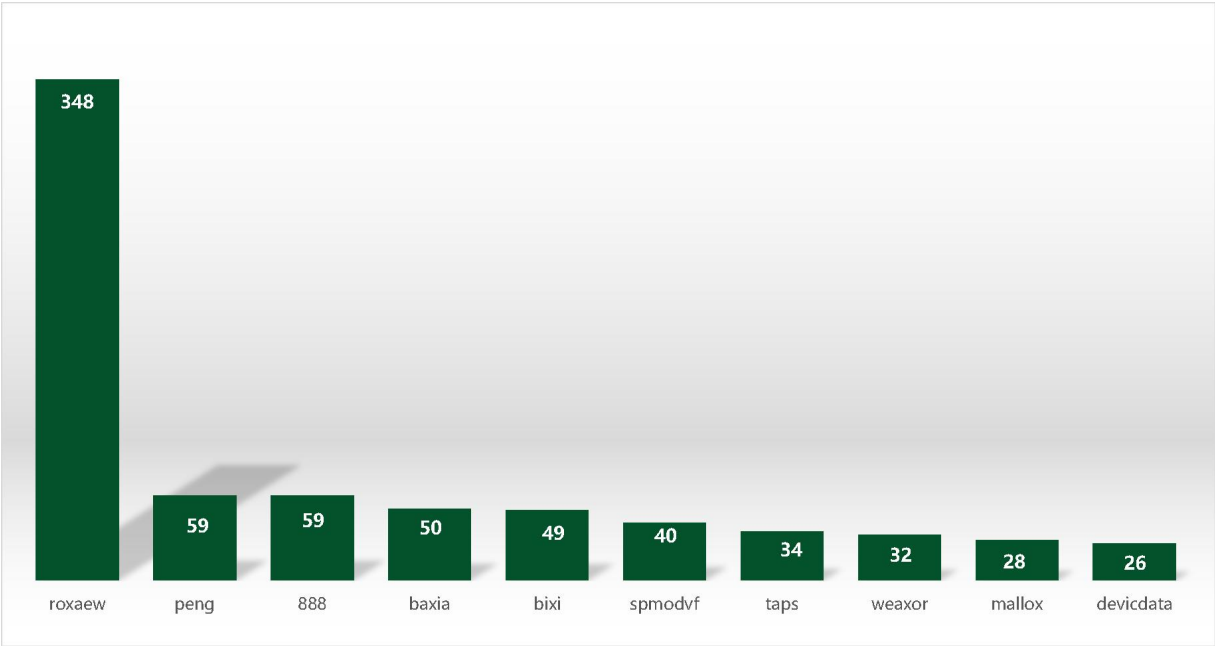


图 10. 2025 年 9 月反病毒搜索引擎关键词搜索排名

解密大师

从解密大师本月解密数据看，解密量最大的是 Phobos 家族，其次是 Crysis 家族。使用解密大师解密文件的用户数量最大的是被 Crysis 家族加密的设备。

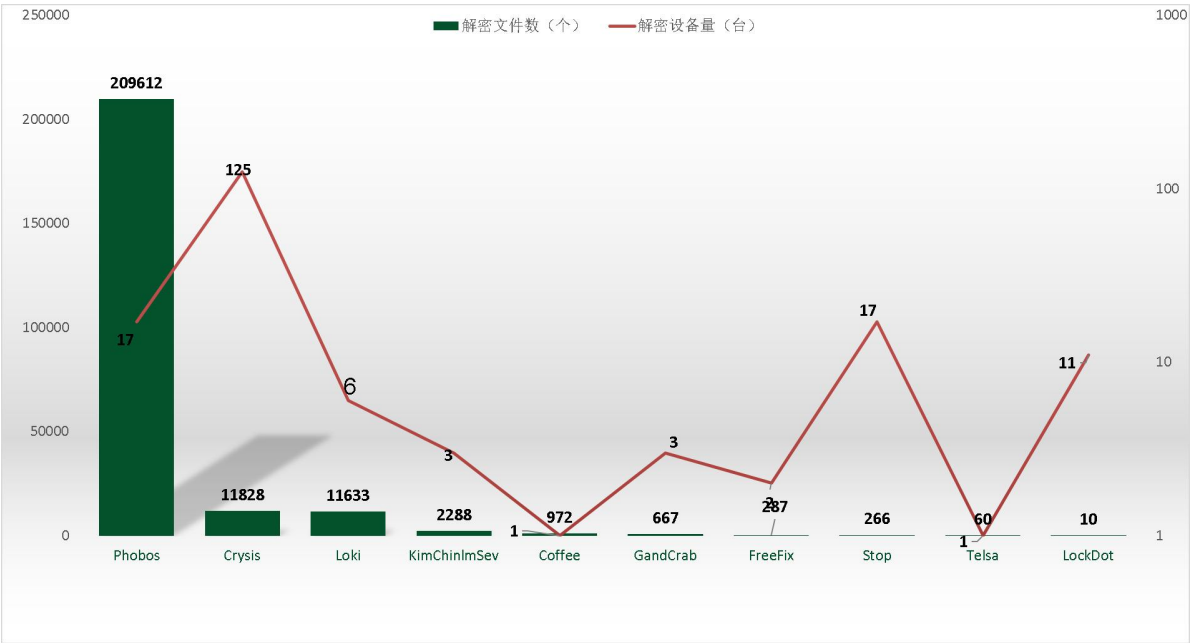


图 11. 2025 年 9 月解密大师解密文件数及设备数排名