重要信息系统安全漏洞情况专报

河南省通信管理局
河南互联网应急中心

2017 年 10 月 23 日

关于“ML314.COM”后门事件的报告

10 月 22 日，接上级部门紧急通报，多部门存在主机被具备“后门”功能的恶意程序控制。恶意控制程序在用户不知情的情况下自动访问境外恶意域名“www.ml314.com”，下载执行恶意脚本，搜集主机信息，并将相关数据信息上传提交至恶意域名的服务器，存在重大风险隐患。经查，恶意域名“www.ml314.com”为境外注册域名，注册商为 GANDI SAS 公司（法国公司），目前解析地址为 13.124.82.254 和 52.78.135.177。

一、我省政府部门和重要企业疑似感染情况

据河南互联网应急中心监测，我省有 914 个 IP 地址与上述 IP 地址有数据通联记录，疑似被该后门程序控制。其中有 46 个 IP 地址涉及我省政府部门和重点企业，建议相关单位及时进行核查。具体信息见下表。

序号	IP 地址所属单位	服务器 IP	所属地区
1	巩义市教育体育局	218.29.219.40	郑州
2	国家广播电影电视总局二九三台	123.15.46.66	郑州
3	河南财政税务高等专科学校现代教育技术中心	218.29.67.242	郑州
4	河南工业大学	123.15.50.22	郑州
5	河南工业大学	123.15.50.28	郑州
6	河南理工大学万方科技学院	218.28.29.26	郑州
7	河南农业大学	218.29.136.35	郑州
8	河南日报报业集团	125.46.11.253	郑州
9	河南省化学工业学校	218.29.79.210	郑州
10	华北水利水电学院	218.29.223.73	郑州
11	省电子政务网	222.143.24.196	郑州
12	省电子政务网	222.143.27.243	郑州
13	郑州大学升达经贸管理学院	125.46.88.116	郑州
14	郑州大学网络管理中心	218.29.64.18	郑州
15	郑州大学网络管理中心	218.29.64.92	郑州
16	郑州大学网络管理中心	125.46.17.50	郑州
17	郑州大学西亚斯国际学院	218.28.247.42	郑州
18	郑州市二七区信息中心	218.28.20.210	郑州
19	郑州市教育局电化教育馆	123.15.32.20	郑州

序号	IP 地址所属单位	服务器 IP	所属地区
20	郑州市教育局电化教育馆	218.29.111.84	郑州
21	郑州市教育局电化教育馆	218.29.111.85	郑州
22	郑州市教育局电化教育馆	218.28.167.167	郑州
23	郑州市中原区信息中心	218.28.135.2	郑州
24	郑州图书馆（郑州少年儿童图书馆）	123.15.53.179	郑州
25	郑州职业技术学院	61.163.69.98	郑州
26	中共郑州市委党校	218.28.40.182	郑州
27	中国人民银行郑州中心支行天苑宾馆	218.28.5.46	郑州
28	中原工学院	61.163.70.216	郑州
29	河南第一火电建设公司	123.160.246.169	郑州
30	河南省社情民意调查中心	1.192.224.251	郑州
31	郑州日产汽车有限公司	222.85.86.114	郑州
32	郑州市港区育人国际学校	171.8.197.106	郑州
33	中石油化工股份有限公司华北分公司	123.52.95.92	郑州
34	中国石化销售有限公司三门峡分公司	222.89.143.103	三门峡
35	大唐热电厂	221.13.128.31	洛阳
36	河南科技大学	222.141.54.78	洛阳
37	洛阳博爱眼科医院	61.136.80.221	洛阳
38	洛阳市第一高级中学	221.13.140.205	洛阳
39	洛阳市公路运输管理处	61.136.80.103	洛阳

序号	IP 地址所属单位	服务器 IP	所属地区
40	洛阳市洛龙区人民政府办公室	221.13.133.203	洛阳
41	洛阳市质量技术监督局	61.54.82.29	洛阳
42	洛阳中科信息产业研究院(中科院计算技术研究所洛阳分所)	123.7.182.111	洛阳
43	汝阳县十八盘乡政府	123.7.180.19	洛阳
44	中国一拖集团有限通信分公司	218.28.152.46	洛阳
45	中色科技股份有限公司（黄河水利水电开发总公司）	61.136.78.84	洛阳
46	开封市水利建筑勘察设计院	123.55.144.30	开封

二、国家互联网应急中心河南分中心（河南互联网应急中心）开展的工作

（一）迅速开展事件分析研判

接上级部门紧急通报后，河南互联网应急中心立即开展应急响应和事件分析研判工作，利用中心网络安全监测平台迅速查找我省疑似被控主机 IP 地址，并对 IP 地址进行快速定位。目前已发现涉及我省政府部门和重点企业的服务器 46 台。

（二）积极监测开展应急处置

河南互联网应急中心立即要求各运营商对该恶意域名及对应 IP 的访问进行封堵，同步监测该恶意域名及 IP 的访问情况。此外，国家互联网应急中心已在国际出入口将该恶意域名及 IP

进行封堵。河南互联网应急中心将对该事件进行密切监测和关注，对有可能出现的情况进行跟踪防范。

三、安全建议

针对此次后门控制网络安全事件，建议各单位要高度重视，重点做好如下工作：

（一）各单位应立即组织全面排查隐患，清除后门控制程序，修复服务器存在的安全漏洞，确保自身系统安全。

（二）各单位应在本单位防火墙侧对该域名及对应 IP 的访问行为进行阻断，并同步监测对该域名及 IP 的访问情况。

报：赵素萍，许甘露，张维宁同志。

省委办公厅，省政府办公厅，省委政法委，省委网信办。

抄送：省教育厅，省交通厅，河南日报报业集团，郑州市政府办公厅，三门峡市政府办公室，洛阳市政府办公室，开封市政府办公室。

电话：0371-63715858　传真：0371-65601667