利用特种木马 窃取数据资料

境外APT窃密势头猛烈 威胁国家安全需加强防御

利用特种木马,对我国航空系统数十台计算机设备实施高强度网络攻击,窃取大量数据资料;专门搭建钓鱼攻击平台阵地,发送钓鱼攻击邮件导致我国军工领域数百份敏感文件被窃取……在第五个“全民国家安全教育日”之际,国家安全部披露多起有关APT(Adavanced Persistent Threat,是指针对明确目标的持续的、复杂的网络攻击)窃密的案例。

记者从国家安全部新闻办了解到,近年来境外各类政府背景APT黑客组织不断加强对我国网络攻击,窃取大量重要敏感信息,极力攻击试图控制我国核心设备和关键设施,势头猛烈,威胁巨大,严重危害我国网络空间国家安全和利益。

习近平总书记指出:没有网络安全就没有国家安全。

国家安全部有关负责人表示,国家安全机关深入学习贯彻习近平总书记关于维护网络安全的重要指示,在总体国家安全观引领下,立足本职,严厉打击境外组织的网络攻击窃密和渗透破坏活动,坚决维护我国网络空间安全。

攻击技术先进规模庞大

国家安全部有关负责人告诉记者,当前,APT窃密行为包括三大特点,即攻击领域广泛,规模庞大;攻击目标多样,全网覆盖;攻击技术先进,手法复杂。

2019年7月,某境外APT组织仿冒我国某军工领域重点单位邮件登录界面,专门搭建钓鱼攻击平台阵地,冒用“系统管理员”身份向该单位多名人员发送钓鱼攻击邮件。该单位职工王某点击了钓鱼攻击邮件,输入了个人邮箱账号和登录密码,导致其电子邮箱被秘密控制。之后,该APT组织定期远程登录王某电子邮箱收取王某邮箱内文件资料,并利用该邮箱向王某的同事、下级单位人员发送数百封木马钓鱼邮件,导致十余人下载点击了木马程序,相关人员工作计算机被控制。

这位负责人说,近年来,境外APT组织不仅加大了对我国党政机关、国防军工、科研院所等核心要害单位的攻击活动,而且延伸到了关键信息基础设施、能源、金融、军民融合等各个领域。攻击来源众多、频次和烈度日益增强。

“2019年,国家安全机关发现并处置的网络攻击窃密活动中,涉及境外APT组织数量多达近百个。其中一组织全年针对我国‘两会’、‘一带一路’高峰论坛以及新中国成立70周年等重大活动的定向攻击,竟多达4000多次。”该负责人说。

与此同时,境外APT攻击目标涵盖了连接互联网的各类设备乃至整个网络空间,从各种服务器、联网计算机,到电子邮箱、移动介质,再到各种网络设备、移动智能终端、工业控制系统和物联设备,总体上形成从单机到网络、从硬件到软件、从外网到内网的全网覆盖。

这位负责人举例说,2019年5月,国家安全机关对我国某能源公司开展技术安全检查时发现,该公司的网页服务器、域控服务器、文件共享服务器等多台网络设备均被境外APT组织攻击控制,该组织还利用公司内外网缺乏边界防护设备的管理漏洞,向内网进行渗透,控制了数十台计算机。

APT攻击技术先进,手法复杂。该负责人告诉记者,境外APT组织广泛运用人工智能、大数据等先进技术,同时采取漏洞攻击、诱骗攻击、“中间人”攻击等多种技术方式和手法,让人不易防范。

2019年9月,某境外APT组织利用特种木马,通过控制多个境外跳板设备对我国航空系统数十台计算机设备实施高强度网络攻击活动。攻击者精心伪装窃密行为,所用特种木马平时处于静默潜伏状态,接收到远程控制指令再激活运行,整个过程十分隐蔽。

6大措施强化防范抵御

如何防范抵御APT攻击?

“我们应当坚持总体国家安全观,树立正确的网络安全意识,多层次多维度地防范抵御网络安全的风险与挑战。”国家安全机关网络安全专家就此回应,并对核心要害单位和重要涉密人员如何防范抵御APT攻击提出6个方面的建议:

要压实各部门网络安全防范主体责任,确保各环节网络安全保密工作职责清晰、责任到人、可究可查。从已发现查处的部分案件看,一些环节的保密职责不清,是漏洞风险存在、案件发生的重要原因之一。因此,在网络安全责任划分时,应针对具体的网络应用情形、业务应用模式和岗位特点,专门制定网络安全保密工作要求,并切实细化分解。

要加强常态化网络安全教育和技能培训,提升网络安全敌情意识和防范技能。工作人员的疏忽大意和违规操作,是绝大多数网络安全事件和失泄密案件发生的主要原因。提高工作人员的网络安全防范意识和技能,彻底杜绝不安全操作行为,是做好网络安全管理的根本。必须严格做到“涉密不上网,上网不涉密”,不在非涉密计算机和移动存储介质中存储涉密资料,不通过互联网邮箱存储传递涉密文件资料,不在固定电话和手机中谈论涉密内容,涉密计算机和移动存储介质严禁连接互联网。

要加强对计算机、电子邮箱的安全防护。除了在办公计算机、手机上安装杀毒、防护软件等措施,还要不定期的对连网设备进行安全检测,发现计算机、手机等是否感染病毒木马程序,存在可疑的网络请求或连接,邮箱是否存在异常的登录情况。在出差特别是出国时,最好携带新的、不存储任何文件的新计算机、新手机,注册新的电子邮箱,在经过技术检测前不轻易使用别人以礼品形式赠送的电子设备。

要加强网络技术防范能力建设,确保技术防范措施到位并发挥实效。根据网络应用情形和保密级别要求,设置相适应的足够强度的技术防范措施;网管员对各技术防护手段设备的运行情况和监测记录要定期查看,既确保设备一直正常有效运转,又能及时发现各种违规、可疑或危险的技术操作行为。

要切实强化网络安全保密规章制度的执行监管。通过强化监管,提醒和约束涉密人员遵守保密制度,推动各项保密要求和保密责任落实到位。同时,抓早抓小,及早发现处置异常情况和安全隐患,尽可能减少信息安全保密的空白点和薄弱点,有效管控风险。

要加强同国家安全机关等专业部门的协作配合。国家安全机关是网络反间谍对敌斗争的专业部门,有责任、有义务指导协助各单位做好网络安全防范工作。国家安全机关将积极协助各涉密单位开展反间谍技术窃密检测,发现计算机网络被境外间谍情报机关攻击窃密情况及运行管理中存在的漏洞和薄弱环节,及时消除危害隐患。同时,指导各单位落实网络安全防范措施,提高技术防范能力,防范敌人网络攻击窃密活动。

(周斌)