新闻热线：010—58884061
E-mail：liangyx@kjrb.com
■责编 梁彦晓
科技日报
2020年6月4日 星期四

视觉中国供图

为防犯罪分子染指，斥资160万美元购买“魔鬼域名”
靠微软一己之力很难扛起域名安全这杆大旗

本报记者 **刘 艳**

看得见的安全风险，永远只是冰山一角。

近期，被称为史上最危险域名的corp.com被微软出资160万美元购买，结束了长达26年的僵持。虽然这项举动切断了网络犯罪分子染指滥用该域名的可能，但并不意味着域名系统（DNS）防护从此可以高枕无忧。

随着物联网应用的迅速普及、5G覆盖提速，加强域名系统安全防护能力已成当务之急。

微软封印“魔戒”，买下史上最危险域名

域名就是网址，谁先注册谁就拥有使用权，它就像互联网空间的门牌号，网站有了域名才能够被访问。

corp.com注册于1994年，一直以来被业界称作“魔鬼域名”，这是因为任何人只要拥有corp.com，就能访问全球主要公司数十万台Windows系统电脑端当中海量密码、电子邮件和其他敏感数据。为什么会这样？个中的原因，还要从微软的Windows操作系统说起。

Active Directory（活动目录）服务是Windows平台的核心组件，企业或组织内网的Windows计算机用它来验证网络上的其他内容，参与本地网络的域名解析。

但是，支持Active Directory的Windows早期版本默认Active Directory路径被指定为“corp”，不少公司没有修改二级域名，而是直接采用了此设置。于是，当他们的员工在公共网络访问该路径时，Windows会尝试将“corp”解析为“corp.com”公有域。

当一个原本在内网使用的域名在公共互联网上解析时，不管是否有意为之，DNS名称空间冲突都会发生。这意味着，敏感数据有可能瞬间流向外网被“分享”到corp.com站点。

据公开报道，2019年，安全专家杰夫·施密特（Jeff Schmidt）在对流向corp.com的企业内部流量分析中发现，有超过37.5万台Windows系统电脑端尝试发送信息，包括尝试登录公司内网及访问网络上的特定共享文件。测试期间，这个安全团队还一度模拟本地Windows网络登录和文件共享环境接管了对corp.com的连接请求，1小时内，corp.com就收到了超过1200万封邮件，其中包括了大量的敏感信息。通过这次实验，施密特等人得出结论：控制corp.com的人极有可能会拥有一个遍布全球的计算机僵尸网络。

多年来，微软发布数个软件更新，试图消除corp.com的潜在威胁，但部署这些修复程序的易受攻击企业并不多。

另外，某网络安全公司工程师告诉科技日报记者：“Active Directory安全机制的先天缺陷很难通过安全更新彻底根除，就如网友所说‘拥有了corp.com就如同获得了魔戒’，企业内部设备访问外网时，有可能向域名控制者发送企业内网敏感信息并不是理论推断，很有可能就是现实。”

那么，微软买下corp.com域名，是不是等于彻底消除了那些将Active Directory构建于“corp”或“corp.com”上的全球客户头顶的“雷”？

对此，微软未做过多回应，只是强调用户安全至上是承诺。有安全专家指出，信息安全领域，不存在绝对的安全承诺。不仅是corp.com，将内部Active Directory网络与任何不受控的域名“绑在一起”都存在安全风险。从目前来看，及时下载安装最新的安全补丁，是免遭漏洞恶意攻击的有效手段。

域名并非生意，安全始终是最深隐患

或许是因为资源有限，也或许是过往域名致富的故事太多，如今，人们更愿意把域名当成一门生意来谈论，相比之下，对安全问题的关注度低了很多。

事实上，尽管全世界的工程师们一直在努力改善域名系统的安全性和抗攻击性，但针对域名系统的攻击依旧是互联网最重大威胁之一，由此引发的安全事件也是层出不穷。

从2009年5月19日晚19点左右开始，我国江苏、安徽、浙江、广西、海南、甘肃六省连续两天出现严重网络故障，很多用户发现网速变慢或者干脆无法访问网站。两天后，相关部门通报这起著名的“519断网事件”，原因为暴风影音网站的域名解析系统受到网络攻击，持续不断地发送大量联网请求，最终造成了大面积的网络堵塞。

2019年2月19日，国家互联网应急中心监测发现，部分用户通过家用路由器访问某些网站时被劫持到涉黄涉赌网站，发生域名劫持的家用路由器DNS地址被发现是有黑客恶意篡改，这次的破坏规模达到400余万个IP地址。

国家互联网应急中心发布的通报显示，很大一部分网络挟持的源头是“放马站点”。“所谓的‘放马站点’，就是被注入了木马的网站。”知名网络安全公司奇安信的工程师介绍，网络病毒主要在一些防护弱、访问量大的网站通过网页“挂马”的方式进行传播，当用户访问这些被黑客“挂马”的网站时，就会被暗中连接到黑客最终“放马”的站点而中毒。

清华大学奇安信集团联合研究中心主任段海新介绍，作为互联网重要的基础设施，域名系统不仅提供了上网必须的域名解析服务，还提供了应用层的路由和负载均衡，作为信任基础提供了邮件服务器的验证、证书申请时域的控制权验证，基于DSSSEC（域名系统安全拓展）还可以提供公开密钥基础设施服务。

段海新强调：“DNS是很多网络服务的基础，域名系统的一点小问题就是互联网的大问题。”

建设数字基础设施，不能放松网络安全

因为运营维护技术复杂且成本较高，域名安全成为了网络安全领域最薄弱的环节之一。如今，域名安全面临的威胁有可能呈几何级增长。因为，如今的移动互联网、物联网及5G依然需要域名系统支持，并且已逐渐深入我们的生活，很多未知的安全威胁随时有可能出现。

物联网通过海量的互联传感器和设备逐渐与我们的现实环境无缝对接，与传统互联网应用最大的不同是，在物联网设备持续不断地与域名系统的交互中，数据交换通常被动产生，没有人员的参与。

2019年9月，互联网名称与数字地址分配机构（ICANN）安全与稳定咨询委员会发布的《SAC105报告》提示，物联网的僵尸网络可以针对互联网基础设施启动大规模分布式拒绝服务（DDoS）攻击，感染成百上千的设备。由于此类设备通常可在无人照管的情况下运行，因此给根除这些僵尸网络造成了很大困难。

针对物联网设备的攻击让我们见识了新威胁的发起途径和严重程度，而5G网络的新型组网与接入方式、边缘数据中心及服务化架构的核心网将面对何等安全挑战，传统安全模式是否适应5G安全建设的需求等一系列5G安全问题也正成为业界更为关注的课题。

工业和信息化部副部长陈肇雄强调，网络安全保障系统要与5G等数字基础设施同步规划、建设、运行，加强5G、工业互联网、数据中心、云平台等设施的安全保障，确保数字基础设施安全平稳可靠运行。

中国工程院院士邬贺铨指出，很多安全挑战是内生的，从基础设施技术开发与网络设计开始就要有内生的安全理念。网络安全能力与基础设施是一个整体，网络安全能力需与基础设施同步建设并融入其中。

360集团董事长兼CEO周鸿祎则表示，万物互联时代，越来越多的未知漏洞将会被利用，但短期内仍然无法通过一整套AI系统自动发现并抵御安全风险，仍需要发挥高水平攻防专家的力量，网络安全的最后战场依然是人与人的对抗。

慎点！来历不明的疫情邮件或是黑客陷阱

实习记者 **于紫月**

如果邮箱里收到标题为《新冠肺炎的诊断和预防措施.xlsm》《武汉旅行信息收集申请表.xlsm》等看似与疫情密切相关的邮件，相信有人会忍不住进行查看。殊不知，鼠标轻轻一点，也许你就踏入了黑客的陷阱。

近期，360技术团队称，在抗疫期间发现有境外黑客组织不断尝试窃取我国医疗卫生行业的相关机密，使用“白利用”手法绕过了部分杀毒软件的查杀，利用新冠疫情题材诱使用户执行木马程序，最终达到控制系统、窃取情报的目的。

事实上，遭受攻击的受害者并非只在我国出现。据此前360发布的报告，该黑客组织发动的高级可持续威胁攻击（APT攻击），涉及地域十分广泛，至少还包括境外36个国家。


视觉中国供图

攻击方式隐蔽难缠

“‘白利用’手法是较为常见的一种网络攻击方法。攻击者通过精心制作木马病毒，利用看起来是‘白名单’之内的文件来实现木马攻击。”近日，北京理工大学计算机网络及对抗技术研究所所长闫怀志接受科技日报记者采访时这样表示。

“具体来说，‘白利用’主要的技术核心是通过移形换影，将远程控制木马进行伪装，并且隐藏在防护系统白名单内的文件中，以此来蒙混过关。”闫怀志进一步解释，“白利用”手法具体有两种实现途径，一是通过正常程序自身的漏洞使该程序可被远程控制，二是木马制作者利用社会工程学等方法，让木马躲过恶意代码查杀工具和沙箱（一种网络编程虚拟执行环境）等主动防御机制，从而鱼目混珠，混入白名单之中。

现有资料显示，“鱼叉攻击”“水坑攻击”等APT攻击手法是该黑客组织的惯用伎俩。

闫怀志告诉科技日报记者，“鱼叉攻击”是钓鱼攻击的重要形式之一，通常将木马病毒作为电子邮件的附件，邮件主题和附件通常会起极具诱惑力的名称，诱使受害者打开附件，从而感染木马，导致目标人群“中招”。“水坑攻击”则是利用被攻击目标经常访问的网站漏洞植入攻击代码，构造一个陷阱，一旦被攻击目标访问该网站即会陷入“水坑”，成为攻击者的“囊中之物”。

需要注意的是，“水坑攻击”无需专门制作钓鱼网站，而是利用了合法网站的脆弱性，因而具有更高的隐蔽性。

根据360此前发布的安全报告可以得知，APT攻击具有针对性强、潜伏期长、攻击覆盖面广等特点。此次发动攻击的黑客组织至少使用了4种不同程序形态、不同编码风格和不同攻击原理的木马程序，恶意服务器遍布全球13个国家，注册的已知域名多达35个。

“这些APT攻击往往使用精密、复杂的恶意程序及技术，持续监控特定目标，潜伏期极长，攻击者对受害者的网络保有控制权的平均时间为一年，最长可达数年。”闫怀志指出，APT攻击非常难缠，通常令人难以招架，发现和防御极为困难。

亟须构建网络空间“雷达”

小到人们的日常生活，大至一个国家的经济、政治、军事及社会稳定，黑客攻击导致的安全事件危害不容小觑。在全球抗击疫情的特殊时期，黑客攻击抗疫一线的组织机构，其心可诛。

“网络攻击是各国面临的共同威胁，在当前新冠肺炎疫情蔓延全球的背景下，针对抗疫机构的网络攻击无疑应当受到全世界人民的同声谴责。”此前，我国外交部新闻发言人耿爽表示。

科技日报记者了解到，不同于以往制造木马病毒的“小毛贼”，此次APT攻击的实施者已经发展为国家级的“大玩家”，其攻击对象直指各类关键基础设施，攻击手段更是层出不穷、防不胜防。尤其是此次黑客攻击利用了新冠肺炎疫情相关题材为诱饵，医疗机构、医疗工作领域无疑会成为首要目标，一旦其攻击得逞，轻则导致数据丢失，引发计算机系统故障，重则影响疫情防控工作推进，后果不堪设想。

“网络安全是国家安全的核心要素，政治安全、经济安全、文化安全、军事安全等，都与网络安全密切相关、相互作用。”闫怀志表示。

在360集团董事长兼CEO周鸿祎看来，构建网络空间“雷达”，发现敌人之所在是赢得这场战争的关键。“这就像现代战争中没有雷达，有再多的火炮和导弹也只是摆设一样。应对APT攻击的关键，首先在于要看得见，而要看得见，不能靠肉眼，不能靠陈旧的思维，必须靠更为先进的‘雷达’。”

他认为，打造网络空间“雷达”需要3个必要条件：安全大数据是看见的基础，威胁情报和知识库帮助筛选，高级别攻防专家起决定性作用。三者结合，才能真正有效进行防御。

行业观察

建工业互联网大数据中心体系 实现对数据统一管理和使用

本报记者 **崔 爽**

“新基建”无疑是今年的热门词，而5G和工业互联网这两项支撑性技术的联手，既是新基建建设的重头戏，更是发展数字经济、提升全社会智能化水平的关键。

面对新冠肺炎疫情的影响，很多制造企业尤其是中小企业无法正常复工，给企业经营带来挑战。在联想集团董事长兼CEO杨元庆看来，“通过工业互联网催生更多数据，充分利用大数据工具和人工智能算法，可以改进各行各业效率和决策方式，加快各行各业智能化步伐”。

提高数字化水平是实现工业互联网的基础

对传统制造企业来说，用工业互联网来破题这条路不好走，第一道坎就是传统制造企业普遍偏低的数字化水平。中国移动集团公司董事、浙江移动董事长郑杰指出，传统制造业特别是中小企业的设备联网率目前还很低，工业无线技术体系主要是基于低速率、局域网的无线短距离通信，针对高速率、广覆盖、大流量的工业无线网络技术标准尚不明确；工业领域的传输协议多达数百种，协议之间兼容性差，第三方解析能力弱，各类工业数据无法整合，互联互通难。“制造企业内网改造在网络互联、数据互通、应用创新等方面具有较大阻力。”郑杰表示。

中国工业互联网研究院院长徐晓兰同样强调了这一问题已经成为了企业提速增效、高质量发展的掣肘。“目前我国企业特别是中小企业的数字化水平较低，我国有超55%的企业尚未完成基础的设备数字化改造。制造业中小微企业发展较为粗放，税后利润仅为3%—5%，无法承受数字化转型和新技术应用的高昂成本，因此中小企业缺乏数字化转型的动力。”徐晓兰说，而另一方面，行业间整体数字化发展水平差距较大，超过50%的中国制造企业的数字化尚处于单点试验和局部推广阶段，应“因‘业’制宜推进不同行业的数字化进程”。

大数据中心体系可解决数据“孤岛”问题

徐晓兰表示，一方面，不同行业具有各自的行业特征，在考虑从顶层推进行业的数字化进程时，需要考虑到行业中生产者和消费者的特征及需求，从而以适当的政策扶持、经济激励来助力行业数字经济的发展。另一方面，通过推动工业互联网行业应用做深、做透，利用工业互联网联合创新中心，找准行业发展的痛点、难点和堵点，提出应用共性和个性问题、促进行业数据流动、打破行业壁垒，构建跨层级、跨地区、跨系统的国家级数据平台，彻底解决行业数据“孤岛”问题。

她尤其强调了国家级数据平台的重要意义。本次疫情防控中，国家工业互联网大数据中心广泛汇聚医院、企业、政府、社会组织等2800余家单位的疫情防控物资需求，发布物资需求达5670多万件，形成对240余万家中小企业复工复产的全方位监测，为“全国一盘棋”提供了有力的数据支撑。

不过，呈爆炸性增长之势的工业互联网数据，却还被孤立、分散、封闭等问题限制，不但制约了数据价值的高效利用，还带来了数据主权和数据安全等问题。为此，徐晓兰认为，虽然已成立国家级工业互联网大数据中心，但要实现对数据的统一管理和使用，还需建设国家工业互联网大数据中心体系，“应将国家工业互联网大数据中心的建设纳入到新基建的重大项目中，以彻底解决数据‘孤岛’问题。”徐晓兰说。

专家呼吁加码个人隐私保护 建立数据全生命周期管理

本报记者 **崔 爽**

日前，我国首份从消费者角度出发，评价数字经济服务质量的《中国数字经济服务质量满意度DES-CSI测评研究报告》发布。报告显示，61.3%的消费者认为目前数字经济服务相关法律法规的健全程度及个人隐私安全保护方面还有很大的提升空间，主要体现在即时通信服务业态上个人隐私安全性的保护。

数据是资产、数据有价值已经是一种社会共识，与此同时，伴随信息的过度收集、未经用户同意收集的争议也由来已久。

按照国家推荐性标准《信息安全技术 个人信息安全规范》的提示，对用户个人信息的收集应有明确的目的，不得超出产品功能相关目的收集额外信息。但在实际生活中，用户在面对无法弃用的各类App时，往往少有“无可奉告”的自由。

“考虑到App类型多样，行业主管部门可以通过发布指南等方式为类型化的业务场景规定信息收集范围。明确权限，细化管理。”北京师范大学网络法治国际中心执行主任、中国互联网协会研究中心秘书长吴沈括表示，如根据全国信息安全标准化技术委员会发布的《信息安全技术 移动互联网应用（App）收集个人信息基本规范（草案）》，个人征信信息须经用户授权查询；金融借贷类App可收集紧急联系人信息，但仅限两人；App应允许用户手动输入联系人信息，而不应强制读取通讯录。

而对于最高级别的生物识别信息，保护力度也自然应是最高级别。生物特征识别技术，尤其是人脸、指纹、虹膜、掌静脉、声纹、步态形体以及基因等识别技术，正在广泛地应用于智能产品中，也暴露出严重的安全问题。生物识别信息无法更改，一旦泄露，个人可能终身暴露在被攻击和骚扰的风险中。因此，有业内人士认为，应明确参与数据全生命周期环节的各类主体，严厉打击各种窃取、滥用、篡改、泄露等非法使用数据的行为。

“针对数据处理全生命周期，就所涉及的各方主体明确权责义务是数据规范化治理的核心。关键点在于实现个人权益、产业利益与社会国家利益在具体场景中的合理平衡。目前社会各界最迫切的需求是数据流转规则体系的建设与落地。”吴沈括解释道。

另外，百度董事长李彦宏也认为，针对特殊时间段采集的个人信息，可以设立退出机制，并加强对已收集数据的规范性管理，研究制定特殊时期的公民个人信息收集、存储和使用的标准和规范。