**“5.29” DEVOS勒索病毒攻击事故追查报告**

1. **事故单位：**通防部，机电部，调度指挥中心
2. **事故时间：**2022年5月29日0点开始
3. **事故地点：**矿数据中心机房
4. **事故类别：**一般
5. **事故性质：**责任事故
6. **事故经过：**

2022年5月29日凌晨3点40分，调度技术主管李瑞强接到调度中心电话说通防部调度台网络出现问题，上传省局的人员定位系统中断无法恢复，迅速来调度中心协助处理。来到现场，通防调度员大致介绍了情况：2点20分左右发现上传省局人员定位系统中断，联系部门技术人员检查无法解决，远程登录上传服务器桌面发现桌面文件与平时不一样，也无法打开，多次尝试仍然无法解决问题。通防部一边联系梅安森厂家工作人员，一边联系调度来协助处理。同时了解到梅安森厂家工作人员此时在机电部处理自动化的问题。李瑞强打开上传服务器的远程桌面，点击桌面几个和平时“不一样”的文件发现后缀都增加了一串值，还有邮箱地址之类，在最后面是Demos的后缀，感觉这东西似曾相识，预感到事情的不妙。马上查看了一下除了桌面以外其他盘上的文件，整个电脑大部分文件都被加了文件后缀。手机上查了一下确认是Demos勒索病毒，这是一种文件加密勒索病毒，它通过使用扩展名“.Demos”加密文件来限制对数据（文档，图像，视频等）的访问，然后试图通过要求以比特币加密货币形式的“赎金”来勒索受害者的钱，以换取对数据的访问权。

感觉到事情的严重性，李瑞强赶紧打电话向主管领导王主任汇报情况，王主任指示减小病毒扩散范围同时找出病毒的源头。于是李瑞强赶紧打电话叫来其他同事，查找病毒的源头，同时确认已经感染病毒的设备并拔掉其网线。最终确认病毒源头是IP为172.168.172.101的设备，通过检查IP表找到是前不久才安装的防灭火在线预警系统的服务器，立即拔掉它网口的网线终止病毒的继续扩散。对已感染病毒的设备安装火绒杀毒软件进行杀毒，没有被病毒加密的文档备份保存。

最后确认通防部上传省局服务器、机电自动化服务器、调度OA服务器以及双预控服务器均受到病毒不同程度攻击，数据被加密，需要解密找回数据。

1. **原因分析：**
2. 直接原因

 西科大提供的防灭火在线预警系统服务器首先被植入病毒，继而以该服务器为母体攻击其他的服务器，造成病毒的扩散。

1. 间接原因
2. 对网络病毒攻击防范意识淡薄，总感觉病毒入侵离我们很遥远；
3. 防范措施不到位，服务器没有安装杀毒软件或者安装了没有开启杀毒软件、没有及时更新杀毒软件；
4. 网络病毒的感染途径和方式多种多样，没有从源头杜绝，比如经常用的U盘。
5. **防范措施：**
6. 全网安装杀毒软件，并全盘查杀，扫描中毒U盘，清除病毒。
7. 还原被隐藏的文件，并开启[U盘保护]功能。
8. 核心设备禁用USB口，禁止使用外设。
9. 进入机房的设备必须先杀毒，不明的或者外来的U盘禁止带入机房使用。
10. 外来人员进入机房施工必须登记，调度必须有专人陪同。
11. **处理决定：**
12. 西科大所提供服务器拆走带给相关部门检测，并出具检测报告；
13. 西科大必须重新更换新的服务器，原服务器不允许给矿上使用；
14. 由调度组织尽快恢复被攻击的服务器，需要厂家支持付费的由矿上先上会讨论垫付，根据相关部门的检测报告再决定西科大此次事故的赔偿费用。