test2检查报告

时间范围:2017-05-30 17:24至2017-06-06 17:24

1. 综述

|  |  |
| --- | --- |
| 检查对象 | test2 |
| 所属行业 | 航空航天 |
| 出口IP | 1.1.1.1 |
| 开始时间 | 2017-05-04 15:58 |
| 持续时间 | 0天15小时18分 |
| 采集流量 | 1227.93GB |

1. 检查结果

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 事件数  100 |  | 受攻击主机数  17 |  | 威胁情报命中数  8 |

1. 事件详情

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 发现时间 | 威胁级别 | 攻击IP | 受害IP | 检查引擎 | 威胁标签 | 通信协议 | 状态 |
| 1 | 2017-06-06 11:50:24 | 高危 | 218.30.116.76 | 172.24.66.78 | 行为模式、基础引擎 | 孔夫子型木马 加密通信 无refer请求告警 DNS频率告警 | http tcp dns | 未处理 |

1. 受攻击主机Top5

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 发现时间 | IP | MAC | 被攻击次数 |
| 1 | 2017-06-06 12:10:31 | 172.24.66.42 | 18:66:da:0b:98:9a | 32 |
| 2 | 2017-06-06 12:10:24 | 172.24.66.33 | fc:aa:14:cc:44:c3 | 25 |
| 3 | 2017-06-06 12:10:31 | 172.24.66.43 | 18:66:da:0b:65:46 | 17 |
| 4 | 2017-06-06 12:10:31 | 172.24.66.51 | f4:8e:38:9b:dd:24 | 14 |
| 5 | 2017-06-06 12:10:31 | 172.24.66.41 | 18:66:da:07:69:d2 | 14 |

1. 威胁情报命中Top5

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | APT名称 | 目标行业 | 感染主机数 | 背景组织 |
| 1 | APT-0007 |  | 3 | 俄罗斯 |

1. 整改建议

一、技术方面

1、将感染的木马病毒清理干净，避免造成进一步危害，建议请专业的安全技术人员来进行处理。

2、采用统一的防病毒软件，并定时更新，抵御常见木马病毒。

3、定期给系统及软件安装最新补丁，防止因为漏洞利用带来的攻击。

4、在网络层面采用能够对全流量进行持续存储和分析的设备，应对未知的高级攻击。

二、管理方面

1、建立好的管理制度，责任落实到人。

2、建立应急响应处理机制，应对突发情况。

3、组织针对性的安全培训，提高人员安全意识。

4、定期安全演练，提升人员安全技能及应对能力。

5、定期安全检查，及时排除安全隐患。

6、制定安全考核办法，进行安全检查。