密级：用户公开

目录

[1 背景声明 4](#_Toc35606378)

[1.1 版权声明 4](#_Toc35606379)

[1.2 编写目的 4](#_Toc35606380)

[2 重点网络安全事件分析 5](#_Toc35606381)

[2.1 概述 5](#_Toc35606382)

[2.2 僵尸网络分析 6](#_Toc35606383)

[2.2.1 全省僵尸网络分布情况 6](#_Toc35606384)

[2.2.2 全省僵尸网络类型占比 6](#_Toc35606385)

[2.2.3 重点受攻击城市态势分析 7](#_Toc35606386)

[2.2.4 攻击泛滥地区态势分析 7](#_Toc35606387)

[2.3 木马程序分析 8](#_Toc35606388)

[2.3.1 全省木马程序分布情况 8](#_Toc35606389)

[2.3.2 全省木马程序类型占比 9](#_Toc35606390)

[2.3.3 重点受攻击城市态势分析 10](#_Toc35606391)

[2.3.4 攻击泛滥地区态势分析 11](#_Toc35606392)

[2.4 蠕虫攻击分析 11](#_Toc35606393)

[2.4.1 全省蠕虫攻击分布情况 12](#_Toc35606394)

[2.4.2 全省蠕虫攻击类型占比 12](#_Toc35606395)

[2.4.3 重点受攻击城市态势分析 13](#_Toc35606396)

[2.5 WEB攻击分析 14](#_Toc35606397)

[2.5.1 全省WEB攻击分布情况 14](#_Toc35606398)

[2.5.2 全省WEB攻击类型占比 15](#_Toc35606399)

[2.5.3 重点受害地区态势分析 16](#_Toc35606400)

[2.5.4 攻击泛滥地区态势分析 17](#_Toc35606401)

[3 各省安全态势分析 19](#_Toc35606402)

[3.1 各市安全态势比较 19](#_Toc35606403)

[4 事件处置建议 21](#_Toc35606404)

[4.1 处置方案 21](#_Toc35606405)

[4.1.1 处置建议 21](#_Toc35606406)

[4.1.2 预防建议 22](#_Toc35606407)

# 背景声明

## 版权声明

本文件

## 编写目的

本文档主要是通过山东省通信管理局网络安全监测分析和业务管理平台监测到的安全事件，通过僵尸网络、木马程序、蠕虫攻击和WEB攻击四种攻击类型为维度，对我省的攻击分布和各市的安全态势进行分析。

# 重点网络安全事件分析

## 概述

自2020年02月10日至2020年02月16日，共监测到僵尸网络、木马程序、蠕虫攻击和WEB攻击事件日志近1162858条，其中，僵尸网络事件量为175945条，木马程序事件量为17658条，蠕虫攻击事件量为3133条，WEB攻击事件量为966122条，如下图。

图1事件类型分布图

由上面饼图可知，僵尸、木马、蠕虫和WEB攻击四大安全事件中，Web攻击事件最多为966122条，占比高达83%；其次为僵尸网络175945条，占比为15%。由此可知，Web攻击和僵尸网络为攻击者主要的攻击手段。

## 僵尸网络分析

自2020年02月10日至2020年02月16日，共监测到僵尸网络事件量为175945条，其中山东省僵尸网络事件量为173250条，占僵尸网络总体事件量的98%。下面通过攻击IP分布、僵尸网络类型和受害地区多个维度对本省僵尸网络安全事件进行分析。

### 全省僵尸网络分布情况

表1本省僵尸网络受害IP分布

|  |  |  |
| --- | --- | --- |
| 序号 | 城市 | 受害IP个数 |
| 1 | 济南 | 1176 |
| 2 | 烟台 | 15 |
| 3 | 淄博 | 11 |
| 4 | 威海 | 8 |
| 5 | 滨州 | 7 |
| 6 | 潍坊 | 7 |
| 7 | 泰安 | 3 |
| 8 | 枣庄 | 1 |

根据2020年02月10日至2020年02月16日的安全事件进行分析可以发现，本省受到的僵尸网络危害最大的城市是济南，有1176个受害IP。

### 全省僵尸网络类型占比

通过对2020年02月10日至2020年02月16日发生的僵尸网络日志分析发现，省内僵尸网络事件数量最多的是疑似IOT僵尸网络Gafgyt-通信信息，事件日志总量达144124次，占省内僵尸网络总事件量超过83%，如表所示。

表2僵尸网络事件日志类型TOP5统计

|  |  |
| --- | --- |
| 事件名称 | 事件数量 |
| 疑似IOT僵尸网络Gafgyt-通信信息 | 144124 |
| 检测到Backdoor.Linux.Dofloo.d DDos登陆 | 22503 |
| 疑似驱动人生恶意域名v.beahh.com访问 | 1770 |
| 疑似驱动人生恶意域名pp.abbny.com访问 | 960 |
| 疑似僵尸网络DDoS.IoT.Mirai通信 - bot端爆破特征[3] | 930 |

根据分析可知，疑似IOT僵尸网络Gafgyt-通信信息占据榜首位置，占比超过85%，是近一周最多的僵尸网络类型。

### 重点受攻击城市态势分析

2020年02月10日至2020年02月16日受僵尸网络危害最严重的城市为济南，共受到了8253次攻击。经平台分析发现，济南前一周的受攻击次数为92433次，本周与之对比，受攻击次数明显减少，如图。

图2受攻击趋势

从上图我们可以发现，本周较上周济南受攻击次数有所下降，环比下降了91.1%。

### 攻击泛滥地区态势分析

僵尸网络的控制端发起攻击次数最多的城市为济南，发起攻击次数为166188次，占省内僵尸网络事件的96%

图3发动攻击趋势

从上图可以发现，本周较上周济南发动的攻击次数有下降，环比下降98.4%。

对全省的攻击IP进行统计，列出TOP2：

表3僵尸网络攻击IP分布TOP2

|  |  |  |
| --- | --- | --- |
| 序号 | 城市 | 攻击IP数量 |
| 1 | 济南 | 75255 |
| 2 | 青岛 | 1 |

根据2020年02月10日至2020年02月16日的安全事件进行分析可以发现，山东省利用僵尸网络攻击的攻击者多分布在济南，只有少数分布在其他城市。

## 木马程序分析

自2020年02月10日至2020年02月16日，共监测到木马程序事件量为17658条，其中山东省木马程序事件量为16893条，占木马程序总体事件量的96%。下面通过攻击IP分布、木马程序类型和受害地区多个维度对山东省木马程序安全事件进行分析。

### 全省木马程序分布情况

表4全省木马分布

|  |  |  |
| --- | --- | --- |
| 序号 | 城市 | 受害IP个数 |
| 1 | 济南 | 1195 |
| 2 | 青岛 | 28 |
| 3 | 潍坊 | 20 |
| 4 | 聊城 | 18 |
| 5 | 枣庄 | 14 |
| 6 | 东营 | 11 |
| 7 | 泰安 | 5 |
| 8 | 烟台 | 4 |
| 9 | 滨州 | 4 |
| 10 | 威海 | 3 |
| 11 | 德州 | 3 |
| 12 | 济宁 | 3 |
| 13 | 淄博 | 2 |
| 14 | 莱芜 | 2 |
| 15 | 菏泽 | 1 |
| 16 | 日照 | 1 |
| 17 | 临沂 | 1 |

由上表可知，济南受到木马程序的侵害最为严重，共1195个IP受到了攻击，其他城市受到木马程序影响的IP较少。

### 全省木马程序类型占比

通过对近一周发生的木马程序日志分析发现，省内木马程序事件数量最多的是“疑似检测到ELF.MrBlack DOS.TF 变种”，事件日志总量达7463次，占省内木马程序总事件量超过44%，如图所示。

表5木马程序日志类型TOP5统计

|  |  |
| --- | --- |
| 事件名称 | 攻击次数 |
| 疑似检测到ELF.MrBlack DOS.TF 变种 | 7463 |
| 疑似Rouge.NetReapar - 通信特征[1] | 2669 |
| 驱动人生后门-pp.abbny.com访问 | 972 |
| 疑似检测到木马Linux/BillGates登录特征 | 956 |
| 疑似EternalBlue SMB-攻击利用成功 | 871 |

通过下图可以看出木马网络类型排行TOP5情况：

图4全省木马程序类型TOP5

由上图可知，疑似检测到ELF.MrBlack DOS.TF 变种占据榜首位置，占比超过58%，是近一周攻击最多的木马类型。

### 重点受攻击城市态势分析

2020年02月10日至2020年02月16日受木马程序危害最严重的城市为济南，共受到了7751次攻击。本周与上周对比，受攻击次数略微减少，如图。

图5受攻击趋势

从上图可以发现，本周较上周受攻击次数有所提升，环比下降了87.2%。

### 攻击泛滥地区态势分析

木马程序的控制端发起攻击次数最多的城市为济南，发起攻击次数为9308次，省内55%的木马程序攻击来自济南。

图6发动攻击趋势

从上图可以发现，本周较上周发动的攻击次数明显减少，环比减少80.5%。

对全省的攻击IP进行统计，列出TOP2：

表6僵尸网络攻击IP分布TOP2

|  |  |  |
| --- | --- | --- |
| 序号 | 城市 | 攻击IP数量 |
| 1 | 济南 | 771 |
| 2 | 青岛 | 5 |

根据2020年02月10日至2020年02月16日的安全事件进行分析可以发现，山东省利用木马程序攻击的攻击者多分布在济南，只存在少数分布在其他城市。

## 蠕虫攻击分析

自2020年02月10日至2020年02月16日，共监测到蠕虫攻击事件量为3133条，其中山东省蠕虫攻击事件量为2733条，占蠕虫攻击总体事件量的87%。下面通过攻击IP分布、蠕虫攻击类型和受害地区多个维度对山东省蠕虫攻击安全事件进行分析。

### 全省蠕虫攻击分布情况

表7全省蠕虫分布

|  |  |  |
| --- | --- | --- |
| 序号 | 省份 | 受害IP个数 |
| 1 | 济南 | 22 |
| 2 | 聊城 | 15 |
| 3 | 青岛 | 7 |
| 4 | 枣庄 | 6 |
| 5 | 潍坊 | 4 |
| 6 | 德州 | 3 |
| 7 | 烟台 | 3 |
| 8 | 泰安 | 2 |
| 9 | 威海 | 2 |
| 10 | 临沂 | 2 |
| 11 | 淄博 | 2 |
| 12 | 日照 | 1 |
| 13 | 菏泽 | 1 |
| 14 | 滨州 | 1 |

根据2020年02月10日至2020年02月16日的安全事件进行分析可以发现，山东省受到的蠕虫攻击危害最大的城市是济南，有22个受害IP。

### 全省蠕虫攻击类型占比

通过对2020年02月10日至2020年02月16日发生的蠕虫攻击日志分析发现，省内蠕虫攻击事件数量最多的是“MS17-010-NSA军火库-永恒之蓝漏洞利用[2]”，事件日志总量达1042次，占省内蠕虫攻击总事件量超过38%，如图所示。

表8蠕虫攻击日志类型TOP5统计

|  |  |
| --- | --- |
| 事件名称 | 攻击次数 |
| MS17-010-NSA军火库-永恒之蓝漏洞利用[2] | 1042 |
| MS17-010-NSA军火库-永恒之蓝漏洞利用[1] | 800 |
| 疑似网络蠕虫WannaCryptor.a - 访问Kill Switch域名 | 598 |
| 疑似检测到RAMNIT.A M2 | 255 |
| 疑似检测到RAMNIT.A M1 | 38 |

通过下图可以看出蠕虫类型排行TOP5情况：

图7全省蠕虫攻击类型TOP5

由上图可知，MS17-010-NSA军火库-永恒之蓝漏洞利用[2]占据榜首位置，占比为38%，是近一周发起攻击最多的蠕虫类型。

### 重点受攻击城市态势分析

2020年02月10日至2020年02月16日受蠕虫攻击危害最严重的城市为济南，共受到了10275次攻击。本周与上周对比，受攻击次数稍微下降，如图。

图8受攻击趋势

从上图我们可以发现，本周较上周受攻击次数有所提升，环比上升了100%。

## WEB攻击分析

自2020年02月10日至2020年02月16日，共监测到Web攻击事件量为966122条，其中山东省Web攻击事件量为897679条，占Web攻击总体事件量的93%。下面通过攻击IP分布、Web攻击类型和受害地区多个维度对山东省Web攻击安全事件进行分析。

### 全省WEB攻击分布情况

表9全省WEB攻击分布

|  |  |  |
| --- | --- | --- |
| 序号 | 省份 | 受害IP个数 |
| 1 | 济南 | 7869 |
| 2 | 潍坊 | 928 |
| 3 | 泰安 | 802 |
| 4 | 莱芜 | 81 |
| 5 | 青岛 | 73 |
| 6 | 德州 | 73 |
| 7 | 济宁 | 32 |
| 8 | 烟台 | 28 |
| 9 | 枣庄 | 22 |
| 10 | 威海 | 15 |
| 11 | 聊城 | 9 |
| 12 | 淄博 | 8 |
| 13 | 临沂 | 7 |
| 14 | 滨州 | 4 |
| 15 | 菏泽 | 2 |
| 16 | 日照 | 2 |
| 17 | 东营 | 1 |

根据排名列出受web攻击危害最为严重的城市排行TOP10

图9受害省份排行TOP10

由上图可知，济南受到web攻击的侵害最为严重，7869个IP受到了攻击，其次是潍坊有928个IP受到了攻击。

### 全省WEB攻击类型占比

我们通过对2020年02月10日至2020年02月16日发生的WEB攻击日志分析发现，省内WEB攻击事件数量最多的“Supervisord远程命令执行 - CVE-2017-11610”，事件日志总量达277326次，占省内WEB攻击总事件量超过31%，如图所示。

表10 web攻击事件日志类型TOP5统计

|  |  |
| --- | --- |
| 事件名称 | 攻击次数 |
| Supervisord远程命令执行 - CVE-2017-11610 | 277326 |
| TROJAN [PTsecurity] Botnet Nitol.B Checkin | 123477 |
| 疑似XXE注入攻击尝试 | 103741 |
| 检测到SQL注入攻击测试语句[1] | 51056 |
| XSS攻击特征[1] | 32276 |

通过下图可以看出web攻击类型排行TOP5情况：

图10全省web攻击类型TOP5

由上图可知，Supervisord远程命令执行 - CVE-2017-11610占据榜首位置，占比47%，是近一周最多的web攻击类型。

### 重点受害地区态势分析

2020年02月10日至2020年02月16日受web攻击危害最严重的城市为济南，共受到了487596次攻击，本周与上周对比，受攻击次数明显下降，如图。

图11受攻击趋势

从上图我们可以发现，本周较上周济南受攻击次数明显下降，环比下降了56.5%。

### 攻击泛滥地区态势分析

利用web攻击发起攻击，次数最多的城市为济南，发起攻击次数为380553次，由此可知，省内42%的web攻击来自济南。

图12发动攻击趋势

从上图我们可以发现，本周较上周发动的攻击次数明显下降，环比下降75.9%。

对全省的攻击IP进行统计，列出TOP2：

表11僵尸网络攻击IP分布TOP2

|  |  |  |
| --- | --- | --- |
| 序号 | 城市 | 攻击IP数量 |
| 1 | 济南 | 2964 |
| 2 | 青岛 | 184 |

根据2020年02月10日至2020年02月16日的安全事件进行分析可以发现，山东省利用web攻击的攻击者多分布在济南，只有少数分布在其他城市。

# 各省安全态势分析

## 各市安全态势比较

山东省各个城市的安全事件分布情况如下表

表12城市安全事件分布情况

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 城市 | 本周受攻击次数 | 上周受攻击情况 | 环比增加/减少 |
| 1 | 济南 | 504222 | 1287215 | 60.8% |
| 2 | 潍坊 | 20573 | 1066 | 1829.9% |
| 3 | 泰安 | 13318 | 14 | 95028.6% |
| 4 | 青岛 | 2055 | 5018 | 59% |
| 5 | 枣庄 | 1815 | 8 | 22587.5% |
| 6 | 莱芜 | 1613 | 5 | 32160% |
| 7 | 威海 | 1212 | 152 | 697.4% |
| 8 | 烟台 | 702 | 249 | 181.9% |
| 9 | 聊城 | 457 | 944 | 51.6% |
| 10 | 济宁 | 375 | 97 | 286.6% |
| 11 | 淄博 | 129 | 792 | 83.7% |
| 12 | 德州 | 95 | 14 | 578.6% |
| 13 | 临沂 | 70 | 648 | 89.2% |
| 14 | 滨州 | 22 | 251 | 91.2% |
| 15 | 东营 | 13 | 9 | 44.4% |
| 16 | 日照 | 5 | 82 | 93.9% |
| 17 | 菏泽 | 5 | 33 | 84.8% |

由表中各市的安全事件环比增减情况可以看到，8个城市被攻击，次数降低其余9个城市均有所提升。但主要受害城市济南受攻击次数明显下降，从而导致总体事件量下降。

我们对济南本周和上周发生的安全事件日志进行分析，如下表。

表13济南日志类型统计

|  |  |  |  |
| --- | --- | --- | --- |
| 安全事件类型 | 本周受攻击次数 | 上周受攻击次数 | 增加/减少量 |
| Web攻击 | 487596 | 1121667 | 56.5 |
| 僵尸网络 | 8253 | 92433 | 91.1 |
| 木马程序 | 7751 | 60591 | 87.2 |
| 蠕虫攻击 | 622 | 12524 | 95 |

由上表可以看出，济南本周安全事件下降的主要原因是Web攻击、僵尸网络、木马程序、蠕虫攻击事件的减少。

# 事件处置建议

## 处置方案

### 处置建议

由于中毒的主机中很可能在多处留存和感染了病毒木马，并且存在无法彻底清除此恶意软件；如果条件允许，建议重装系统，能够彻底清除病毒。（注：重装系统前请务必做好重要资料备份！）

如果不想重装系统，建议执行以下操作：

1）断开网络

由于中了僵尸木马病毒后，会尝试对主控端进行通信，断开网络则断开与控制端的一切联系。

2）备份重要文件

为了减轻损失，对于电脑上保存的重要的数据、邮件、文档等，应该在断开网络后立刻将其备份到其他设备上。

3）全面杀毒

在没有后顾之忧之后，进行病毒的查杀，可通过正版安全杀毒软件，对其主机进行全盘杀毒。

4）卸载所有未知或者不必要的软件，常用办公必要软件必须通过官方网站进行下载安装。

5）修改电脑密码以及常用软件密码，并且密码设置不低于8个字符，包含大小写以及特俗字符。

### 预防建议

通过数据分析中的病毒如：僵尸网络系列病毒、木马远控系列病毒等，主要通过以下方式进行传播：

1）捆绑软件

2）U盘等外接设备传播

3）钓鱼邮件和钓鱼网站传播

4）系统漏洞传播

5）扫描主机弱口令漏洞传播

根据病毒的传播方式，建议进行以下操作来预防：

1）所有下载软件必须通过官网网站进行下载安装

2）通过“控制面板-系统与安全-WINDOWS防火墙”开启系统防火墙，并关闭不必要的端口。

3）下载安装正版安全杀毒与检测软件，开启实时监控与外接设备安全监测，定时对系统进行查杀病毒木马。

4）未知邮件以及未知网址，点开前需确认其的安全性，如果不能确认，尽量不要点开。

5）非安全性的外接设备禁止接入，开启安全软件U盘检测功能，自身的外接设备也不要轻易接入其他电脑，防止外接设备携带其病毒木马安装进电脑。