新闻热线：010—58884062
E-mail：adaxuqian@126.com
■责编 许 茜
科技日报 2020年1月22日 星期三

僵尸网络横行，“豌豆射手”难觅

实习记者 **于紫月**

近日，国家互联网应急中心发布报告称，2018年我国基础电信企业、域名服务机构等成功关闭了772个规模较大的僵尸网络。同时，网络安全公司ESET前不久发布研究报告称，一个名为“Stantinko”的僵尸网络正在操控全球数以万计的计算机挖掘加密货币“门罗币”。

这一日益猖獗的僵尸网络究竟是何方“神圣”？它的攻击能力如何？在游戏“植物大战僵尸”中，豌豆射手是抵御僵尸进攻的主力。那么，目前在网络安全领域是否有“豌豆射手”呢？

针对上述问题，科技日报记者采访了业内相关专家。

黑客可随意驱使被感染设备

在恐怖电影中，我们经常能看到这样的场景：一群僵尸疯狂地追逐、攻击人类，却在“赶尸人”面前非常老实、听话。

“僵尸程序就是如此，被其感染的硬件设备，就如同僵尸群一样可以被随意驱使、控制，成为被人利用的工具。”北京理工大学计算机网络及对抗技术研究所所长闫怀志对科技日报记者说，僵尸程序是指恶意控制硬件设备功能的一种程序代码，它能够自动执行预定义的命令。大量主机感染僵尸程序后，在僵尸程序控制者和众多被感染主机之间会形成一对多的被控制网络，这就是僵尸网络。

“危害性大的僵尸网络具有较强的传染性，同时被严格地控制着。”北京交通大学计算机与信息技术学院信息安全系主任王伟在接受科技日报记者采访时表示，所谓传染性就是说，该“僵尸”样本不仅具备与计算机病毒类似的特点，还可感染与其相邻的其他硬件设备。但与计算机病毒不同的是，僵尸网络高度可控，其具有金字塔式的控制结构：位于底层的是数量庞大的被感染主机，处在塔尖的则是网络攻击的发动者，即整个僵尸网络的控制者。

王伟强调，传统的计算机病毒具有一定的破坏性，更高级一些的病毒，如蠕虫病毒等，虽具有传染性，但发布者很难对其进行有效控制。相比之下，僵尸网络则既具有较强的传染性又可被有效控制，因而危害性更大、攻击力也更强。

闫怀志介绍道，当前，大多数僵尸网络使用互联网中继聊天（Internet Relay Chat，IRC）协议来实现通信和控制。1999年，“SubSeven 2.1”发布，该程序利用IRC网络构建出攻击者对僵尸主机的控制信道，被认为是世界上首个真正意义上的僵尸程序。随后，黑客们开始借助蠕虫病毒促进僵尸程序的主动传播，并进一步采用P2P结构构建控制信道，进而加速了僵尸网络的泛滥。

发动僵尸网络攻击门槛低

“近年来，僵尸网络攻击愈发猖獗，呈现愈演愈烈之势。”谈及原因，王伟认为，当前具有组织性的各种网络攻击数量上升，僵尸网络的攻击方式也日渐增多，甚至出现了所谓的“高级可持续威胁攻击”（APT）。APT也被称为定向威胁攻击，是指针对特定对象展开的、持续有效的攻击活动。在这类攻击中，相当一部分攻击发起者是具有一定背景的黑客组织，他们专门研究如何有组织性地发动僵尸网络攻击。

王伟介绍道，具体到攻击手法上，僵尸网络既可被用于直接窃取重要的机密数据或信息，也可被用于获取群体性大数据，以分析、提炼出关键信息，还能用其发动拒绝服务（DOS）攻击造成大面积网络瘫痪，甚至可以效仿“震网”病毒攻击电网等大型基础设施，形成更严重的破坏。

闫怀志也认为，僵尸网络传播迅速、规模庞大，其攻击方式复杂多变，一旦发起攻击，其后果十分严重。

科技日报记者了解到，2016年10月，代号为“Mirai”的僵尸网络感染了数以十万计的物联网设备，造成美国东部地区大面积网络瘫痪。后来发现，“Mirai”的研制者竟是一名年仅21岁的年轻人，他研制该僵尸网络的目的，只是希望骗取钱财。很难想象，有国家背景的黑客组织精心织就的以发动战争而非赚钱为目的的僵尸网络，将会造成怎样的破坏。

说到赚钱，王伟认为，牟利也是僵尸网络的主要研制目的之一。例如，控制大量计算设备合力“挖矿”，赚取数字货币；利用僵尸网络大范围推送广告，以赚取广告费；发动勒索攻击，索要赎金等。早在2017年，美国Proofpoint公司的研究人员就曾发现名为“Adylkuzz”的僵尸网络，该网络控制了全球数十万台计的计算机或服务器，驱使其挖掘“门罗币”。

僵尸网络的用途如此多样，若要发动这种攻击，发起者是否需要掌握高超的技术呢？

“实际上并不需要。”王伟指出，现在互联网上有大量的开源僵尸程序，不法分子可以直接将其下载下来使用，甚至可以在其基础上进行修改升级。

防御需技术、管理两手抓

闫怀志谈到，在实际网络环境中，很多僵尸程序兼具了病毒、木马、间谍软件等多种恶意代码的特征，体现了恶意代码的组合化、复杂化的发展趋势，为僵尸网络的检测和防御工作带来了极大困难。

“很多僵尸网络只在需要时才被启动，平时则‘潜伏’伺机，隐蔽性强。”王伟表示，有些僵尸程序非常“聪明”，在潜伏时，它们有的每隔一段时间有规律地向控制者汇报情况，有的则无规律地“报平安”。常规的检测手段很难将它们检测出来，有时只能通过检测同一网络中不同主机与控制者间的相似数据传输，才能发现僵尸网络的“蛛丝马迹”。

“但是，即使能够发现它，也很难找到其背后的控制者。”王伟解释道，僵尸网络从控制者到受控计算机之间，可能存在多个层级，逐级进行控制，追踪者需要一级级溯源才能找到“真凶”。更为复杂的是，有些僵尸网络的某些控制层级位于暗网之中，控制者隐藏在暗网之后，当前的溯源技术对其几乎起不到任何作用。

“此外，对僵尸网络的防御还面临一个难题。”王伟介绍道，僵尸网络往往利用操作系统或软件漏洞传染硬件设备并扩大其规模，现有的网络防御系统大多只能检测、抵御已知漏洞的僵尸程序。但无论多完善的软件系统都会存在未知漏洞，黑客们只要发现并利用这些新的漏洞，就可以展开僵尸网络攻击。

隐蔽性强、溯源困难，我们要“种出”怎样的“豌豆射手”才能避免“僵尸”横行网络空间？

“现阶段，要想有效应对僵尸网络攻击，需要在主机、网络、管理等三个层面采取相应措施。”王伟认为，在主机层面，我们需要为自己的计算机、手机、物联网等设备安装杀毒等防御软件并按时更新，保证其能抵御已知的僵尸网络攻击。在网络层面，比如一个学校或企业的局域网，要及时进行针对僵尸网络的全网检测，一旦发现要及时处理。

“相比技术层面的措施，管理层面的措施更为重要。”王伟强调，企业、政府机关等各个机构要对员工加强系统化的网络安全教育，提高网络安全意识。比如，提醒员工要按规章制度管理和维护设备，及时更新杀毒软件、不采用“123456”等低级密码等。“Mirai”就曾利用大量摄像头，采用默认密码等弱口令，发动分布式拒绝服务攻击，造成了数小时的网络瘫痪。

5G网络废热多，但用它取暖尚不现实

本报记者 **张 蕴**

近日据报道，德国能源巨头意昂集团最近发布的一份研究报告显示，5G网络将大幅增加数据中心的耗电量，由此产生的废热可用于市政供暖。

那么，5G网络为何会使耗电量激增？我们又该如何收集、利用这些废热？针对上述问题，科技日报记者采访了业内相关专家。

通信网络设备占耗电大头

“5G网络大幅增加了数据中心的耗电量，这主要由于其通信网络、电源、环境调控等设备耗费了较多的电量。”中国科学院工程热物理研究所副所长、研究员陈海生对科技日报记者说，占耗电量大头的，是通信网络设备，它主要由基带处理单元（BBU）和有源天线处理单元（AAU）组成。BBU主要负责处理基带数字信号，AAU主要负责将基带数字信号转为模拟信号，再调制成高频射频信号，然后通过功放单元（PA）放大至足够功率后，由天线将信号发射出去。与传统网络相比，5G通信网络设备的AAU耗电量更大。

“例如，某通信运营商在广州、深圳对不同厂家5G基站功耗的测试结果显示，在4G网络中，AAU满载时的耗电量是289.7瓦，换成5G网络，其耗电量就升至1127.3瓦；5G通信网络设备耗电量基本是4G的2倍至3倍。”中国科学院工程热物理研究所研究员王亮在接受科技日报记者采访时说。

“2018年，全国范围内的数据中心共‘吃’掉了1608.89亿千瓦时的电量。”北京工业大学环境与能源工程学院研究员吴玉庭在接受科技日报记者采访时表示，相比4G网络，5G网络数据中心使用了更多的中央处理器（CPU），耗电量也会随之增加。5G网络数据中心运行的中央处理器及内存，会产生较多热量。这些热量如不能被及时“带走”，会导致中央处理器和内存温度不断升高，进而可能导致相关设备受损。

此外，陈海生补充道，5G基站的信号覆盖面积要远小于4G基站。要达到相同的覆盖效果，5G基站数量需要是4G的1.5倍至2倍，这也导致5G网络的耗电量进一步增加。

废热温度或难达到供暖标准

“从目前已有的5G网络耗电量资料来分析，相关废热主要从通信网络、环境调控、电源等设备中来。其中，通信网络设备是废热最主要的来源，特别是其组成部分——AAU设备，它是产生废热的‘大户’。”王亮说，在AAU设备中，其功放单元是最耗电、效率最低的器件。据统计，AAU设备的功放单元消耗了通信网络设备40%到50%的用电量，且一半以上的用电量都产生了废热。

我们该如何收集这些废热呢？

“可以用空气、水等换热介质收集5G网络废热。”陈海生对记者说，空气收集方式，是利用肋片、热管等装置将废热进行传导，空气流过这些装置时就会“带走”废热，以实现废热的收集。而水收集方式，是利用基站室内热空气流过空气—水换热器，将废热传递给水，进而实现废热收集；也可在基站设备中增加换热管道，水在换热管道内流动，就可吸收由设备产生的废热。

那么，目前能否将收集到的废热，用于市政供暖呢？

“理论上可行，但实际操作存在很大难度。”王亮对记者说，首先，5G网络设备的废热主要来源于AAU设备，而AAU位于室外通信铁塔上，如何高效收集其产生的废热，目前来看是比较难解决的问题；其次，市政供暖热对温度要求较高，通常要在70摄氏度到120摄氏度之间，而工业级电子元器件一般能耐受的温度不超过85摄氏度，网络设备的废热温度目前可能难以达到市政供暖标准。

“目前，市政供暖主要有热空气、热水和蒸汽这几种方式。”中国科学院工程热物理研究所凌浩恕博士对科技日报记者表示，热空气供暖方案，是利用加热设备产生热空气直接送入建筑进行供暖，技术原理简单。热水供暖方案，主要是利用热泵、供热锅炉等产生热水，再结合风机盘管、散热器、辐射地板进行供暖，是我国最常用的供暖方式。蒸汽供暖方案，则是利用电厂水蒸气进行供暖，可以满足多种用热需要；这种方式的适用范围广，常被用于工业厂区供暖。

“目前来看，这几种市政供暖方式，很难‘兼容’由5G网络所产生的废热。若想有效利用5G废热，还需要从技术上对其进行深入研究。”凌浩恕对记者说。

行业观察

备受互联网巨头追捧的数字中台究竟是什么

陈永伟

最近一两年，“数字中台”这一概念突然火了起来。不仅腾讯、阿里巴巴等互联网巨头纷纷着力建设数字中台，很多中小型互联网企业也开始在内部引入数字中台。

与数字中台概念火爆相随的，是中台服务行业的迅速成长。据艾瑞咨询公布的《2019年中国数字中台行业研究报告》，2018年我国数字中台服务市场的规模仅为22.2亿元，但到2022年底，该市场规模有望达179.4亿元。未来，这个行业甚至可能成长为一个千亿元级别的市场。

那么，如今火爆的数字中台到底是什么？它究竟有何用？企业又该如何建设自己的数字中台？

中台最早被应用于军事领域

从渊源上来看，中台其实是个外来概念。在英文中，它所对应的单词和“平台”是相同的，都是platform。由platform的含义，我们不难得知，它的作用主要是连接、沟通。不过，与一般的platform不同，中台是构建于企业内部的，位置处在前后台之间，故而得名。

最初，中台主要被用在军事指挥上。在现代战争中，军队的单位变得越来越小，不同军种间的微观配合变得越来越频繁，因此传统的指挥模式就不适合这种作战方式了。为适应这种变化，美军率先发明了指挥中台，对前方作战单位进行统一协调。在多场局部战争中，这种中台策略都发挥了重要作用。后来，这种方式逐步被企业学习并采用。

就笔者所知，在国内企业中，阿里巴巴是最早采用数字中台的。2015年，该集团创始人马云参观了著名游戏公司Supercell（超级细胞）。在参观期间，他被这个仅有200人公司的高效所深深震撼。于是，他决定学习Supercell的做法，对阿里巴巴进行中台化改造，组建了“共享业务事业部”（Shared Services Platform），通过这一部门沟通前端的业务部门和后端的云平台。这次改革极大地提升了阿里巴巴内部各部门间的协调能力，在很大程度上促进了其内部各部门间在数据、产品等资源的共享。阿里巴巴的这种做法，很快被其他企业所效仿，由此催生了现在的“中台热”。

从构架上来看，数字中台包含人和物两方面。所谓人，是指居于企业内部，进行部门协调的人员；所谓物，指的是对企业内部业务进行协调的软硬件系统。对于一个完整的中台来说，这两者缺一不可。

中台蹿红与互联网商业模式有关

为什么数字中台会突然在互联网企业中火爆起来？究其原因，这和互联网企业的商业模式有关。我们知道，平台模式是互联网企业最乐于采用的商业模式，而采用平台模式会带来几个重要的后果。

首先，同一个平台企业往往需要面临多个不同的市场，分处在不同市场的业务很可能差异巨大。其很可能导致，不同业务之间的工作人员缺乏沟通，使企业内部合作很难进行，企业合力难以发挥出来。这就需要在企业内部由一个数字中台来实现部门间的沟通、打破部门间的隔阂。

其次，采用平台模式的企业常会通过“平台包抄”战略，借助在原有市场上的优势进入新的市场。这就意味着企业随时可能“长”出新的业务线，使得原有的组织架构难以适应新变化。面对这种情况，企业当然可以通过调整组织架构来应对，但一般来说，这样做的成本是巨大的。如果采用了中台化战略，那么就可以在维持企业架构稳定的前提下，推进业务不断发展。

最后，对于多数平台企业来讲，数据都是最宝贵的资源。然而，在传统的企业组织架构之下，企业各部门、各市场之间的数据往往是不流通的，甚至数据的搜集和存储也各有各的规矩，“数据孤岛”现象十分明显。这样一来，企业就很难综合利用自己搜集到的数据信息来进行决策。而在建立数字中台后，企业就可通过中台实现不同部门之间数据的同质化处理，让数据在企业内部流动起来，这样就能大大提升企业利用数据的效率。

相关投资建设需理性分析

虽然数字中台概念十分火爆，但作为对企业内部资源进行整合的一种方式，其本身具有很强的特殊性，并非适合所有企业，也不是所有企业都需要建中台。如果有些企业不顾自身实际情况，偏要凑热闹，为建数字中台而建数字中台，其结果很可能适得其反。

究竟什么样的企业需要建数字中台？

总体而言，它至少需要满足如下条件：首先，企业的业务范围应该比较广，不同业务间的独立性比较强、沟通难度较大。其次，企业对于迅速反应的诉求比较高。再次，数据在企业的决策中扮演的角色较重，不同部门间的数据隔离现象较为严重。笔者认为，只有满足了上述条件，投入资金去建设数字中台才比较划算。

那么，企业应该如何建设数字中台？

笔者认为，对于这个问题，并没有一个标准的答案，需要根据具体情况而定。公司在推行中台战略时，必须要将顶层设计与底层推动有机结合起来。尽管如此，在建设中台的过程中，如下两项原则是值得重视的。

首先，企业要有自上而下的顶层设计，统筹考虑外部需求环境、业务发展阶段、能力属性以及与组织形态的匹配性，以保证数字中台可以通过较强的执行力来打破部门的藩篱，执行企业决策。

其次，企业应当充分调动部门的积极性和能动性，与数字中台形成良性配合，从而保证数字中台的协调效果可以在不同部门体现出来。

（作者系《比较》杂志研究部主管）