网络攻击西工大，神秘黑客身份锁定

原来是美国国安局员工，“二次约会”间谍软件是新证据

近日，国家计算机病毒应急处理中心和360公司对一款名为“二次约会”的间谍软件进行了技术分析，分析报告显示，该软件是美国国家安全局（NSA）开发的网络间谍武器。据了解，在国家计算机病毒应急处理中心会同360公司配合侦办西北工业大学被美国国家安全局（NSA）网络攻击案过程中，成功提取了这款间谍软件的多个样本，并锁定了这起网络间谍行动背后美国国家安全局（NSA）工作人员的真实身份。

据技术分析报告显示，“二次约会”间谍软件是美国国家安全局（NSA）开发的网络间谍武器，该软件可实现网络流量窃听劫持、中间人攻击、插入恶意代码等恶意功能，它与其他恶意软件配合可以完成复杂的网络“间谍”活动。

国家计算机病毒应急处理中心高级工程师杜振华表示，该软件是具有高技术水平的网络间谍工具，使攻击者能够全面接管被攻击的（目标）网络设备以及流经这些网络设备的网络流量，从而实现对目标网络中主机和用户的长期窃密，同时还可以作为下一阶段攻击的“前进基地”，随时向目标网络中投送更多网络攻击武器。

据专家介绍，“二次约会”间谍软件长期驻留在网关、边界路由器、防火墙等网络边界设备上，其主要功能包括网络流量嗅探、网络会话追踪、流量重定向劫持、流量篡改等。另外，“二次约会”间谍软件支持在各类操作系统上运行，同时兼容多种体系架构，适用范围较广。

杜振华称，该间谍软件通常是结合特定人侵行动办公室（TAO）的各类针对防火墙、网络路由器的网络设备漏洞攻击工具一并使用。一旦漏洞攻击成功，攻击者成功获得了目标网络设备的控制权限，就可以将这款网络间谍软件植入到目标的网络设备中。

报告显示，国家计算机病毒应急处理中心和360公司与业内合作伙伴在全球范围开展技术调查，经层层溯源，发现了上千台遍布各国的网络设备中仍在隐蔽运行“二次约会”间谍软件及其衍生版本，并发现被美国国家安全局（NSA）远程控制的跳板服务器，其中多数分布在德国、日本、韩国、印度和中国台湾。

“在多国业内伙伴的通力配合下，我们的联合调查工作取得突破性进展。目前已经成功锁定了针对西北工业大学发动网络攻击的美国国家安全局（NSA）相关工作人员的真实身份。”杜振华表示。

来源：央视新闻

“数字”间谍来自何处，有何招式？

当前网络技术发展突飞猛进，5G、元宇宙、ChatGPT等崭新事物骈兴错出，令人惊呼“未来已来”。而与之一同到来的，还有隐藏其中的大量网络安全风险隐患。

攻击来自何处？

当前，网络空间已经成为境外间谍情报机关对我国开展网络间谍工作的重要阵地，我国已成为高级别持续性威胁（APT）攻击的主要受害国。近年来，国家安全机关已发现不同国家、地区的数十个间谍情报机关对我境内开展网络攻击活动。他们或组建专门机构力量、成立“掩护公司”、研发专业手段对我直接实施网络攻击渗透行动，或通过“幕后操控”“服务外包”等方式指使专业公司机构、黑客组织实施，或通过“购买”数据、漏洞、工具等方式拉拢引诱境内机构、人员实施，也有国家打着“前出狩猎”等幌子拉拢他国共同实施。

谁是潜在目标？

从攻击目标看，除了持续对我国家机关、涉密单位等“传统目标”开展网络攻击外，境外间谍情报机关还不断加强对我关键信息基础设施、重大基础设施网络系统的攻击渗透，并将黑手进一步伸向我高等院校、科研机构、大型企业、高科技公司等机构和企业高管、专家学者等群体。

境外对我网络攻击常见手法　网络截图

从受攻击情况看，涉及电子邮件、办公自动化、用户管理、安全防护等各类软件系统，服务器、计算机、交换机、路由器等各种硬件设备，以及手机、WIFI、摄像头等民用家用设备，可谓“无孔不入”。

有何招式手段？

与一般社会黑客不同，境外间谍情报机关可调动资源多、技术能力强大，网络攻击活动经验丰富、手法更加隐蔽。

他们有的搜集窃取个人信息数据，运用社会工程学，针对目标对象精准伪造“钓鱼”邮件和网站进行诱骗攻击；有的通过挖掘、购买关键软件系统、硬件设备“零日漏洞”，直接对我开展攻击渗透；有的先侵入控制我供应链企业或运维服务机构网络，再以此为“跳板”攻击下游用户单位；有的大规模渗透控制我民用网络、家用网设备，建立“阵地”对我及其他国家开展网络攻击活动。极具专业性、隐蔽性的攻击手法背后，往往是更加危险的企图！

造成多少危害？

境外间谍情报机关网络攻击活动规模大、层次深、持续性强。我国家机关、涉密单位及其他重要企业机构网络系统一旦遭攻击、侵入，所存储、处理的国家秘密、重要数据、文件资料等就可能被“一网打尽”。我关键信息基础设施、重大基础设施网络系统一旦被侵入、控制，就会面临随时被干扰、破坏的“致命一击”风险。境外间谍情报机关网络攻击窃取我企业机构商业秘密、知识产权，长期监控我公民网络通信内容，也严重侵害我公民、组织合法权益。

来源：国家安全部

外星人？墨西哥议会展出“非人类”化石

紫台专家：尚未发现确凿的外星生命证据

9月14日，“墨西哥展出两具疑似外星生物遗骸”话题冲上微博热搜，引发网友讨论。真的是外星人？紫金山天文台专家在接受现代快报记者采访时表示，这两具遗骸的真实性和是否来自外星文明，均需要进行详尽的科学研究和鉴定。目前，科学家尚未发现确凿的外星生命证据。

现代快报+记者
蔡梦莹 综合


◀展出的疑似是“外星生物”遗骸　网页截图

▲中国航天科技集团官方账号在知乎上的回答　网页截图

疑似“外星生物”遗骸亮相

据央视财经报道，当地时间9月12日，墨西哥议会首次召开与“不明异常现象”相关的公开听证会，两具被认为疑似是“外星生物”的遗骸亮相。根据CBS新闻等外媒报道，在当天的听证会上，不明飞行物研究者杰米·莫桑介绍，这两具遗骸于2017年在秘鲁被发现，距今分别有1800年和700年。从遗骸中提取的DNA显示，它们并非人类。据当地媒体报道，墨西哥方面计划通过听证会推动相关立法工作。该国可能因此成为全球首个承认“外星生物”存在的国家。

从直播现场照片来看，遗骸的头部细长，后脑勺偏大，体型小，每只手有3根手指。有网友把直播画面截图与史蒂文·斯皮尔伯格1982年拍摄的《E.T.外星人》电影中的外星人形象进行对比，“这外星人长得也太像外星人了”。也有网友认为，外星人可能有类似人形的，也可能有其他形状的，只是还没发现而已。

可信度遭到质疑

据美联社报道，长期坚信有不明飞行物存在的墨西哥记者何塞·海梅·毛桑，2017年在秘鲁曾宣称发现了非地球生物的遗体。然而，秘鲁检察官办公室的一份报告说，所谓遗体实际上是“近期生产的玩偶，表面覆盖有纸和合成胶水的混合物，以模仿皮肤”。报告说，几乎可以肯定这些“遗体”为人造，并非所谓的古代外星人遗体。由于当年提及的遗体并未公开展示，因此无法判断是否与如今呈交墨西哥国会展示的遗骸一样。

墨西哥海军健康科学研究所主要负责人何塞·德热赫斯·萨尔塞·贝尼特斯出席听证会作证。他说，已经对这两具遗骸进行X射线扫描、3D重建和DNA分析。“我能确定，这些遗体与人类无关”。

现代快报记者梳理发现，从目前的报道来看，还没有其他官方科研机构可以佐证“遗骸”的来源。当地时间9月13日，墨西哥国立大学重新发布一份声明。声明称，2017年5月，其加速器质谱国家实验室（LEMA）对一组样本进行了放射性碳定年法，这些样品约为0.5克皮肤等组织。此外，声明称这项工作只是为了确定样品的年龄，无论如何，都不会对上述样本的来源做出结论。

有媒体报道，研究者杰米·莫桑有过外星生物发现记录，后被科学家们证实是假的。这也让此次亮相的两具遗骸的可信度遭到质疑。

不少科学家也质疑“外星生物”遗骸的真实性。墨西哥国立自治大学天文研究所研究员胡列塔·菲耶罗说，这两具遗骸的不少细节“解释不通”。她说，科学家需要更先进的技术，而非仅凭X射线扫描，才能判断钙化的“干尸”是否“非人类”。

尚未发现确凿证据

对此，紫金山天文台科普部朱留斌表示，对于这两具遗骸的真实性和它们是否真的来自外星文明，需要进行详尽的科学研究和鉴定。这可能包括DNA分析、化学分析、放射性碳定年等多种科学方法。只有在这些方法都得出明确的结论后，才能确定它们是否属于外星生物。

朱留斌表示，外星生命的探索是一个复杂和持久的过程。虽然在太阳系的其他行星和一些系外行星上，已经探测到水分子和有机分子的存在，这些分子被认为是生命存在的可能性的关键因素之一。然而，确定生命存在仍然需要更多的证据和研究。截至目前，科学家尚未发现确凿的外星生命证据。至于是否存在外星生命，如果存在，可能是什么形式的，期待未来会有更多的研究和发现。

9月14日上午，中国航天科技集团官方在知乎相关问题下作出回答：“截至目前，我们在航天活动中尚未发现可证明外星人存在的确凿证据。”