勒索软件流行态势分析

2024 年 6 月

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。

2024 年 6 月，全球新增的双重勒索软件家族有 Cicada3301、Trinity、ElDorado。新增的传统勒索软件家族有 Anony。其中 Anony 在国内广泛传播并出现多个变种。

以下是本月值得关注的部分热点：

1. 过节也不消停——TellYouThePass 的“端午攻势”

2. Black Basta 勒索软件组织与 Windows 的 0day 攻击有关联

3. Ratel 远控软件针对过时的安卓手机发动勒索攻击

4. Brain Cipher 攻击印度尼西亚数据中心

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：TargetCompany(Mallox)家族占比 60.27%居首位，第二的是 phobos 占比 12.05%，BeiJingCrypt 家族以 8.04%位居第三。

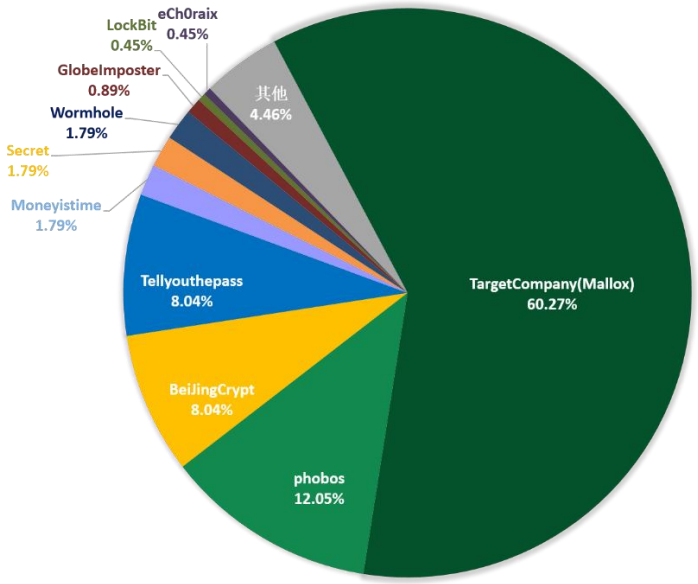

图 1. 2024 年 6 月勒索软件家族占比

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 2012 以及 Windows Server 2008。

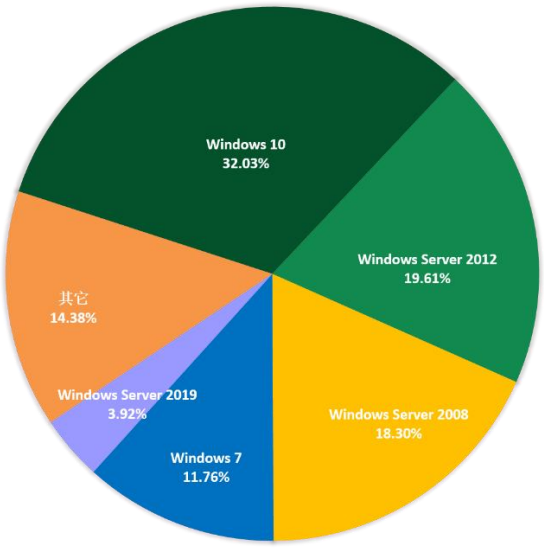

图 2. 2024 年 6 月勒索软件入侵操作系统占比

2024 年 6 月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型桌面 PC 与服务器平台的攻击比例基本相当。

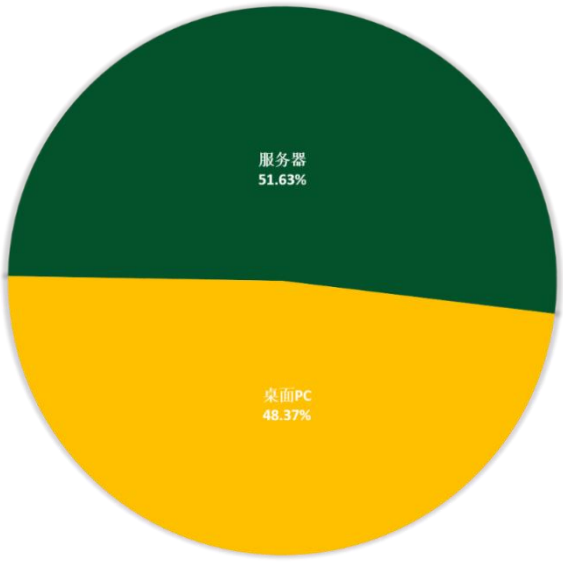

图 3. 2024 年 6 月勒索软件入侵操作系统类型占比

勒索软件热点事件

过节也不消停——TellYouThePass 的“端午攻势”

随着端午节假期的结束，大家也都逐步回到了日常的工作生活当中。而 360 安全大脑则监控到，就在端午节假期期间，一个熟悉的勒索病毒家族再度开启了新一轮的“攻势”。

结合目前的监控数据来看，本轮攻击最早见于 2024 年 6 月 8 日 15 时左右。而攻击的源头是来自于一个针对 PHP-CGI 的参数注入攻击漏洞，漏洞的 CVE 编号为“CVE-2024-4577”。根据 CVE 官方的记述，在带有该漏洞的环境中，PHP-CGI 模块可能会将 Windows 系统传入的参数误识别为 PHP 的配置选项传递给正在运行的 PHP 程序，进而可能被恶意攻击者利用来实现“任意代码执行”的操作。

而在 6 月 8 日时，360 安全大脑便监控到了该漏洞的在野攻击。在实际触发的在野攻击中，系统中的 HTTP 守护进程会将可触发漏洞的参数传递给 php-cgi 程序，进而导致 php-cgi.exe 调起系统的 cmd 命令行工具运行 mshta 解释器来获取在线的远程 hta 脚本（实际为 vbs 脚本）到本地并运行。

而最终执行的脚本，则会释放其中经过编码过的恶意程序并运行。这个最终被释放到本地并被运行起来的恶意程序，便是我们阴魂不散的“老朋友”，TellYouThePass 勒索软件。至此，TellYouThePass 借助这个新公开的 PHP 漏洞展开了又一轮的攻击。

Black Basta 勒索软件组织与 Windows 的 0day 攻击有关联

Black Basta 勒索软件被怀疑利用 Windows 的提权漏洞 CVE-2024-26169 进行传播。该漏洞是 Windows 错误报告服务中存在的一个严重问题，其允许攻击者提升其权限至 SYSTEM 级别。微软在 2024 年 3 月 12 日的常规下发的每月“补丁星期二”更新中修复了这一漏洞，而在其描述页面中显示该漏洞尚未发现被真实的在野攻击所利用。

而赛门铁克的一份报告则指出，CVE-2024-26169 可能已被 Black Basta 勒索软件的运营团队——红衣主教网络犯罪集团（Storm-1811，UNC4394）利用，并指出它很有可能是在其尚处于未知的 0day 漏洞阶段时期就已被利用作为入侵手段之一。赛门铁克调查了一起勒索攻击事件，该事件中使用了针对 CVE-2024-26169 漏洞的攻击工具，该漏洞是在黑暗之门加载器（Black Basta 一直在使用该加载器）首次感染后被利用的。

安全分析人员认为攻击者与“Black Basta”有关联，因为他们使用了批处理脚本伪装成软件更新，目的是执行恶意命令并对被入侵的系统建立持久连接——这也正是该组织的常见策略。同时，研究人员观察到的攻击工具利用了 Windows 文件 werkernel.sys 在创建注册表键时使用空安全描述符的事实。该工具利用这一点创建了一个注册表键，并将“Debugger”值设置为自身的可执行文件路径，从而允许其以 SYSTEM 权限启动一个命令提示符窗口。

在这份研究成果中有一个有趣的情况：其中一个攻击工具的编译时间戳是 2024 年 2 月 27 日，而另一个样本的编译时间则更早，是 2023 年 12 月 18 日。这意味着 Black Basta 在微软最终为该提权漏洞发布修复方案的 14 至 85 天之间便已拥有了该漏洞的利用工具。虽然这个时间戳可以被修改，但目前看来攻击者没有伪造时间戳的动机，所以这种情况的可能性并不大。

为了降低 Black Basta 利用这一漏洞进行传播所带来的风险，建议用户及时安装最新的 Windows 安全更新补丁。目前，安全研究机构观察到较新版本的 BiBi Wiper 会用随机数据破坏非系统文件，并在文件后附加一个包含“BiBi”字符串的随机扩展名。与过去的版本相比，这些较新的变种仅针对地区标记在以色列操作系统，并且不再删除系统快照或禁用系统的错误恢复功能。但它们现在会从硬盘中删除分区表信息，这种专门针对系统分区表展开的攻击，因其会导致安全人员无法恢复硬盘布局而将数据恢复工作复杂化，并最大程度地破坏数据。CI Wiper 则主要针对地区标记为阿尔巴尼亚的系统，它使用“EIRawDisk”驱动程序执行擦除操作并将预定义的缓冲区覆盖到物理驱动器的对应位置中。

Ratel 远控软件针对过时的安卓手机发动勒索攻击

一种名为“Rafel RAT”的开源 Android 恶意软件被多个网络犯罪组织广泛部署用于攻击过时的安卓设备，其中一些团伙还试图使用勒索软件模块将设备锁定，并通过 Telegram 要求支付赎金。

据安全分析人员报告称，他们发现了 120 多起利用 Rafel RAT 恶意软件发动的攻击活动。而攻击目标则多为包括政府和军事部门在内的敏感组织，受害者大多来自美国、中国和印度尼西亚。

研究发现在大多数感染案例中，受害者使用的多是已经过时的 Android 版本，并且不再接收安全更新，因此容易受到已知或已公布的漏洞的攻击。所谓过时指的是 Android 11 及更早版本，此类设备在所有被攻击的设备中占比为 87.5%。而被攻击的目标品牌和型号，则涵盖了各种各样的产品：包括三星 Galaxy、谷歌 Pixel、小米 Redmi、摩托罗拉 One 以及一加、vivo 和华为的设备。这也证明 Rafel RAT 是一种能够有效攻击多种不同 Android 设备的攻击工具。Rafel RAT 的传播方式也很多，最常见的则是伪装成 Instagram、WhatsApp、电子商务平台或防病毒软件等来诱导人们下载其恶意 APK 安装包。

它所支持的命令因版本而异，但通常包括以下内容：

命令	描述
rehber_oku	将电话簿发送给控制服务器
sms_oku	将所有短信发送给控制服务器
send_sms	向指定号码发送短信
device_info	发送设备信息
location_tracker	将当前位置发送给控制服务器
arama_gecmisi	将通讯记录发送给控制服务器
screen_message	向受害者发送屏幕消息
wipe	删除指定路径下的所有文件
LockTheScreen	锁定设备屏幕
ransomware	启动文件加密进程
changewallpaper	更改设备壁纸
vibrate	进行设备振动 20s
deletecalls	擦除通讯历史记录
voice_message	用不同语言播放攻击者发来的文字信息
get_list_file	将指定路径的目录树发送给控制服务器
upload_file_path	将特定文件发送给控制服务器
application_list	发送所有已安装应用程序的列表

表 1. Rafel 指令表

根据研究，大约有 10%的案例中出现了“ransomware”命令。Rafel RAT 的勒索软件模块旨在通过控制受害者的设备并使用预先定义的 AES 密钥加密其文件来实施敲诈勒索计划。如果攻击者已经在设备上获得了

DeviceAdmin 权限，那么勒索软件就可以控制设备的关键功能，例如更改锁定屏幕密码和在屏幕上添加定制消息（通常是勒索通知）。如果用户试图撤销管理员权限，勒索软件还会立即更改密码并锁定屏幕。

研究人员发现，攻击者在执行加密模块之前通常会利用 Rafel RAT 的其他功能进行侦察。之后再通过清除通话记录；修改设备壁纸为自定义消息；锁定屏幕；激活设备振动功能；并发送了一条包含勒索信息的短信等一系列操作来要求受害者通过 Telegram 联系他们以“解决当前问题”。

Brain Cipher 攻击印度尼西亚数据中心

印度尼西亚正在建设国家数据中心用来安全地存储政府用于在线服务和数据托管的服务器。而就在 6 月 20 日，其中一个临时国家数据中心遭遇网络攻击，政府服务器遭到加密，同时移民服务、护照检查、活动许可发放以及其他在线服务也均被中断。当地政府证实此次袭击是由名为 Brain Cipher 的新勒索软件攻击造成的，影响了 200 多个政府机构。

而 Brain Cipher 方面则要求受害机构使用门罗币支付折合 800 万美元的赎金用以获取解密器，并防止泄露据称是在攻击中窃取的数据。媒体报道称，攻击者在谈判对话中表示他们将发布一份关于此次攻击中“个人数据保护质量”的“新闻稿”，这很可能意味着数据已被窃取。尽管该勒索软件团伙最初并未建立数据泄露网站，但他们在最新的勒索赎金通知信息中指向了一个网站，这意味着受害者的数据同样处于危险之中，并将可能被用于双重勒索的威胁之中。

据分析，Brain Cipher 是使用泄露的 LockBit 3.0 构建器创建的。与其他勒索软件类似，Brain Cipher 会入侵企业网络并横向传播到内网中的其他设备上。一旦攻击者获得了 Windows 域管理员权限，他们就会在整个网络中部署勒索软件。然而，在对文件进行加密之前，攻击者还会窃取公司的数据以便在后续的勒索行动中增加谈判筹码以及提高赎金金额。

Brain Cipher 在窃取数据方面也不例外，该组织最近推出了一个新的数据泄露网站，而目前该网站中所列出的唯一受害者就是印度尼西亚的数据中心。但在该数据泄露页面中，Brain Cipher 表示不会泄露盗取的数据，同时，会在 7 月 3 日时免费交出用于恢复被加密文件的密钥。对于本次攻击行为，该勒索家族解释为此次攻击仅是为了提醒受害者应重视安全防护。

黑客信息披露

以下是本月收集到的黑客邮箱信息：

Barbara.li@gmx.com	admin@stex777.xyz	bitsupportx@protonmail.com
emily.florez@zohomail.com	ramachandra7@india.com	bitsupportx@cock.li

getdataback@rambler.ru	5j3Kyz7F2@gmail.com	decrypt@europe.com
amaya_payne2@aol.com	decryptthelp@cock.li	reservereserv@airmail.com
nikki.lond2@aol.com	skynet45@cock.li	emmanuel.earsome@aol.com
admin@sectex.net	skynet45@tutanota.com	mclainmelvin@aol.com
admin@sectex.world	delta@onionmail.org	GetDecoding@zimbabwe.su
boost	delta@bingzone.net	getdecoding@msgsafe.io
boston.crypt@tuta.io	decryptinfo@protonmail.com	Client9522@tutanota.com
koreadec@tutanota.com	decryptinfo@cock.li	decfile1@protonmail.com
yourrealdecrypt@airmail.cc	future911@tuta.io	rapax123@protonmail.com
Enigmawave@zohomail.com	dragon2024@onionmail.org	michael_ethan@zohomail.eu
helpservice@cyberfear.com	dragon2024@tutanota.com	michael.ethan@onionmail.org
youhau@tutamail.com	paybit@aol.com	valorantskins108@gmail.com
China.Helper@aol.com	paybit765@aol.com	jinwooksransome@gmail.com
China.Helper@india.com	pexdatax@gmail.com	geometrical@geometrical.ransome.kr
sergev_petrov1983@mail.ru	admin@spacedatas.com	duca17512@gmail.com
clovergroup@skiff.com	teamdecrypt@disroot.org	lord_bomani@keemail.me
Helpyoudc1966@Gamil.com	teamVV@cock.li	jbomani@protonmail.com
zkungfu@skiff.com	xcsset@criptext.com	Bomani@Email.Com
anony@mailum.com	xcsset@aol.com	salesrestoresoftware@firemail.cc
ithelp08@decorous.cyou	squadhack@email.tg	salesrestoresoftware@gmail.com
ithelp08@wholeness.business	back_data@foxmail.com	getbtc@aol.com
mail4restore@swismail.com	getdecoding@protonmail.com	steloj@bk.ru
welcome24dat@outlook.com	prancesonce@tuta.io	steloj@lycos.com
returnal_data@proton.me	prancesonce@cock.li	stelo@onet.eu
returnaldata@airmail.cc	ebc83e48b03b390223e3f0b9eb2983d6	admin@fentex.net
returnal_data@tuta.io	operator@cypherx.info	admin@fentex.world
AdminLoki@onionmail.org	Operatorb@cock.li	admin@datastex.club
LokiAdmin@mail2tor.com	fidelio.bartyn@aol.com	dkqcnr@cock.li
8filesback@onionmail.org	glynnaddey@aol.com	d.hanry@tutamail.com
foo8tbFpc@gmail.com	888@cock.email	LBfdgpo.info.ru@onionmail.com
my0day@aol.com	getscoin3@protonmail.com	Rdpdik6@gmail.com
daysupp@aol.com	getscoin@tuta.io	Rdpp771@gmail.com
biashabtc@redchan.it	decrypt@files.mn	purchase@lnt-corp.com
Bit_decrypt@protonmail.com	techwin@post.cz	xwolf69@onionmail.org
1Buba@protonmail.com	timesungroup@skiff.com	admin@lntdeal.com
filesgetback@protonmail.ch	marshall@airmail.cc	purchase@lntdeal.com
getthefiles@airmail.cc	orderof@tuta.com	devos-2686@libertymail.net
fastrecovery@onionmail.org	Rileyb0707@aol.com	support@bloomscollect.com
fastrecovery2@msgsafe.io	Rileyb0707@cock.li	93048decoder@tutanota.com
restoreassistance@decorous.cyou	tiprltd@skiff.com	pasomnicadecryption@gmail.com
restoreassistance@wholeness.business	bluecrap8@gmail.com	NJUnju@skiff.com
BAD.JERRY@AOL.COM	bluecrap@my.com	frankmoffit@aol.com
BADJERRY@COCK.LI	diane.freen2@aol.com	emcrypts@tutanota.de

admin@stex777.com	opalburgh@aol.com	russoschwartz@onionmail.org

表 2. 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）。

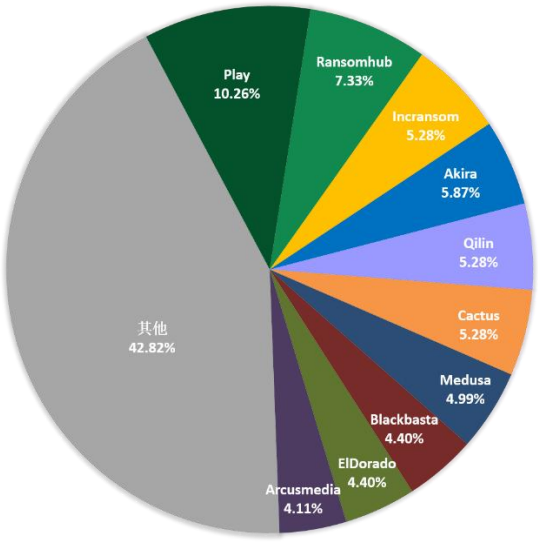

图 4. 2024 年 6 月通过数据泄露获利的勒索软件家族占比

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 340 个组织/企业遭遇勒索攻击，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 5 个组织/企业未被标明，因此不在以下表格中。

Wayne Memorial Hospital	Exhaustpro shops	Concrete
a4hs-dom.local	Sacred Heart Community Service (shcstheheart.org)	manncorp.com
lambertz.de	Gorrie-Regan	sgvfr.com
life.vet.br	BankSelfStorage	CBSTRAINING
jla.com	Tri-City College Prep High School	www.novabitsrl.it
pandacare.ae	Fitzgerald, DePietro & Wojnas CPAs, P.C.	smicusa.com
DRM Resources	AJE	www.ham.org.br
Clima Lodi	GED Lawyers & ..	Seafrigo
DatAnalítica	CIFSOLUTIONS.COM	Special Health Resources

Freightliner of Grand Rapids & Kalamazoo	Gokals Consumer Electronics & Computers Retail · Fiji	NJORALSURGERY.COM
Puyallup Tribe (ptoi.local)	Basement Systems	WinFashion ERP
City Of Coon Rapids	ASST Rhodense	Kutes.com
Cambridge University Press & Assessment	Maintel	apex.uk.net
Spandex.com	Access Group	AlphaNovaCapital
midamea.com	SAWA INTERNATIONAL	AMI Global Assistance
Wilmots (Legal services)	www.invisio.com	filmetrics corporation
Power Lube Industrial	Behavioral Health Response (bhr.local)	CentralSecurities.com
ASI	Synnovis	Embotits Espina, SLU
Francesco Parisi	suminoe.us	a-agroup
Gestores Administrativos Reunidos	Lindermayr	Harper Industries
GBA GROUP	Perfumes & Companhia	nordspace.lt
equinocioplay.com.br	DERBY SCHOOL	Arge Baustahl
www.cipl.org.in	First Baptist Medical Center	www.ugrocapital.com
buyeazzy.com	Circle K Atlanta	transportlaberge.com
promarkbrands.com	kinslerfamilydentistry	sanyo-shokai.co.jp
landmarklife.com	sofidel.com	wave2.co.kr
www.mangimifusco.it	sky-light.com	jmthompson.com
www.cloudeurope.it	reawire.com	ctsystem.com
coca-cola.com - Myanmar office	malca-amit.com	ctgbrands.com
daniellegroup.com	www.gbricambi.it	SolidCAM
conferenceusa.com	Seoyon E-Hwa	Rockford Public School District
KADOKAWA Corporation	GIANNI CUCUINI	CONTROLNET
Total Revisjon DA	OCEANAIR	EvoEvents
Ontario West and Bill Blaney Insurance Brokers	The Kansas City Kansas Police Department	Barrett Eye Care
North Coast Petroleum	northcottage.com	Parrish-McCall Constructors
Longviewbridge.com	St Vincent de Paul Catholic School	California Rice Exchange
Ruland-viersen.de	wielton.com.pl	Allied Toyota Lift
Ocasa	grupoamper.com	Hoppecke
Gallos Metal Solutions	TETRA Technologies, Inc.	Jones
Waterbury Newton	A-Line Staffing Solutions	Elite Limousine Plus Inc
YKS	www.liderit.es	ccmaui.org
US Dermatology Partners	Sensory Spectrum	talalayglobal.com
Better Business Bureau	Acteon Group	akdenizchemson.com
Utility Datacenter	pkaufmann.com	Reinhold Sign Service
PCI Developments	modplan.co.uk	Axip Energy Services
Beckett Thermal Solutions	parlorenzo.com	aloft
competenz.co.nz	www.domainatcleveland.com	RAVEN Mechanical
decreditos.com	Virum Apotek	dmedelivers.com
Planar	Next Step Healthcare	fpr-us.com

rbbschools.net	cosimti.com	Panasonic Australia
axiavg.com	fifcousa.com	dynasafe.com
keybenefit.com	mgfsourcing.com	robson.com
scrubsandbeyond.com	journohq.com	elutia.com
ibewlocal1.org	Production Machine & Enterprises	ssiworld.com
doityoungs.com	CETOS Services	driver-group.com
keeservices.com	Kiemle-Hankins	TBMCG.com
theeyeclinicsurgicenter.com	Legrand CRM	www.vet.k-state.edu
sanglier.org.uk	MRI	www.uccretrievals.com
arangobillboard.com	Ma'agan Michael Kibbutz	HTE Technologies
tpocc.org	Oahu Transit Services	goughhomes.com
middletown-township.org	Sun City Pediatrics PA	Baker Triangle
www.harrisranchbeef.com	InVogue Women Healthcare, PLLC (USA,TX)	www.tankerska.hr
www.concisa.eng.br	Lee Trevino Dental (USA,TX)	cityofpensacola.com
hydmech.com	Peregrine Petroleum	thunderbirdcc.org
westfalia-automotive.com	svmasonry.com	www.itasnatta.edu.it
Agron (Five Ten) Adidas TERREX	EnviroApplications	panzersolutions.com
multi-wing.com	MBE CPA	lindostar.it
bitzsoftwares.com.br	New Balance Commodities	burotec.biz
www.sicoob.com.br	www.gannons.co.uk	celplan.com
Compagnia Trasporti Integrati S.R.L	Victoria Racing Club	adamshomes.com
VTWin.ca	Mundocar.eu	Health People
Revolution Resources	Diogenet S.r.l.	IPPBX
TPI	Dordt University	Market Pioneer International Corp
Harvey Construction	Borrer Executive Search	Mercy Drive Inc
Belle Tire	www.bigalsfoodservice.co.uk	Radiosurgery New York
Hedrick Brothers Construction	Cukierski & Associates, LLC	Inside Broadway
World inquest	www.racalacoustics.com	Oracle Advisory Services
Bunger Steel	2K Dental	Women's Sports Foundation
RRCA Accounts Management	Kito Canada	www.crezit.com
ProMotion Holdings	Bock & Associates, LLP	Moshe Kahn Advocates
Custom Concrete	Walder Wyss and Partners	craigsteven.com
federalreserve.gov	Celluphone	Elfi-Tech
Ladco	Me Too Shoes	Davis & Young
millimages.com	Ab Monsteras Metall	E-T-A
www.glynmarais.co.za	Amarilla Gas	Dubai Municipality (UAE)
hundhausen.de	Aldenhoven	www.clevo.com.tw
fbttransport.com	Refcio & Associates	Premium Broking House
daystar.com	City Builders	Vimer Industrie Grafiche Italiane
qftemb.com	Eurotrol B.V.	Voorhees Family Office Services
deskcenter.com	Seagulf Marine Industries	Mahindra Racing
Zerto Security	Western Mechanical	naprodgroup.com

marvell.com	Trisun Land Services	Madata Data Collection & Internet Portals
at-global.com	GEMCO Constructors	Río Negro
City of Newburgh	Dynamo Electric	Mountjoy
Erivan Gecom Inc	Farnell Packaging	Langescheid GbR
CBIZ, Inc	Diverse Technology Industrial	Franja IT Integradores de Tecnología
Greenheck Fan	Air Cleaning Specialists	Duque Saldarriaga
Rotor Team	Corbin Turf & Ornamental Supply	BHMAC
Heli Securite	Kinter	Botselo
BLADE	Goodman Reichwald-Dodge	Immediate Transport – UK
Maryhaven (MHCLINICAL.LOCAL)	3GL Technology Solutions	Above All Store Fronts
Ashtons Legal LLP	Brainworks Software	PFAM
MEL aviation Ltd	Eagle Materials	Logimodal Operações Logísticas
Longview Oral & Maxillofacial Surgery	Great Lakes International Trading	cfymca.org
prinsotel.com	Smartweb	Northern Minerals Limited
oexpress.id	Peterbilt of Atlanta	ISETO CORPORATION
LCS and Partners	Chroma Color	Nidec Motor Corporation
Topserve Service Solutions	Shinnick & Ryan	Anderson Mikos Architects
TC Capital Asia Limited	ZeepLive	smithandcaugheys.co.nz
Wise Construction	ANTECH-GUTLING Gruppe	Wealth Depot LLC Data Leak
Taiyo Kogyo Co., Ltd.	hydefuel.com	Frontier
Hokushinko Co., Ltd.	IPM Group (Multimedia Information & Production Company)	

表 3. 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 10 以及 Windows Server 2016。

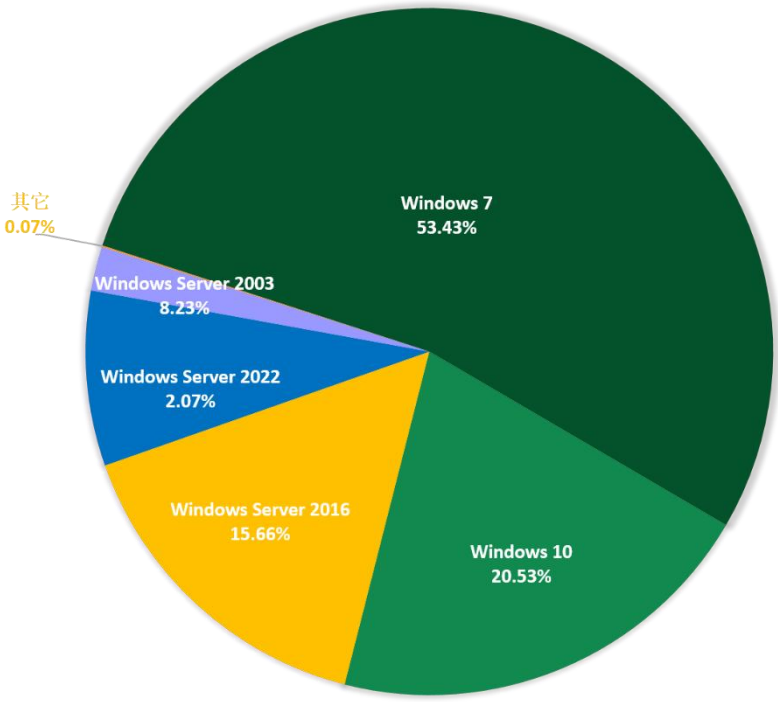

图 5. 2024 年 6 月受攻击系统占比

对 2024 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。

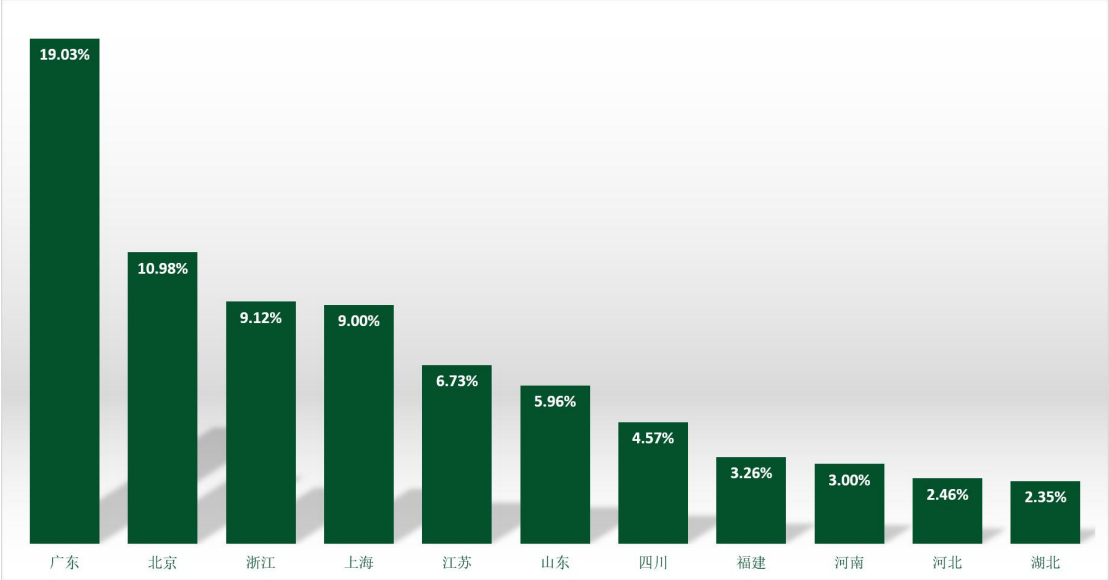

图 6. 2024 年 6 月国内受攻击地区占比排名

通过观察 2024 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。

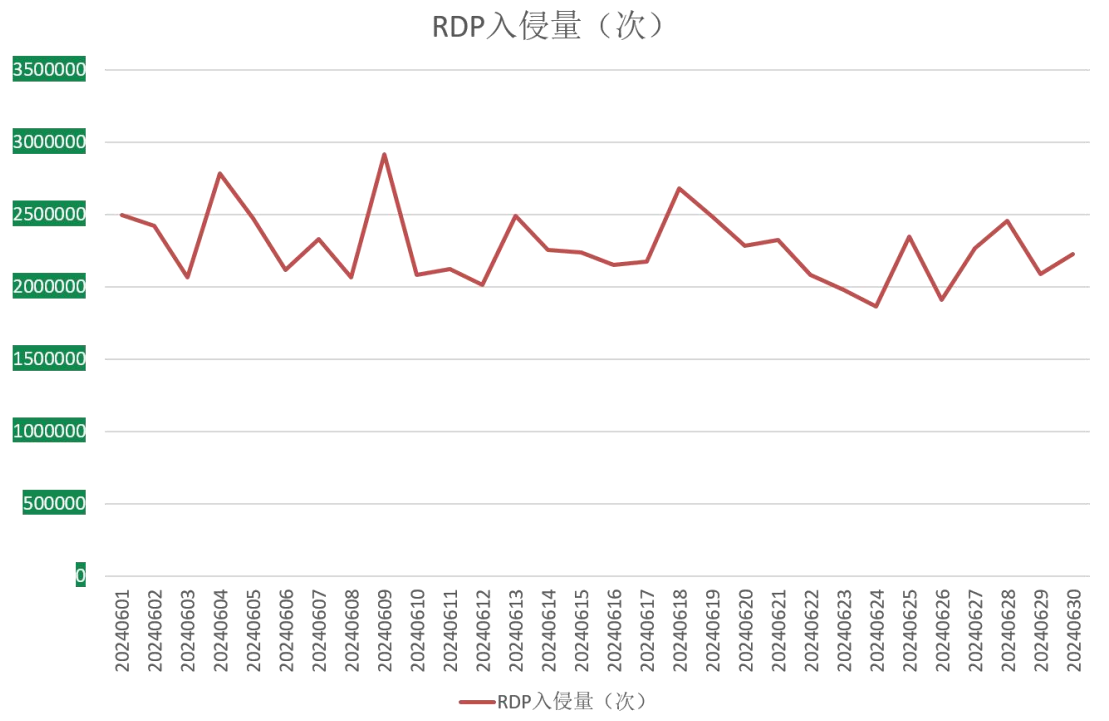

图 7. 2024 年 6 月监控到的 RDP 入侵量

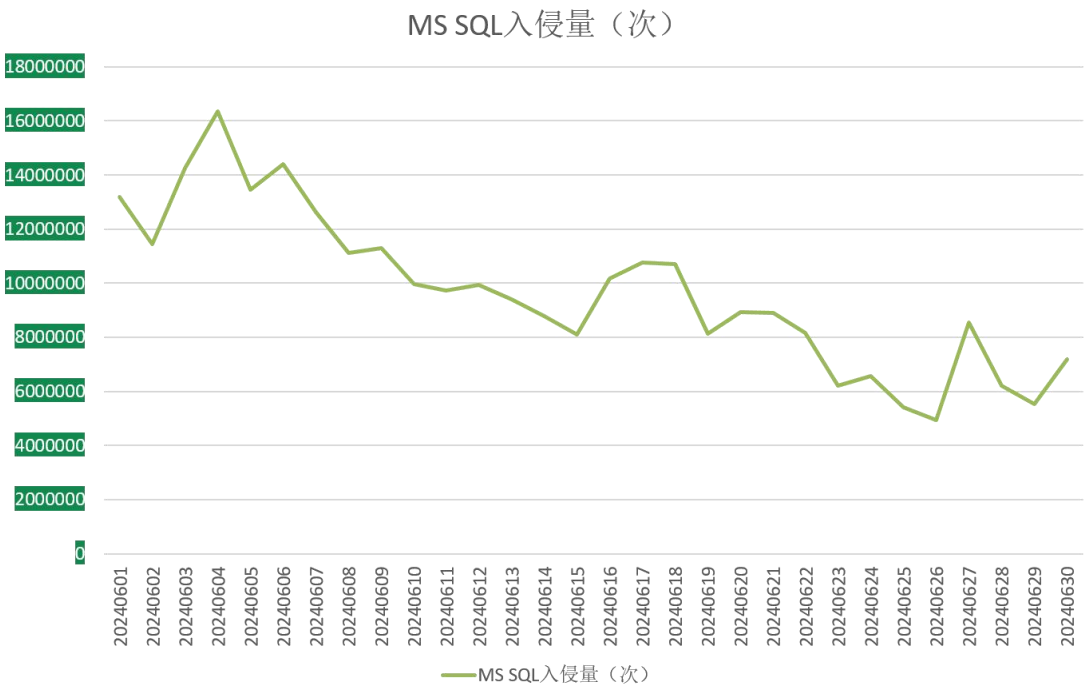

图 8. 2024 年 6 月监控到的 MS SQL 入侵量

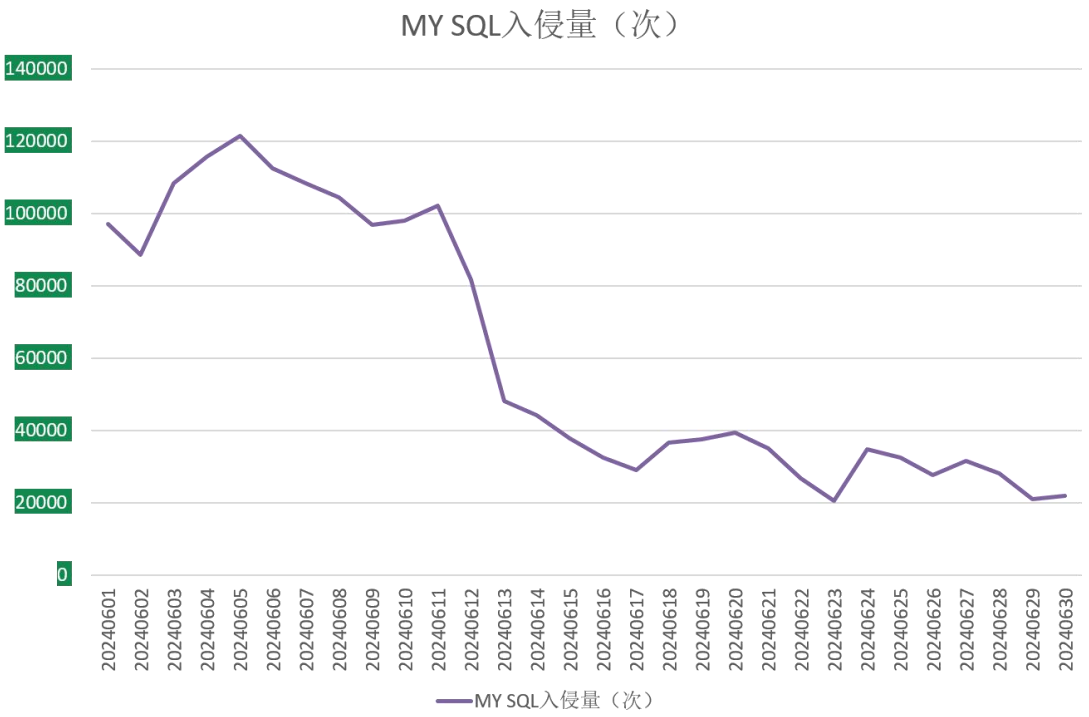

图 9. 2024 年 6 月监控到的 MYSQL 入侵量

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。

- hmallox：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，今年起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本曾通过匿影僵尸网络进行传播。

- 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。

- svh：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。

- anony：属于 Anony 勒索软件家族，由于被加密文件后缀会被修改为 anony 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：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与数据库弱口令成功后手动投毒。

- 360：同 halo。

- src：同 svh。

- rmallox：同 hmallox。

- mallox：同 hmallox。

- faust： 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。

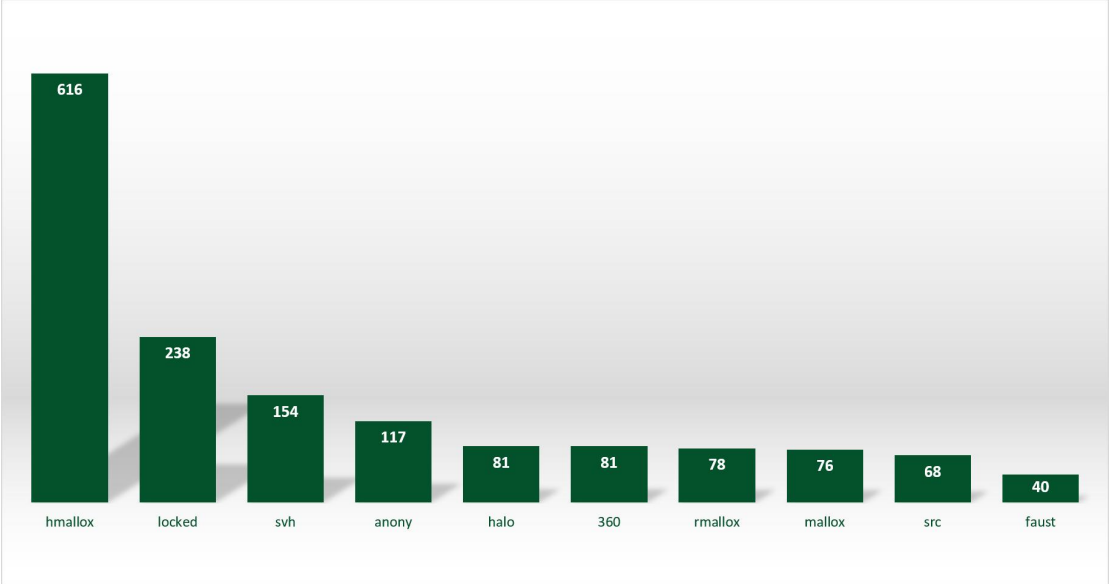

图 10. 2024 年 6 月反病毒搜索引擎关键词搜索排名

解密大师

从解密大师本月解密数据看，解密量最大的是 Crysis 其次是 Buran。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。

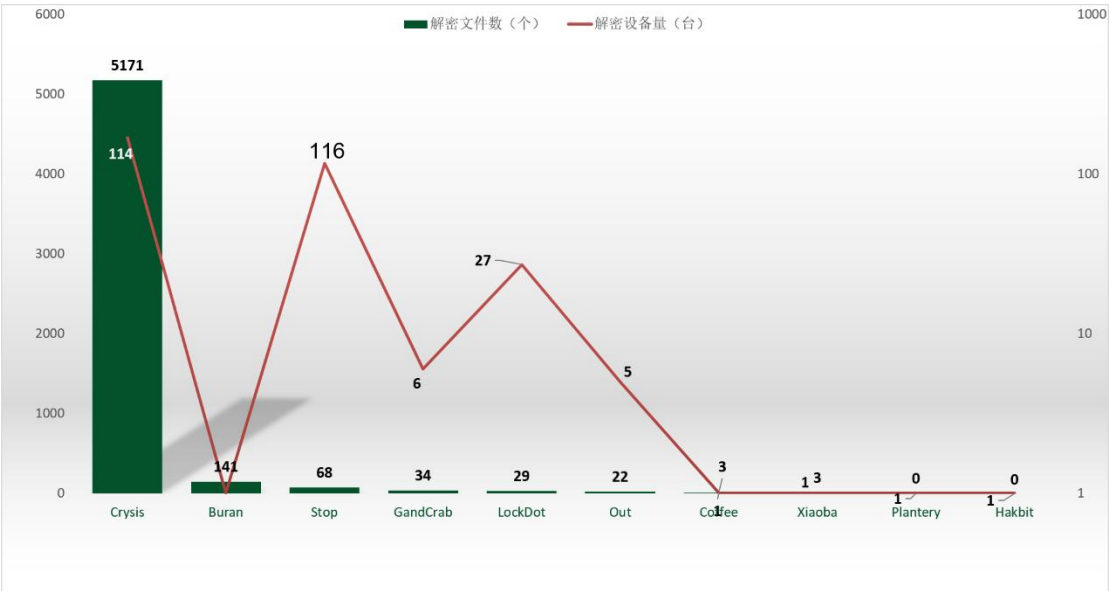

图 11. 2024 年 6 月解密大师解密文件数及设备数排名


360数字安全
数 字 安 全 的 领 导 者
360安全大脑