关于切实防范Elasticsearch服务器

遭勒索攻击的预警通报

各有关运维单位：

接省公安厅通报，工作中发现有黑客利用Elasticsearch服务器存在未授权访问漏洞，攻击入侵暴露在互联网上的Elasticsearch系统，实施数据窃取和勒索。攻击者删除Elasticsearch数据库中部分数据，插入名为“read\_me”的“勒索信”（见附件），告知用户支付0.015比特币索回被删除数据，并附比特币收款地址、联系邮箱地址以及比特币购买网址等信息。

为确保我省教育技术中心网络和数据安全，请各单位迅速开展以下工作：一是全面排查梳理Elasticsearch系统使用和受影响情况，在确保安全的前提下及时修复系统漏洞、消除安全隐患。二是及时备份主机内重要文件，开展系统自查自检和安全加固，提高系统安全防护能力，严防网络攻击事件。三是如存在暴露在互联网上的Elasticsearch服务器，请及时联系我中心进行处置。

附件：“勒索信”截图

附件

“勒索信”截图

