**漏洞扫描总结分析报告**

1. **漏洞扫描时间：2017年 9月15日。**
2. **安全范围：主要涉及到公司员工pc以及ftp服务器操作系统漏洞、木马、病毒、系统危险项、安全配置项。**
3. **扫描工具：360安全卫士，360企业版控制中心**

|  |  |  |
| --- | --- | --- |
| **服务器端** | **FTP服务器** | **Ip：** |
| **客户端** | **公司员工pc** | **Ip：** |

1. **总体漏洞扫描分析**

**扫描结果参考如下：**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **人员** | **IP地址** | **体验得分** | **漏洞** | **病毒** | **木马** | **插件** | **系统危险项** |
| 卢峰 | 68-F7-28-83-5F-2D | **48** | **2** | **0** | **0** | **0** | **1** |
| 乔文平 | 68-F7-28-4F-EB-48 | **64** | **1** | **0** | **0** | **0** | **0** |
| 邰晓鹏 | 50-7B-9D-AF-3F-27 | **45** | **3** | **0** | **0** | **1** | **0** |
| 王晓玲 | 1C-39-47-31-F8-FC | **36** | **1** | **0** | **0** | **0** | **1** |
| 张超 | 50-7B-9D-61-4F-7F | **47** | **3** | **0** | **0** | **1** | **0** |
| 张建伟 | 50-7B-9D-61-50-72 | **42** | **1** | **0** | **0** | **0** | **0** |
| 李坚 | 1C-39-47-31-EB-D4 | **48** | **2** | **0** | **0** | **0** | **0** |
| 李清元 | 1C-39-47-2A-AC-7D | **64** | **1** | **0** | **0** | **0** | **0** |
| 马帅 | 3C-97-0E-87-ED-4A | **28** | **2** | **0** | **0** | **0** | **0** |
| 张利 | 50-7B-9D-E7-27-FE | **47** | **1** | **0** | **0** | **0** | **0** |
| 杨征军 | 60-F8-1D-AC-92-A4 | **56** | **1** | **0** | **0** | **0** | **0** |
| 王飞 | F0-76-1C-AB-D5-F4 | **40** | **4** | **0** | **0** | **0** | **0** |
| 吴杰 | 68-F7-28-1A-07-E7 | **30** | **4** | **0** | **0** | **0** | **0** |
| 张星 | 68-F7-28-1A-08-01 | **18** | **6** | **0** | **0** | **0** | **0** |
| 马俊涛 | 50-7B-9D-DF-10-6D | **46** | **2** | **0** | **0** | **0** | **0** |
| 张沅涛 | 68-F7-28-5F-4B-A4 | **32** | **4** | **0** | **0** | **0** | **1** |
| 张浩 | 68-F7-28-01-88-09 | **43** | **3** | **0** | **0** | **0** | **0** |
| 杨远明 | B0-83-FE-95-63-3F | **32** | **6** | **0** | **0** | **0** | **0** |
| 王馨 | B0-83-FE-47-38-54 | **18** | **10** | **0** | **0** | **3** | **2** |
| 王俐骄 | 50-7B-9D-56-AA-6C | **28** | **4** | **0** | **0** | **0** | **0** |
| 张宁 | 50-7B-9D-34-58-09 | **0** | **12** | **0** | **1** | **1** | **4** |
| 王志敏 | 50-7B-9D-BC-63-87 | **60** | **2** | **0** | **0** | **0** | **0** |
| 张良松 | 50-7B-9D-A6-C2-53 | **16** | **4** | **0** | **0** | **3** | **2** |
| 李健 | 10-40-F3-57-8C-31 | **46** | **3** | **0** | **0** | **0** | **0** |
| 杨志佳 | 10-40-F3-5D-36-47 | **20** | **5** | **0** | **1** | **0** | **3** |
| 宠茗允 | 10-40-F3-92-73-C2 | **25** | **6** | **0** | **0** | **0** | **0** |
| 崔纪 | E0-AC-CB-66-69-E4 | **16** | **8** | **0** | **0** | **1** | **3** |
| 陈纲 | C8-69-CD-A3-21-68 | **42** | **5** | **0** | **0** | **0** | **0** |
| 樊妮娜 | E0-AC-CB-66-69-E4 | **34** | **4** | **0** | **0** | **0** | **0** |
| 蔡博 | 68-F7-28-C0-5B-37 | **34** | **8** | **0** | **0** | **0** | **0** |
| 牛蕾 | 68-F7-28-67-8B-B1 | **28** | **9** | **0** | **0** | **0** | **0** |
| 吴国强 | 68-F7-28-36-A3-78 | **32** | **6** | **0** | **1** | **0** | **0** |
| 谢妍 | 68-F7-28-69-48-53 | **21** | **7** | **0** | **0** | **0** | **0** |
| 王林娣 | 10-40-F3-87-CB-B4 | **42** | **5** | **0** | **0** | **0** | **0** |
| 贾敏 | 98-01-A7-DF-25-8F | **35** | **3** | **0** | **0** | **0** | **0** |
| 张涛 | 18-5E-0F-52-80-EB | **20** | **4** | **0** | **0** | **0** | **0** |
| 孙马秋 | 50-7B-9D-93-9D-B6 | **16** | **6** | **0** | **0** | **0** | **5** |
| 牛德标 | 50-7B-9D-93-96-CE | **47** | **4** | **0** | **0** | **0** | **0** |
| 郭倜颖 | 3C-97-0E-6E-B6-A1 | **52** | **3** | **0** | **0** | **0** | **0** |
| 张胜飞 | 3C-97-0E-3A-D1-63 | **21** | **8** | **0** | **0** | **0** | **0** |
| 赵亮 | 3C-97-0E-86-9B-92 | **0** | **12** | **0** | **2** | **0** | **6** |
| 赵青华 | 3C-97-0E-4E-C1-B1 | **17** | **8** | **0** | **0** | **0** | **2** |
| 孙金凯 | 3C-97-0E-94-78-83 | **21** | **6** | **0** | **1** | **0** | **0** |
| 翟海新 | 3C-97-0E-95-A7-7D | **18** | **12** | **0** | **0** | **0** | **3** |
| 张倬 | 3C-97-0E-99-76-93 | **42** | **5** | **0** | **0** | **0** | **0** |

1. **5．扫描结果分析**
2. 多数为捆绑的插件。系员工上网安装软件时没有重视软件安装提示所致；
3. 没有更新安全类的更新程序，导致系统存在更新类的漏洞。
4. 在安装软件时，没有去除不需要的快捷方式生成或者是一些运行类程序，从而导致存在危险项。

## 处理建议

1. 员工安装程序时应该有意识的去选择安装的插件，避免不必要的插件安装到电脑上；
2. 在发现有不寻常的图标时，无法判断是否有损电脑健康的情况下，使用360进行扫描，避免有病毒或者木马的存在；
3. 员工应定时使用360来对电脑进行扫面，减少漏洞存在的可能性；
4. 系统管理员定期对整网电脑进行监控，发现有漏洞应及时通知员工进行修复；

## 6漏洞处理结果

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **人员** | **IP地址** | **体验得分** | **漏洞** | **病毒** | **木马** | **插件** | **系统危险项** |
| 卢峰 | 68-F7-28-83-5F-2D | **100** | **0** | **0** | **0** | **0** | **0** |
| 乔文平 | 68-F7-28-4F-EB-48 | **100** | **0** | **0** | **0** | **0** | **0** |
| 邰晓鹏 | 50-7B-9D-AF-3F-27 | **100** | **0** | **0** | **0** | **0** | **0** |
| 王晓玲 | 1C-39-47-31-F8-FC | **94** | **0** | **0** | **0** | **0** | **0** |
| 张超 | 50-7B-9D-61-4F-7F | **100** | **0** | **0** | **0** | **0** | **0** |
| 张建伟 | 50-7B-9D-61-50-72 | **100** | **0** | **0** | **0** | **0** | **0** |
| 李坚 | 1C-39-47-31-EB-D4 | **100** | **0** | **0** | **0** | **0** | **0** |
| 李清元 | 1C-39-47-2A-AC-7D | **100** | **0** | **0** | **0** | **0** | **0** |
| 马帅 | 3C-97-0E-87-ED-4A | **100** | **0** | **0** | **0** | **0** | **0** |
| 张利 | 50-7B-9D-E7-27-FE | **100** | **0** | **0** | **0** | **0** | **0** |
| 杨征军 | 60-F8-1D-AC-92-A4 | **97** | **0** | **0** | **0** | **0** | **0** |
| 王飞 | F0-76-1C-AB-D5-F4 | **100** | **0** | **0** | **0** | **0** | **0** |
| 吴杰 | 68-F7-28-1A-07-E7 | **100** | **0** | **0** | **0** | **0** | **0** |
| 张星 | 68-F7-28-1A-08-01 | **100** | **0** | **0** | **0** | **0** | **0** |
| 马俊涛 | 50-7B-9D-DF-10-6D | **100** | **0** | **0** | **0** | **0** | **0** |
| 张沅涛 | 68-F7-28-5F-4B-A4 | **100** | **0** | **0** | **0** | **0** | **0** |
| 张浩 | 68-F7-28-01-88-09 | **100** | **0** | **0** | **0** | **0** | **0** |
| 杨远明 | B0-83-FE-95-63-3F | **100** | **0** | **0** | **0** | **0** | **0** |
| 王馨 | B0-83-FE-47-38-54 | **100** | **0** | **0** | **0** | **0** | **0** |
| 王俐骄 | 50-7B-9D-56-AA-6C | **100** | **0** | **0** | **0** | **0** | **0** |
| 张宁 | 50-7B-9D-34-58-09 | **100** | **0** | **0** | **0** | **0** | **0** |
| 王志敏 | 50-7B-9D-BC-63-87 | **100** | **0** | **0** | **0** | **0** | **0** |
| 张良松 | 50-7B-9D-A6-C2-53 | **100** | **0** | **0** | **0** | **0** | **0** |
| 李健 | 10-40-F3-57-8C-31 | **100** | **0** | **0** | **0** | **0** | **0** |
| 杨志佳 | 10-40-F3-5D-36-47 | **100** | **0** | **0** | **0** | **0** | **0** |
| 采购助理 | 10-40-F3-92-73-C2 | **100** | **0** | **0** | **0** | **0** | **0** |
| 崔纪 | E0-AC-CB-66-69-E4 | **100** | **0** | **0** | **0** | **0** | **0** |
| 陈纲 | C8-69-CD-A3-21-68 | **100** | **0** | **0** | **0** | **0** | **0** |
| 樊妮娜 | E0-AC-CB-66-69-E4 | **100** | **0** | **0** | **0** | **0** | **0** |
| 蔡博 | 68-F7-28-C0-5B-37 | **100** | **0** | **0** | **0** | **0** | **0** |
| 牛蕾 | 68-F7-28-67-8B-B1 | **100** | **0** | **0** | **0** | **0** | **0** |
| 吴国强 | 68-F7-28-36-A3-78 | **100** | **0** | **0** | **0** | **0** | **0** |
| 谢妍 | 68-F7-28-69-48-53 | **98** | **0** | **0** | **0** | **0** | **0** |
| 王林娣 | 10-40-F3-87-CB-B4 | **100** | **0** | **0** | **0** | **0** | **0** |
| 贾敏 | 98-01-A7-DF-25-8F | **100** | **0** | **0** | **0** | **0** | **0** |
| 张涛 | 18-5E-0F-52-80-EB | **100** | **0** | **0** | **0** | **0** | **0** |
| 孙马秋 | 50-7B-9D-93-9D-B6 | **100** | **0** | **0** | **0** | **0** | **0** |
| 牛德标 | 50-7B-9D-93-96-CE | **100** | **0** | **0** | **0** | **0** | **0** |
| 郭倜颖 | 3C-97-0E-6E-B6-A1 | **100** | **0** | **0** | **0** | **0** | **0** |
| 张胜飞 | 3C-97-0E-3A-D1-63 | **100** | **0** | **0** | **0** | **0** | **0** |
| 赵亮 | 3C-97-0E-86-9B-92 | **95** | **0** | **0** | **0** | **0** | **0** |
| 赵青华 | 3C-97-0E-4E-C1-B1 | **100** | **0** | **0** | **0** | **0** | **0** |
| 孙金凯 | 3C-97-0E-94-78-83 | **100** | **0** | **0** | **0** | **0** | **0** |
| 翟海新 | 3C-97-0E-95-A7-7D | **100** | **0** | **0** | **0** | **0** | **0** |
| 张倬 | 3C-97-0E-99-76-93 | **100** | **0** | **0** | **0** | **0** | **0** |

**5、扫描总结**

通过本次扫描，发现了大量的高位系统漏洞，北京易才博普奥建议对存在漏洞的进行漏洞修补、安全增强。

1. 建议所有windows系统使用windows update 进行更新
2. 对大量终端用户而言，可以采用360安全卫士进行自动补丁更新，也可以由360企业控制即使对所有终端用户进行补丁更新。
3. 由于其他原因不能及时安装补丁的系统，考虑在网络边界、路由器、防火墙上设置严格的访问控制策略，以保证网络的动态安全。
4. 建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重。
5. 漏洞，攻与防的循环，伴随每个主流操作系统、应用服务的生命周期。建议采用网络入侵检测系统实时监控网络流量，及时发现病毒感染源。 
6. 建议定期对网络进行漏洞扫描和评估，真正做到未雨绸缪。