CIA实施“颜色革命”五大阴招被曝光

中国揭露CIA长期使用的恶毒手段(下)

分析发现，尽管CIA的后门程序和攻击组件大都以无实体文件的内存驻留执行的方式运行，这使得对相关样本的发现和取证难度极大。即使这样，联合技术团队还是成功找到了解决取证难题的有效方法，发现了CIA所使用的9个类别的攻击武器，包括攻击模块投递类、远程控制类、信息收集窃取类、第三方开源工具类等。

其中，联合技术团队偶然提取到CIA使用的一款信息窃取工具，它属于网络曝光的美国国家安全局机密文档《ANT catalog》48种先进网络武器中的一个，是美国国家安全局的专用信息窃取工具。这种情况说明美国中央情报局和美国国家安全局会联合攻击同一个受害目标，或相互共享网络攻击武器，或提供相关技术或人力支持。这为对APT-C-39攻击者身份的归因溯源补充了新的重要证据。2020年，360公司独立发现了一个从未被外界曝光的APT组织，将其单独编号为APT-C-39。该组织专门针对中国及其友好国家实施网络攻击窃密活动，受害者遍布全球各地。

此外，CIA攻击武器的威力和危害性可以从第三方开源工具类中一窥端倪。该类攻击手段是指CIA经常使用现成的开源黑客工具进行攻击活动。CIA网络攻击行动的初始攻击一般会针对受害者的网络设备或服务器实施，也会进行社会工程学攻击。在获得目标权限之后，其会进一步探索目标机构的网络拓扑结构，在内网中向其他联网设备进行横向移动，以窃取更多敏感信息和数据。被控制的目标计算机，会被进行24小时实时监控，受害者的所有键盘击键都会被记录，剪切板复制粘贴信息会被窃取，USB设备的插入状态也会被实时监控，一旦有USB设备接入，受害者USB设备内的私有文件都会被自动窃取。条件允许时，用户终端上的摄像头、麦克风都会被远程控制和访问。

最新报告通过实证分析发现，CIA网络武器使用了极其严格的间谍技术规范，各种攻击手法前后呼应、环环相扣，现已覆盖全球几乎所有互联网和物联网资产，可以随时随地控制别国网络，盗取别国重要、敏感数据，而这无疑需要大量的财力、技术和人力资源支撑。报告建议，政府机构、科研院校、工业企业和商业机构在采用自主可控国产化设备的同时，应尽快组织开展APT攻击的自检自查工作，并逐步建立起长效的防御体系，抵御高级威胁攻击。

来源：中国新闻网

世卫组织：新冠疫情不再构成

“国际关注的突发公共卫生事件”

世卫组织：新冠疫情不再构成“国际关注的突发公共卫生事件”

2020年1月30日，世卫组织宣布新冠疫情构成“国际关注的突发公共卫生事件”，3月11日宣布新冠疫情具有大流行特征。根据《国际卫生条例》规定，世卫组织总干事要定期重新召集突发事件委员会审查疫情形势。

2023年1月30日，世卫组织在官网发布声明称，世卫总干事谭德塞认为，新冠疫情仍然构成“国际关注的突发公共卫生事件”。当时，谭德塞还曾表示，认同委员会的观点，即新冠大流行可能正处于过渡阶段。他感谢委员会提出的应谨慎应对这一过渡阶段并减轻潜在负面影响的建议。

来源：中国新闻 网

资料图：民众在美国纽约曼哈顿街头做新冠检测。中新社记者 廖攀 摄