澳洲幸运10计划准定第六名计划

EMCm7DuGMf9lBRLV

澳洲幸运10计划准定第六名计划美情报机构攻击中国大型商用密码产品提供商，调查报告公布

2024年，国家互联网应急中心CNCERT发现处置一起美情报机构对中国大型商用密码产品提供商网络攻击事件。本报告将公布此事件网络攻击详情，为全球相关国家、单位有效发现和防范美网络攻击行为提供借鉴。

一、网络攻击流程

（一）利用客户关系管理系统漏洞进行攻击入侵

该公司使用了某客户关系管理系统，主要用于存储客户关系及合同信息等。攻击者利用该系统当时尚未曝光的漏洞进行入侵，实现任意文件上传。入侵成功后，攻击者为清除攻击痕迹，删除了部分日志记录。

（二）对两个系统进行攻击并植入特种木马程序

2024年3月5日，攻击者在客户关系管理系统植入了特种木马程序，路径为/crm/WxxxxApp/xxxxxx/xxx.php。攻击者可以通过该木马程序，执行任意的网络攻击命令。为防止被监测发现，木马程序通信数据全过程加密，并进行特征字符串编码、加密、压缩等一系列复杂处理。2024年5月20日，攻击者通过横向移动，开始攻击该公司用于产品及项目代码管理的系统。

二、窃取大量商业秘密信息

（一）窃取客户及合同信息

2024年3月至9月，攻击者用14个境外跳板IP连接特种木马程序并窃取客户关系管理系统中的数据，累计窃取数据量达950MB。客户关系管理系统中有用户600余个，存储客户档案列表8000余条，合同订单1万余条，合同客户包括我相关政府部门等多个重要单位。攻击者可以查看合同的名称、采购内容、金额等详细信息。

（二）窃取项目信息

2024年5月至7月，攻击者用3个境外跳板IP攻击该公司的代码管理系统，累计窃取数据量达6.2GB。代码管理系统中有用户44个，存储了3个密码研发项目的代码等重要信息。

三、攻击行为特点

（一）攻击武器

通过对xxx.php特种木马程序的逆向分析，发现其与美情报机构前期使用的攻击武器具有明确同源关系。

（二）攻击时间

分析发现，攻击时间主要集中在北京时间22时至次日8时，相对于美国东部时间为10时至20时。攻击时间主要分布在美国时间的星期一至星期五，在美国主要节假日未出现攻击行为。

（三）攻击资源

攻击者使用的17个攻击IP完全不重复，同时可秒级切换攻击IP。攻击IP位于荷兰、德国和韩国等地，反映出其高度的反溯源意识和丰富的攻击资源储备。

（四）攻击手法

一是善于利用开源或通用工具伪装躲避溯源，例如在客户关系管理系统中还发现了攻击者临时植入的2个常见的网页木马。二是攻击者善于通过删除日志和木马程序，隐藏自身的攻击行为。

四、部分跳板IP列表

来源：“中国网络空间安全协会”微信公号

飞艇6码稳定公式图

澳洲10开奖结果历史1688

澳洲10开奖结果历史1688

赢钱游戏一天赚200

168澳洲幸运10开奖官网开奖记录

澳洲幸运10计划全天免费软件官网

教你一个逢赌必赢的办法

澳洲5机器人平台出租

2025澳洲幸运8开奖记录

澳洲幸运10开奖结果开奖号码

河内5分必中一注

极速赛车辅助器(免费)

168幸运飞开艇历史开奖记录

168澳洲幸运5开奖历史记录

澳洲10开奖号码查询

9码雪球一个月60万表图片

飞艇pk10一天稳赚5000

千里马人工计划免费版

澳洲幸运5计划精准人工计划软件