



OWASP

Open Web Application  
Security Project

# 关于应急响应那些事



THE SHELTER

# THE SHELTER安全团队介绍



**THE SHELTER安全团队成立于2017年，是一个非盈利性的民间网络安全技术团队，致力于分享渗透测试、安全服务、应急响应等高质量干货及案例，营造良好的技术分享氛围。**

**团队以攻与防的研究探索为核心理念。**

应急响应是为了应对**突发**信息安全事件的发生所做的准备以及在事件发生后所采取的措施。

应急响应是信息安全防护的最后  
一道防线！





# 方法论在应急响应工作上有效吗？



# 应急响应具体实施过程

常规操作：拔网线、关闭端口、IP  
加入黑名单等

# 理想中的应急过程

- 1) 是否有异常进程、用户
- 2) 敏感端口开放情况
- 3) 密码强度
- 4) 日志分析
- 5) 异常启动项、服务、计划任务
- 6) 注册表信息
- 7) 其它



# 真实的应急响应

销售? 客户?



男人的嘴 骗人的鬼

# 案例分享一

# Windows环境

## 现象：CPU占用100%，经常蓝屏。



# 案例分享一

问题一：为什么CPU占用100%

答：感染门罗币挖矿病毒。

问题二：为什么病毒删不干净

答：病毒具有持久化模块。

问题三：为什么会有大量电话

答：病毒具有横向感染模块。

The screenshot displays a threat intelligence dashboard with several key components:

- Network Traffic Log:** A list of IP addresses and their associated actions. The log shows a series of IP addresses including 192.168.199.1/24, 10.0.0.1/24, and 192.168.159.128. The actions include '远控' (Remote Control) and '恶意软件(1)' (Malware (1)).
- Threat Reports Table:** A table with columns for '情报源' (Source), '时间' (Time), '情报内容' (Content), and '状态' (Status).
 

情报源	时间	情报内容	状态
ThreatBook Labs	2019-04-25 10:00:00	永恒之蓝漏洞攻击	有效
ThreatBook Labs	2019-04-01 16:15:35	失陷主机	已过期
- Open Source Intelligence Table:** A table with columns for '情报源' (Source), '时间' (Time), '情报内容' (Content), and '状态' (Status).
 

情报源	时间	情报内容	状态
开源情报	2019-02-23 17:49:32	远程执行工具psexec攻击	有效
- Article Snippet:** A snippet from a blog titled "PowerShell版mimikatz获取登录密码" (PowerShell版mimikatz获取登录密码) dated 2019-07-16 02:43:41. The article discusses a PowerShell script for mimikatz.

1、永恒之蓝漏洞攻击

2、SMB弱口令爆破攻击

3、远程执行工具psexec攻击

4、PowerShell版mimikatz获取登录密码



# 案例分享一

## 威胁情报结论

单位感染挖矿病毒，通过威胁情报确认与“驱动人生”事件的“永恒之蓝木马下载器”病毒一致。



153.92.449

选报校 新加坡 新加坡

用户标 恶意软件(2) 门罗币挖矿(1) 中漏洞(1) 失联主机(0) 嫌疑(0)

开放端口 0 IP上相关URL 2 与该IP通信样本 20+

情报聚合 28 IP反查 19 开放端口 0 可视化 数字签名 0 用户标签 0

威胁情报

情报源	时间	情报内容	状态
ThreatBook Labs	2019-02-21 20:37:09	远控	已过期

开源情报 威胁情报的准确性进行验证，不能直接作为决策依据，仅供参考!

情报源	时间	情报内容	状态
开源情报	2019-04-15 00:32:41	恶意软件	有效
开源情报	2019-02-20 22:10:49	恶意软件	已过期

相关事件

情报源	时间
<a href="https://guanjq.qq.com/news/n3/2473.html">https://guanjq.qq.com/news/n3/2473.html</a>	2019-04-29 09:00:09
<a href="https://www.symantec.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china">https://www.symantec.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china</a>	2019-06-11 09:50:09
<a href="https://blog.talosintelligence.com/2019/05/threat-roundup-0503-0510.html">https://blog.talosintelligence.com/2019/05/threat-roundup-0503-0510.html</a>	2019-07-16 02:43:41



v.beahh.com

选报校 Cryptinject木马 驱动人生后门

用户标 远控服务器(0) 失联主机(0) 嫌疑(0)

开放端口 0 IP上相关URL 1 与该IP通信样本 19

情报聚合 33 域名解析 6 子域名 5 WHOIS 21 可视化 数字签名 0 用户标签 1

威胁情报

情报源	时间	情报内容	状态
ThreatBook Labs	2019-01-25 00:00:00	远控	有效
ThreatBook Labs	2019-04-01 16:15:35	失联主机	已过期

开源情报 威胁情报的准确性进行验证，不能直接作为决策依据，仅供参考!

情报源	时间	情报内容	状态
开源情报	2019-02-22 00:29:53	恶意软件	有效

## 案例分享二

## Linux环境



你妈喊你回家吃饭



# 案例分享二

```
nohup.out
58195711 2019-05-30 11:57:46,388 INFO [transceiver.sender.SocketSender.java:155] - sorry no file in cache of mapping 'localtohresource'
58195712 2019-05-30 11:57:46,388 INFO [transceiver.sender.SocketSender.java:155] - sorry no file in cache of mapping 'localtomzdxww'
58195713 2019-05-30 11:57:46,388 INFO [transceiver.sender.SocketSender.java:155] - sorry no file in cache of mapping 'localtohnews'
58195714 2019-05-30 11:57:46,469 INFO [transceiver.sender.SocketSender.java:155] - sorry no file in cache of mapping 'localtoyxww'
58195715 2019-05-30 11:57:46,469 INFO [transceiver.sender.SocketSender.java:155] - sorry no file in cache of mapping 'localtofjyt'
```

```
[root@CentOS6 45310]# lsof -p 45310
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
bash 45310 root cwd DIR 202,2 4096 2 /
bash 45310 root rtd DIR 202,2 4096 2 /
bash 45310 root txt REG 202,2 941720 142512 /bin/bash
bash 45310 root mem REG 202,2 157072 31327 /lib64/ld-2.12.so
bash 45310 root mem REG 202,2 1928936 38987 /lib64/libc-2.12.so
bash 45310 root mem REG 202,2 22536 6661 /lib64/libdl-2.12.so
bash 45310 root mem REG 202,2 134792 17010 /lib64/libtinfo.so.5.7
bash 45310 root mem REG 202,2 99160384 31734 /usr/lib/locale/locale-archive
bash 45310 root mem REG 202,2 26060 6610 /usr/lib64/gconv/gconv-modules.cache
bash 45310 root 0u IPv4 63712573 0t0 TCP 172.16.4. :50447->45.32.114.106.vultr.com:6554 (ESTABLISHED)
bash 45310 root 1u IPv4 63712573 0t0 TCP 172.16.4. :50447->45.32.114.106.vultr.com:6554 (ESTABLISHED)
bash 45310 root 2u IPv4 63712573 0t0 TCP 172.16.4. :50447->45.32.114.106.vultr.com:6554 (ESTABLISHED)
bash 45310 root 3u IPv4 63712573 0t0 TCP 172.16.4. :50447->45.32.114.106.vultr.com:6554 (ESTABLISHED)
```

页面

general\hr\training\analysis\index.php	2	简版Zend加密(可疑)	
general\system\workflow\flow_hook\condition_set_ajax.php	2	简版Zend加密(可疑)	
general\vmest\upload\temp\555.php.lll	4	Eval后门(参数:base64_decode(\$_POST["xjsbl23gun"]))	51 2019-03-28 14:43:52 F719F
general\crm\modules\Marketing\DetailView\DetailFooter.php	2	简版Zend加密(可疑)	138 2018-07-27 22:56:45 BACT2
general\crm\modules\Marketing\EditView\EditFooter.php	2	简版Zend加密(可疑)	137 2018-07-27 22:56:45 684DC
general\crm\modules\Marketing\EditView\EditHeader.php	2	简版Zend加密(可疑)	137 2018-07-27 22:56:45 6E3C0
general\crm\modules\ReportView\report>ShowRowsAndColsReportOutput.php	2	简版Zend加密(可疑)	135 2018-07-27 22:56:47 523C9
general\crm\studio\modules\Guide\tree.php	2	简版Zend加密(可疑)	173 2018-07-27 22:56:52 B582F
			127 2018-07-27 22:57:23 9CB46
			197 2018-07-27 22:57:24 E1DF1

```
H? H%Çèö?ÿH%A<EüH`HÁa<0x03>H<0x03>ÈàH? ? H%ÇèU?ÿfE?<E?Ei|Xè4?ÿ...At
<0x90><0x90><0x90><0x90><0x90><0x90><0x90><0x90>ôÄfffff.<0x0f><0x1f>? H%l$ØL&d$àH??<0x04>
>1?<0x1f>@ L%úL%òD%íÄÿ<0x14>ÜHfÁ<0x01>H9èrèH\<$<0x08>H<l$<0x10>L<d$<0x18>L<l$
8>H?? Hföÿt<0x19>? <0x10>? <0x0f><0x1f>>D
x01> <0x02>
0x14> <0x01>xZr <0x01>x<0x10><0x01><0x1b><0x0c><0x07><0x08>? <0x1c> <0x1c>
0e><0x10>?C
0e>@????<0x02>X<0x0e><0x08>
y close sleep __libc_start_main write GLIBC_2.2.5 /lib64/ld-linux-x86-64.so.2
```

```
执行 参数: {"0+(){}|/([,/]*)0*", "$v...
'localtojryaw'
'localtowuping'
'localtosxww'
'localtozkfqa'
'localtosxww'
'localtozaxww'
'localtomazucity'
'localtojrjonews'
'localtofjqlw'
```



## 威胁事件结论



炊少

精通linux，擅长web提权，留后门，目前入侵国内多家媒体网站，例如光明网，等各类知名站点

黑客由兄弟单位入侵至本单位，利用

劫持页面<http://edu.gmw.cn/kaima/index.htm>

目前在马来西亚从事博彩黑产业，自己手里有多个博彩盘口，月入500万以上

黑产手段如博彩页面进行盈利，关联至”

盘口如下

“黑产黑客-炊少”人物。

<https://18n.com/18彩票>

<https://www.998f.cc> 久久发彩票

<https://www1000.cc> 千亿娱乐

等10多个盘口

曾经做过名为亚洲集团的引流导航网站



4,106.vultr.com  
IPA - Choopa, LLC.

API接口



# 威胁情报驱动应急响应

IOC(攻陷指标) ≠ 威胁情报

# 怎么样才能称之为威胁情报？

数据 + 分析 + 传播 = 威胁情报

# 分享是人性深处的一种本能



## 微信公众号

# 感谢观看

**THANKS FOR WATCHING**