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！

OWASP
Open Web Application Security Project

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

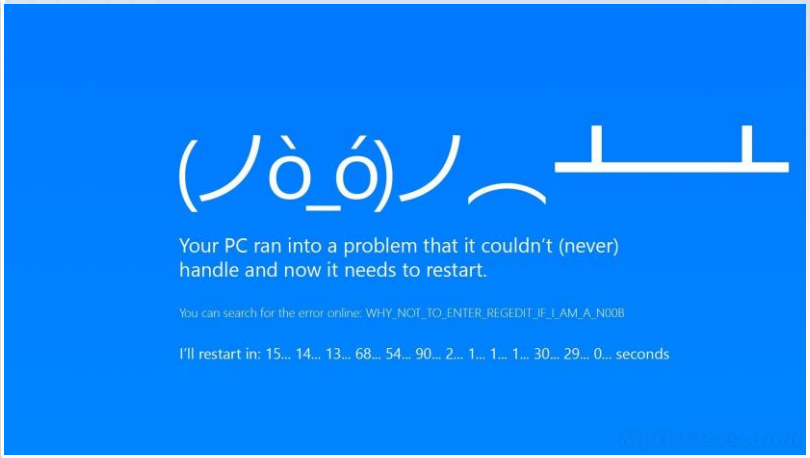
1) 是否有异常进程、用户
2) 敏感端口开放情况
3) 密码强度
4) 日志分析
5) 异常启动项、服务、计划任务
6) 注册表信息
7) 其它

真实的应急响应

销售？客户？

案例分享一 Windows环境

现象：CPU占用100%，经常蓝屏。



OWASP
Open Web Application Security Project

案例分享一

问题一：为什么CPU占用1

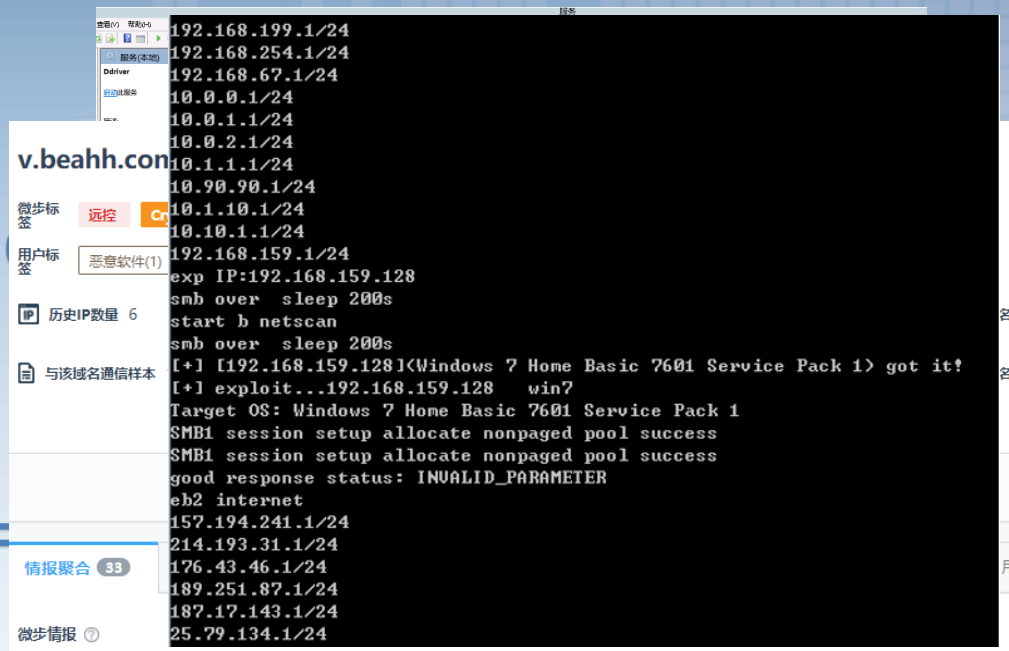
答：感染门罗币挖矿病毒。

问题二：为什么病毒删不干

答：病毒具有持久化模块。

问题三：为什么会有大量电

答：病毒具有横向感染模块。



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

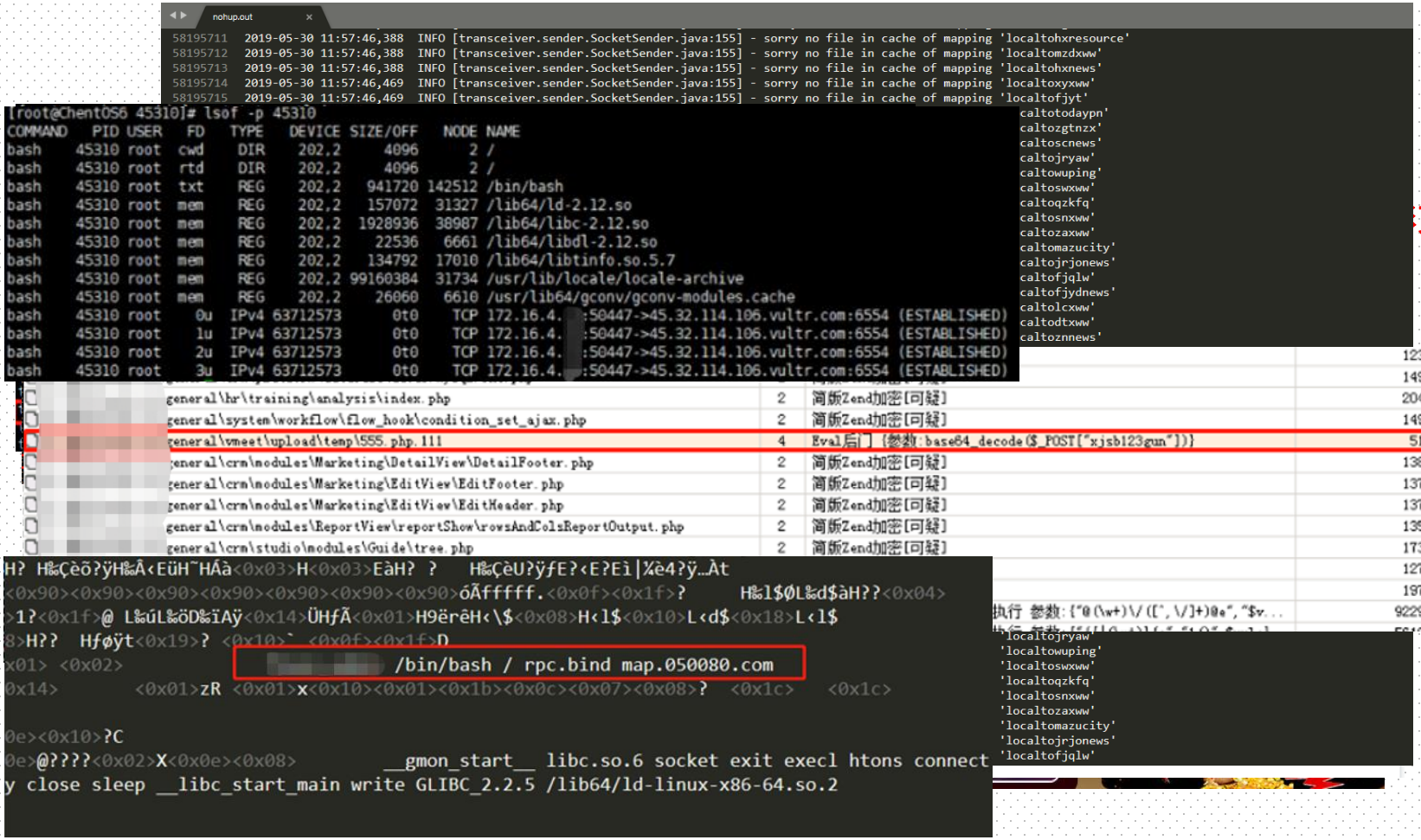
单位感染挖矿病毒，通过威胁情报确认与“驱动人生”事件的“永恒之蓝木马下载器”病毒一致。

案例分享二 Linux环境

你妈喊你回家吃饭

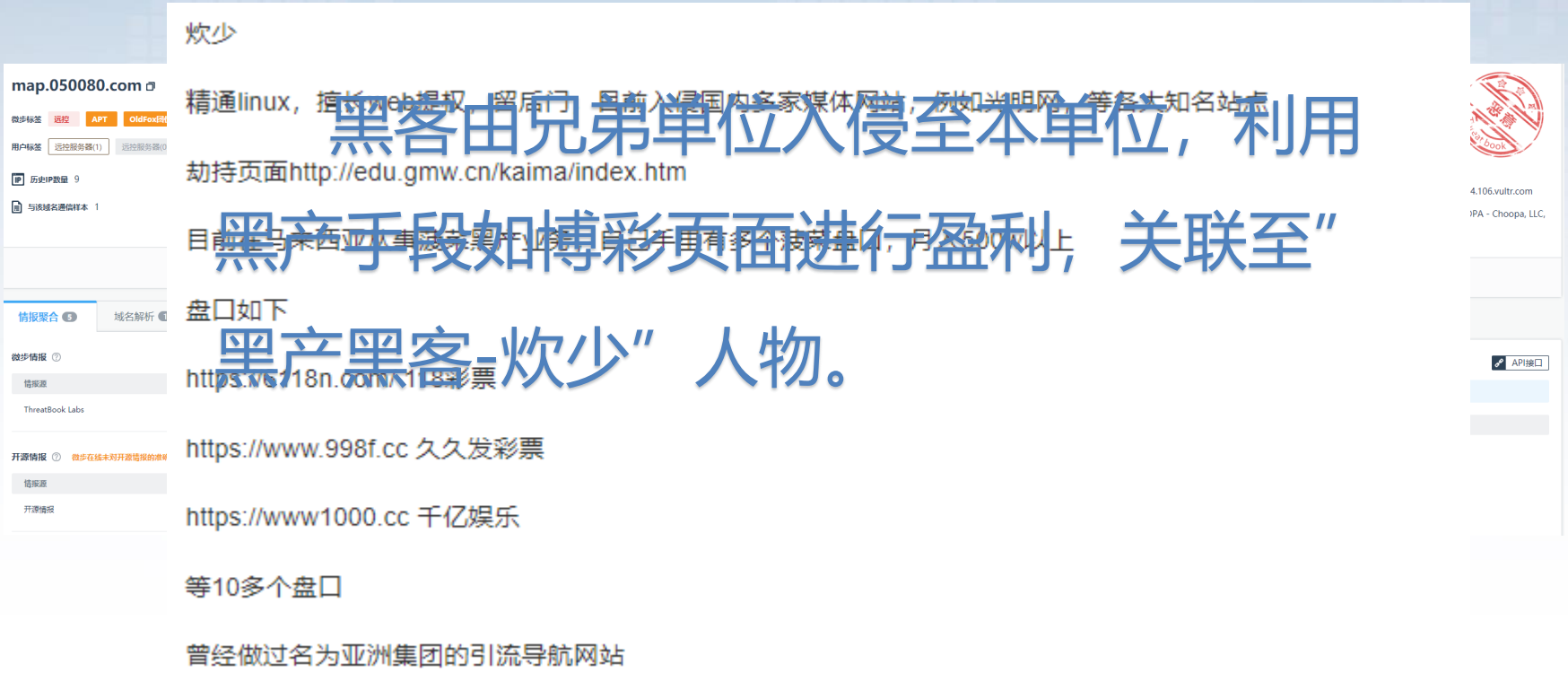
OWASP
Open Web Application Security Project

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 'localtohxresource'
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 'localtohxnews'
58195714 2019-05-30 11:57:46,469 INFO [transceiver.sender.SocketSender.java:155] - sorry no file in cache of mapping 'localtoxyxww'
58195715 2019-05-30 11:57:46,469 INFO [transceiver.sender.SocketSender.java:155] - sorry no file in cache of mapping 'localtofjyt'
[root@ChentOS6 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)
caltotodaypn'
caltozgtnzx'
caltoscnews'
caltojryaw'
caltowuping'
caltoswxww'
caltoqzkfq'
caltosnxww'
caltozaxww'
caltomazucity'
caltojrjonews'
caltofjqlw'
caltofjydnews'
caltolcxww'
caltodtxww'
caltoznnews'
页面
general\hr\training\analysis\index.php 2 简版Zend加密[可疑] 123 2018-07-27 22:56:49 B9F8D
general\system\workflow\flow_hook\condition_set_ajax.php 2 简版Zend加密[可疑] 149 2018-07-27 22:56:49 5D107
general\vmeet\upload\temp\555.php.111 4 Eval后门（参数:base64_decode($_POST["xjsb123gun"])） 204 2018-07-27 22:57:04 26F96
general\crm\modules\Marketing\DetailView\DetailFooter.php 2 简版Zend加密[可疑] 149 2018-07-27 22:57:31 1C4A8
general\crm\modules\Marketing\EditView\EditFooter.php 2 简版Zend加密[可疑] 51 2019-03-28 14:43:52 F719F
general\crm\modules\Marketing\EditView\EditHeader.php 2 简版Zend加密[可疑] 138 2018-07-27 22:56:45 BAC72
general\crm\modules\ReportView\reportShow\rowsAndColsReportOutput.php 2 简版Zend加密[可疑] 137 2018-07-27 22:56:45 684DC
general\crm\studio\modules\Guide\tree.php 2 简版Zend加密[可疑] 137 2018-07-27 22:56:45 6E3C0
135 2018-07-27 22:56:47 523C9
173 2018-07-27 22:56:52 B582F
127 2018-07-27 22:57:23 9CB46
197 2018-07-27 22:57:24 E1DF1
执行 参数:{"@(\w+)\/([^,\/]+)@e","$v... 9229 2018-07-27 22:58:59 6E289
H? H‰ÇèÕ?ÿH‰Â‹EüH¯HÁà<0x03>H<0x03>ÈàH? ? H‰ÇèU?ÿƒE?‹E?Ei|%è4?ÿ…Àt
<0x90><0x90><0x90><0x90><0x90><0x90><0x90>óÃfffff.<0x0f><0x1f>? H‰l$ØL‰d$àH??<0x04>
>1?<0x1f>@ L‰úL‰ÕD‰ïAÿ<0x14>ÜHƒÃ<0x01>H9ërêH‹\$<0x08>H‹l$<0x10>L‹d$<0x18>L‹l$
8>H?? Hƒøÿt<0x19>? <0x10>` <0x0f><0x1f>D
x01> <0x02>
/bin/bash / rpc.bind map.050080.com
0x14> <0x01>zR <0x01>x<0x10><0x01><0x1b><0x0c><0x07><0x08>? <0x1c> <0x1c>
0e><0x10>?C
0e>@????<0x02>X<0x0e><0x08> __gmon_start__ libc.so.6 socket exit execl htons connect
y close sleep __libc_start_main write GLIBC_2.2.5 /lib64/ld-linux-x86-64.so.2
'localtojryaw'
'localtowuping'
'localtoswxww'
'localtoqzkfq'
'localtosnxww'
'localtozaxww'
'localtomazucity'
'localtojrjonews'
'localtofjqlw'

案例分享二 Linux环境

威胁情报结论



黑客由兄弟单位入侵至本单位，利用黑产手段如博彩页面进行盈利，关联至”黑产黑客-炊少”人物。

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

OWASP
Open Web Application
Security Project

感谢观看

THANKS FOR WATCHING