抓包分析

2018年5月26日 22:40

1. 软件先发一个向百度的请求,然后学校的代理服务器进行拦截,然后返回一个要登陆的地址

```
GET / HTTP/1.1
User-Agent: China Telecom Client
Host: www.baidu.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Cache-control: no-cache
Connection: close
Content-Type: text/html
Content-length: 369

<html>
<head>
<script type="text/javascript">location.href="http://124.225.128.205:10001/xyportal/?wlanuserip=10.20.2.141&wlanacip=202.100.206.253"</script>
</head>
<body>
Authentication is required. Click <a href="http://124.225.128.205:10001/xyportal/?wlanuserip=10.20.2.141&wlanacip=202.100.206.253">here</a> to open the authentication page.
</body>
</html>
```

2. 软件请求登陆地址,得到UUID和真正的登陆地址

```
GET /xyportal/?wlanuserip=10.20.2.141&wlanacip=202.100.206.253 HTTP/1.1
User-Agent: China Telecom Client
Host: 124.225.128.205:10001
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/xml;charset=utf-8
Transfer-Encoding: chunked
Date: Sat, 26 May 2018 09:54:25 GMT
Connection: close

240
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGatewayParam.xsd">
        <Redirect>
                <AccessProcedure>1.0</AccessProcedure>
                <AcName>202.100.206.253</AcName>
                <UserIp>10.20.2.141</UserIp>
                <LoginURL>http://124.225.128.205:10001/xyportal/wisp/login</LoginURL>
                <Uuid>871i2gkcjrjnuqokas05e7y9uo1itxfmguyk35qg3j6woltu2tpg8qfq875mqi2y</Uuid>
                <MessageType>100</MessageType>
        <ResponseCode>0</ResponseCode>
    </Redirect>
</WISPAccessGatewayParam>
```

3. 向真正的登陆地址发送登陆信息,

包括

uuid	acname	userip	username	加密后的passwd	ratingtype

```
POST /xyportal/wisp/login HTTP/1.1
User-Agent: China Telecom Client
Content-Length: 187
Content-Type: application/x-www-form-urlencoded
Host: 124.225.128.205:10001
Connection: Keep-Alive

uuid=871i2gkcjrjnuqokas05e7y9uo1itxfmguyk35qg3j6woltu2tpg8qfq875mqi2y&acname=
202.100.206.253&userip=10.20.2.141&username=17389717332&password=
57A45DB00874F58676D0C04B4FC89D09&ratingtype=0
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/xml;charset=utf-8
Transfer-Encoding: chunked
Date: Sat, 26 May 2018 09:54:25 GMT
Connection: close

232
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://wlan.ct10000.com/WISPAccessGatewayParam.xsd">
    <AuthenticationReply>
        <MessageType>120</MessageType>
        <ResponseCode>200</ResponseCode>
        <LogoffURL>http://124.225.128.205:10001/xyportal/wisp/logout</LogoffURL>
        <AcName>202.100.206.253</AcName>
        <UserIp>10.20.2.141</UserIp>
        <Uuid>
        c8vs2noin8bcbnthzkvciwm1v1v8netpjskmko2av1aidauzznr980br0n9v621z</Uuid>
    </AuthenticationReply>
</WISPAccessGatewayParam>
0
```

4. 下线

```
POST /xyportal/wisp/logout HTTP/1.1
User-Agent: China Telecom Client
Content-Length: 111
Content-Type: application/x-www-form-urlencoded
Host: 124.225.128.205:10001
Connection: Keep-Alive

uuid=c8vs2noin8bcbnthzkvciwm1v1v8netpjskmko2av1aidauzznr980br0n9v621z&userip=
10.20.2.141&acname=202.100.206.253


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
```

```
Content-Type: text/xml;charset=utf-8
Transfer-Encoding: chunked
Date: Sat, 26 May 2018 09:54:48 GMT
Connection: close

1a9
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.wlan.ct10000.com/WISPAccessGatewayPara
m.xsd">
	<LogoffReply>
		<MessageType>130</MessageType>
		<ResponseCode>255</ResponseCode>
		<AcName>202.100.206.253</AcName>
		<UserIp>10.20.2.141</UserIp>
		<Date>20180526175448</Date>
	</LogoffReply>
</WISPAccessGatewayParam>
0
```