WPAD ATTACK

sanr

2016.12.14

是什么　　危害　　原理

WPAD

攻击测试　　Case分享　　修复方案

简述

Wpad全称网络代理自动发现协议WPAD（Web Proxy Autodiscovery Protocol），
通过让浏览器自动发现代理服务器,由于配置代理服务器的方式对于用户来说是透明的，无需用户手动操作的，几乎所有操作系统都支持WPAD，但只有Windows系统默认启用这个协议。按照WPAD协议，系统会试图访问http://WPAD/wpad.dat，以获取代理配置脚本

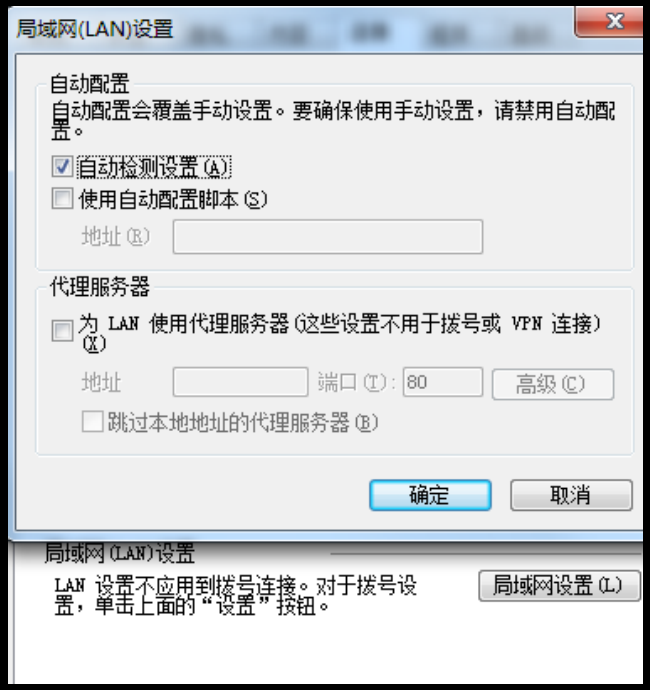
危害

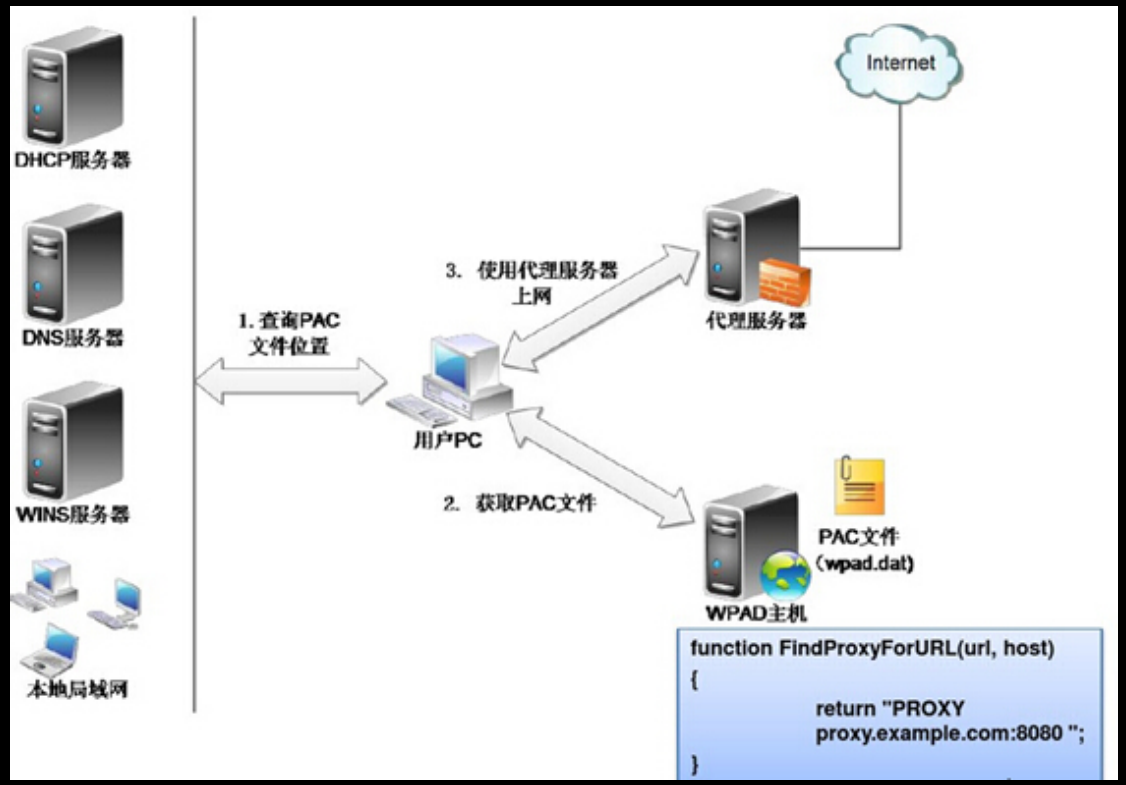
劫持“WPAD”名称之后，可以劫持用户的网络通信,进行缓存攻击,更新劫持,cookie劫持等操作。

2012年Flame蠕虫病毒使用WPAD劫持Windows Update的请求,受害者下载假冒的补丁包

原理

PAC文件查找






```
function FindProxyForURL(url, host) {
  if (shExpMatch(url,"*.google.com*")) {
    return "SOCKS5 127.0.0.1:1080";
  }
  return "DIRECT";
}
```

原理　DHCP

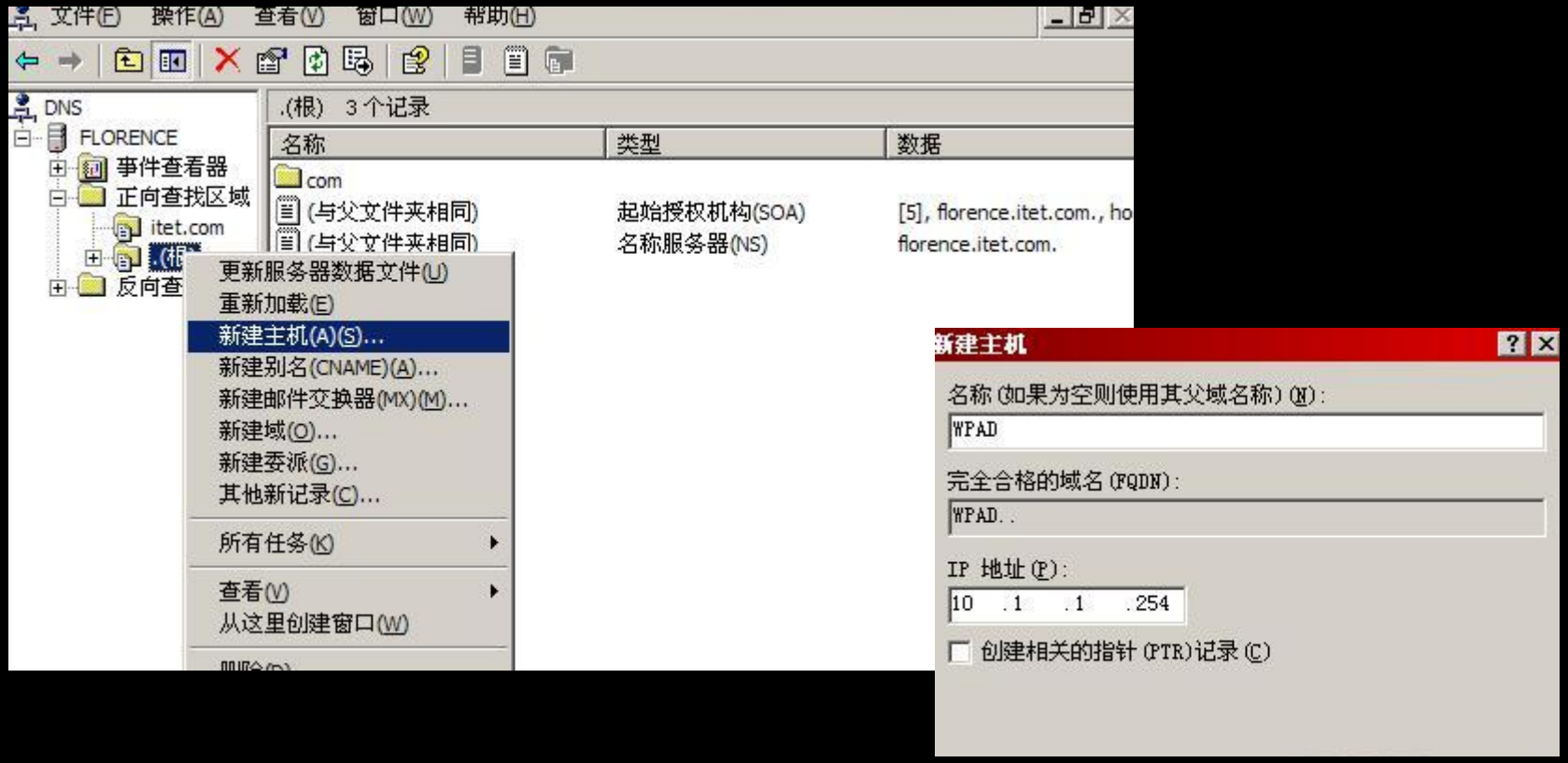

文件(F)
操作(A)
查看(V)
帮助(H)
DHCP
florence [10.1.1.101]
作用域 [10.1
地址池
地址租约
保留
作用域选
服务器选项
显示统计信息(S)...
新建作用域(P)...
新建超级作用域(U)...
新建多播作用域(M)...
备份(B)...
还原(O)...
协调所有作用域(A)...
定义用户类别(N)...
定义供应商类别(C)...
设置预定义的选项(E)...
所有任务(K)
查看(V)
删除(D)
刷新(F)


预定义的选项和值
选项类别(N):
DHCP 标准选项
选项名(O):
002 时间偏移
添加(A)...
编辑(E)...
删除(D)
描述:
UCT 偏移(以秒计)
值
长整型(L):
0x0

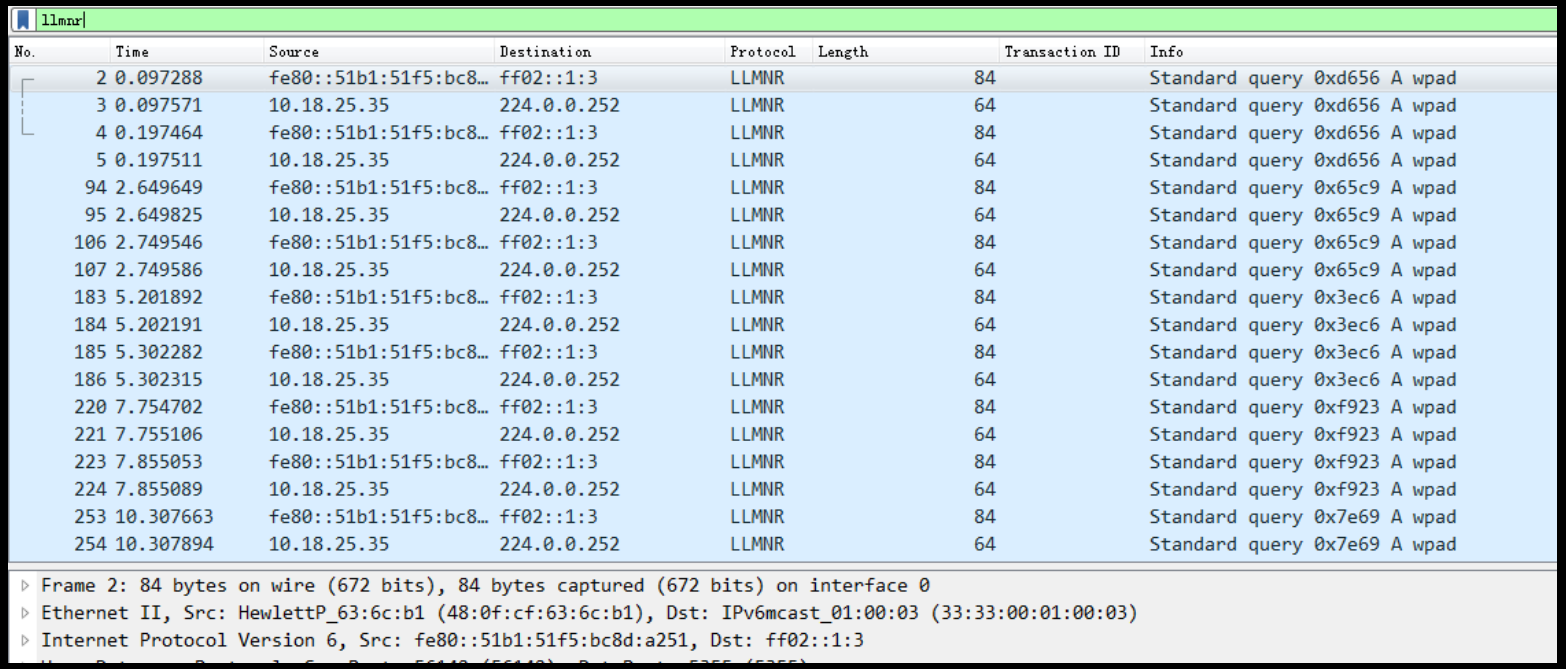
类别:
全局
名称(N):
WPAD
数据类型(D):
字符串
数组(A)
代码(C):
252
描述(E):
确定
取消
51CTO.com


选项类别(N):
DHCP 标准选项
选项名(O):
252 WPAD
添加(A)...
编辑(E)...
删除(D)
描述:
值
字符串(S):
http://10.1.1.254:8000/wpad.dat

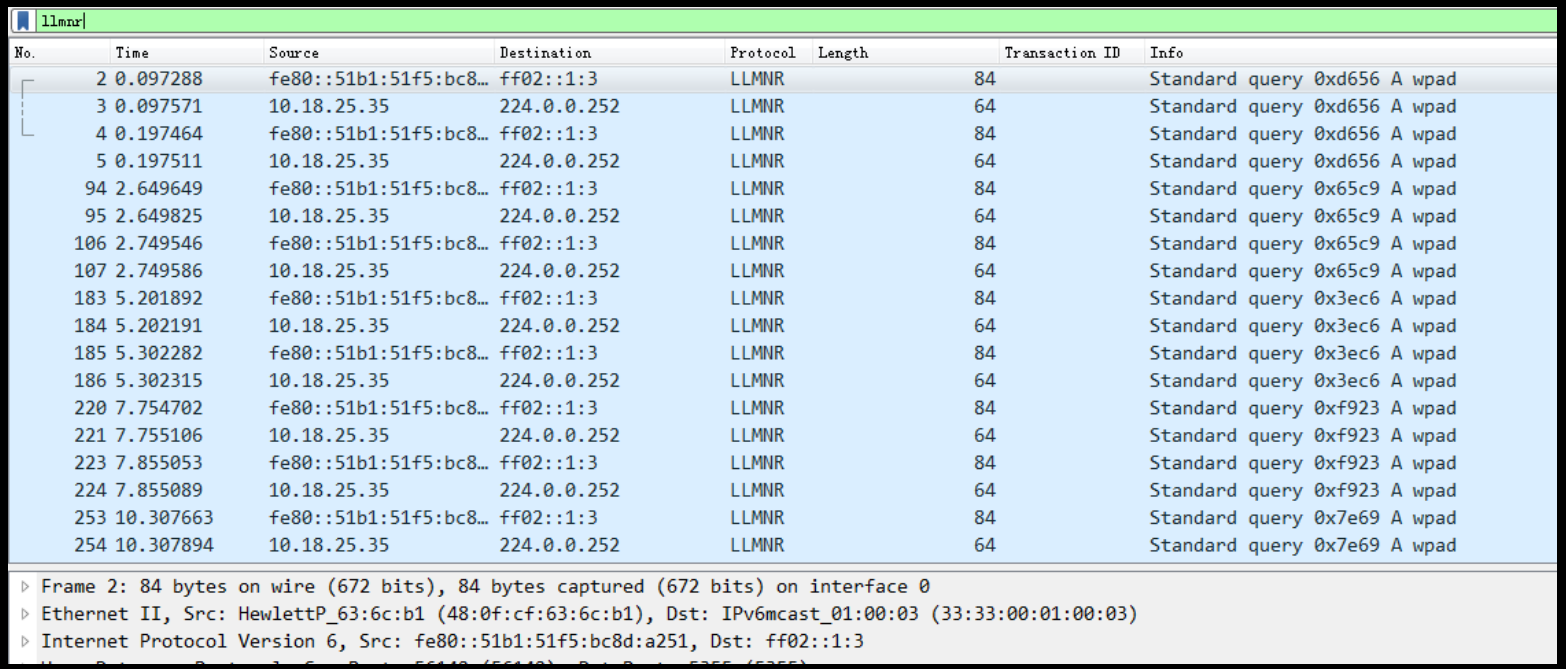
原理　DNS


文件(F)
操作(A)
查看(V)
窗口(W)
帮助(H)
DNS
FLORENCE
事件查看器
正向查找区域
itet.com
反向查
.(根)　3 个记录
名称
类型
数据
com
(与父文件夹相同)
起始授权机构(SOA)
[5], florence.itet.com., ho
(与父文件夹相同)
名称服务器(NS)
florence.itet.com.
更新服务器数据文件(U)
重新加载(E)
新建主机(A)(S)...
新建别名(CNAME)(A)...
新建邮件交换器(MX)(M)...
新建域(O)...
新建委派(G)...
其他新记录(C)...
所有任务(K)
查看(V)
从这里创建窗口(W)
新建主机
名称(如果为空则使用其父域名称)(N):
WPAD
完全合格的域名(FQDN):
WPAD..
IP 地址(P):
10 .1 .1 .254
创建相关的指针(PTR)记录(C)

原理　LLMNR （Vista加入）



原理 NBNS

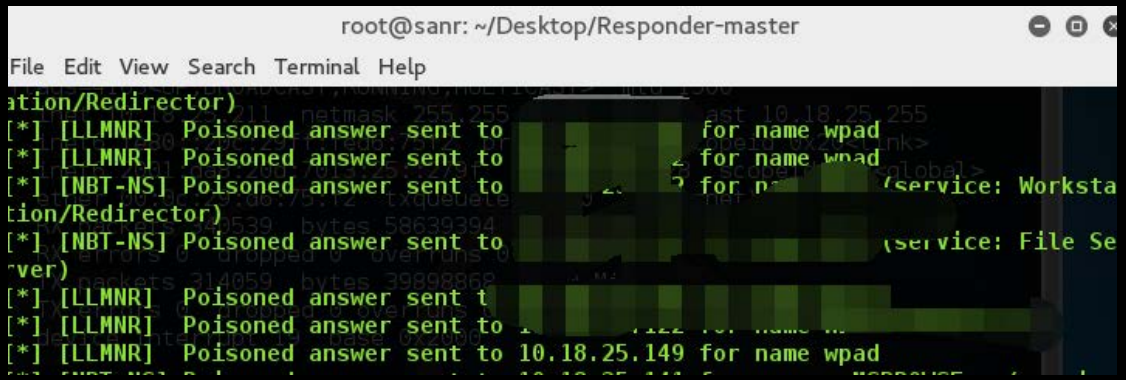

llmnr
No. Time Source Destination Protocol Length Transaction ID Info
2 0.097288 fe80::51b1:51f5:bc8… ff02::1:3 LLMNR 84 Standard query 0xd656 A wpad
3 0.097571 10.18.25.35 224.0.0.252 LLMNR 64 Standard query 0xd656 A wpad
4 0.197464 fe80::51b1:51f5:bc8… ff02::1:3 LLMNR 84 Standard query 0xd656 A wpad
5 0.197511 10.18.25.35 224.0.0.252 LLMNR 64 Standard query 0xd656 A wpad
94 2.649649 fe80::51b1:51f5:bc8… ff02::1:3 LLMNR 84 Standard query 0x65c9 A wpad
95 2.649825 10.18.25.35 224.0.0.252 LLMNR 64 Standard query 0x65c9 A wpad
106 2.749546 fe80::51b1:51f5:bc8… ff02::1:3 LLMNR 84 Standard query 0x65c9 A wpad
107 2.749586 10.18.25.35 224.0.0.252 LLMNR 64 Standard query 0x65c9 A wpad
183 5.201892 fe80::51b1:51f5:bc8… ff02::1:3 LLMNR 84 Standard query 0x3ec6 A wpad
184 5.202191 10.18.25.35 224.0.0.252 LLMNR 64 Standard query 0x3ec6 A wpad
185 5.302282 fe80::51b1:51f5:bc8… ff02::1:3 LLMNR 84 Standard query 0x3ec6 A wpad
186 5.302315 10.18.25.35 224.0.0.252 LLMNR 64 Standard query 0x3ec6 A wpad
220 7.754702 fe80::51b1:51f5:bc8… ff02::1:3 LLMNR 84 Standard query 0xf923 A wpad
221 7.755106 10.18.25.35 224.0.0.252 LLMNR 64 Standard query 0xf923 A wpad
223 7.855053 fe80::51b1:51f5:bc8… ff02::1:3 LLMNR 84 Standard query 0xf923 A wpad
224 7.855089 10.18.25.35 224.0.0.252 LLMNR 64 Standard query 0xf923 A wpad
253 10.307663 fe80::51b1:51f5:bc8… ff02::1:3 LLMNR 84 Standard query 0x7e69 A wpad
254 10.307894 10.18.25.35 224.0.0.252 LLMNR 64 Standard query 0x7e69 A wpad
Frame 2: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Ethernet II, Src: HewlettP_63:6c:b1 (48:0f:cf:63:6c:b1), Dst: IPv6mcast_01:00:03 (33:33:00:01:00:03)
Internet Protocol Version 6, Src: fe80::51b1:51f5:bc8d:a251, Dst: ff02::1:3

劫持测试

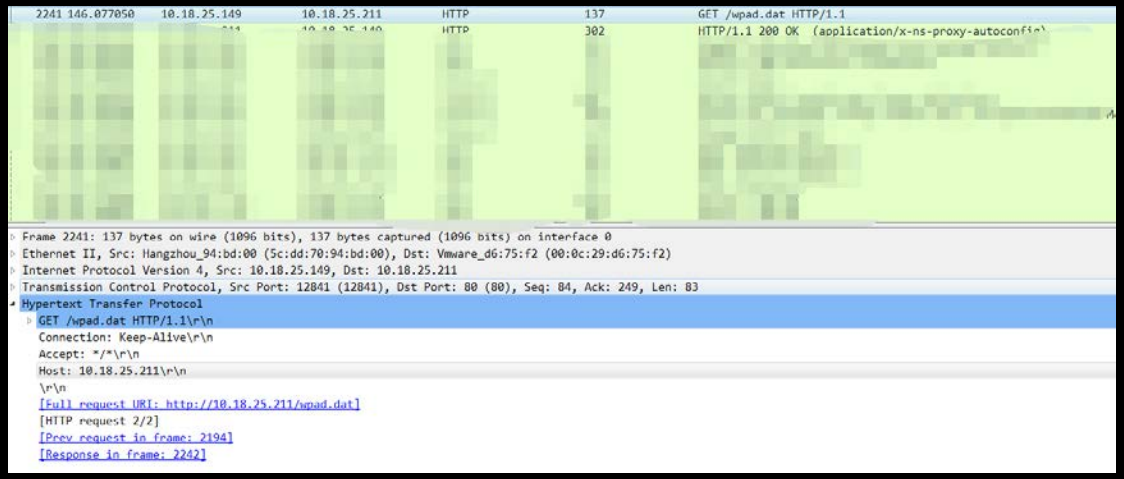
劫持测试

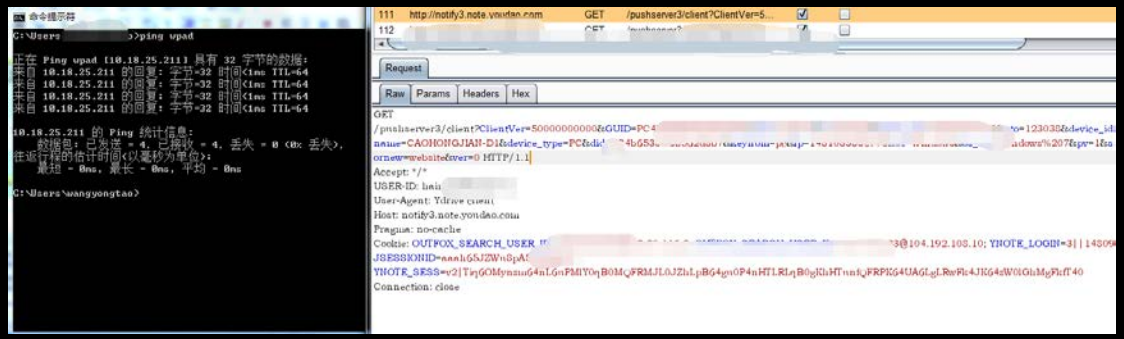
2236 145.876038	fe80::15cd:cfa7:f8c…	ff02::1:3	LLMNR	84	Standard query 0x6930 A wpad
2237 145.876228	10.18.25.149	224.0.0.252	LLMNR	64	Standard query 0x6930 A wpad
2238 145.876954	10.18.25.211	10.18.25.149	LLMNR	84	Standard query response 0x6930 A wpad A 10.18.25.211

```
▷ Frame 2237: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
▷ Ethernet II, Src: HewlettP_3f:ae:41 (40:a8:f0:3f:ae:41), Dst: IPv4mcast_fc (01:00:5e:00:00:fc)
▷ Internet Protocol Version 4, Src: 10.18.25.149, Dst: 224.0.0.252
▷ User Datagram Protocol, Src Port: 61014 (61014), Dst Port: 5355 (5355)
▷ Link-local Multicast Name Resolution (query)
```



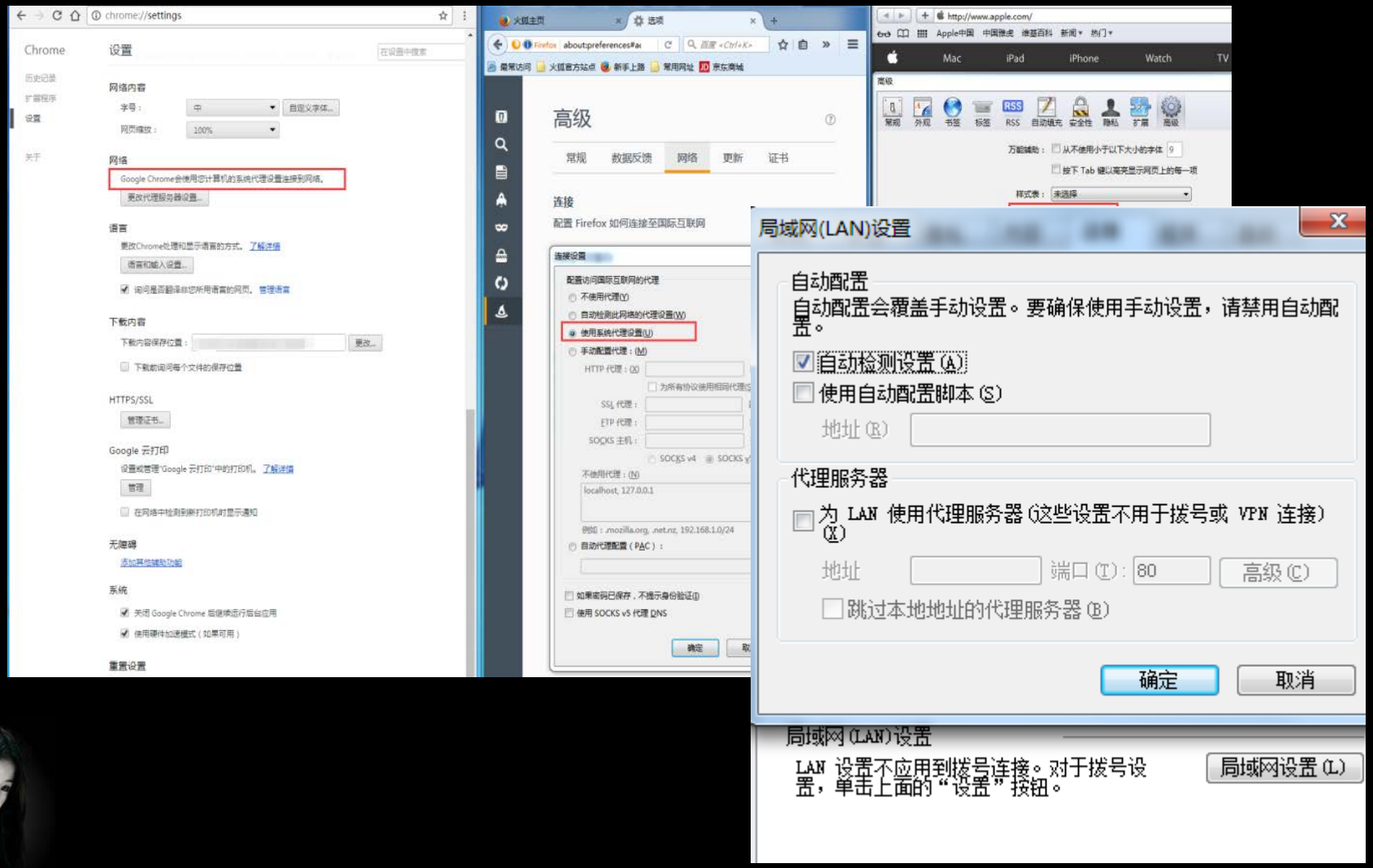
劫持测试


2241 146.077050 10.18.25.149 10.18.25.211 HTTP 137 GET /wpad.dat HTTP/1.1
HTTP 302 HTTP/1.1 200 OK (application/x-ns-proxy-autoconfig)
Frame 2241: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0
Ethernet II, Src: Hangzhou_94:bd:00 (5c:dd:70:94:bd:00), Dst: Vmware_d6:75:f2 (00:0c:29:d6:75:f2)
Internet Protocol Version 4, Src: 10.18.25.149, Dst: 10.18.25.211
Transmission Control Protocol, Src Port: 12841 (12841), Dst Port: 80 (80), Seq: 84, Ack: 249, Len: 83
Hypertext Transfer Protocol
GET /wpad.dat HTTP/1.1\r\n
Connection: Keep-Alive\r\n
Accept: */*\r\n
Host: 10.18.25.211\r\n
\r\n
[Full request URI: http://10.18.25.211/wpad.dat]
[HTTP request 2/2]
[Prev request in frame: 2194]
[Response in frame: 2242]

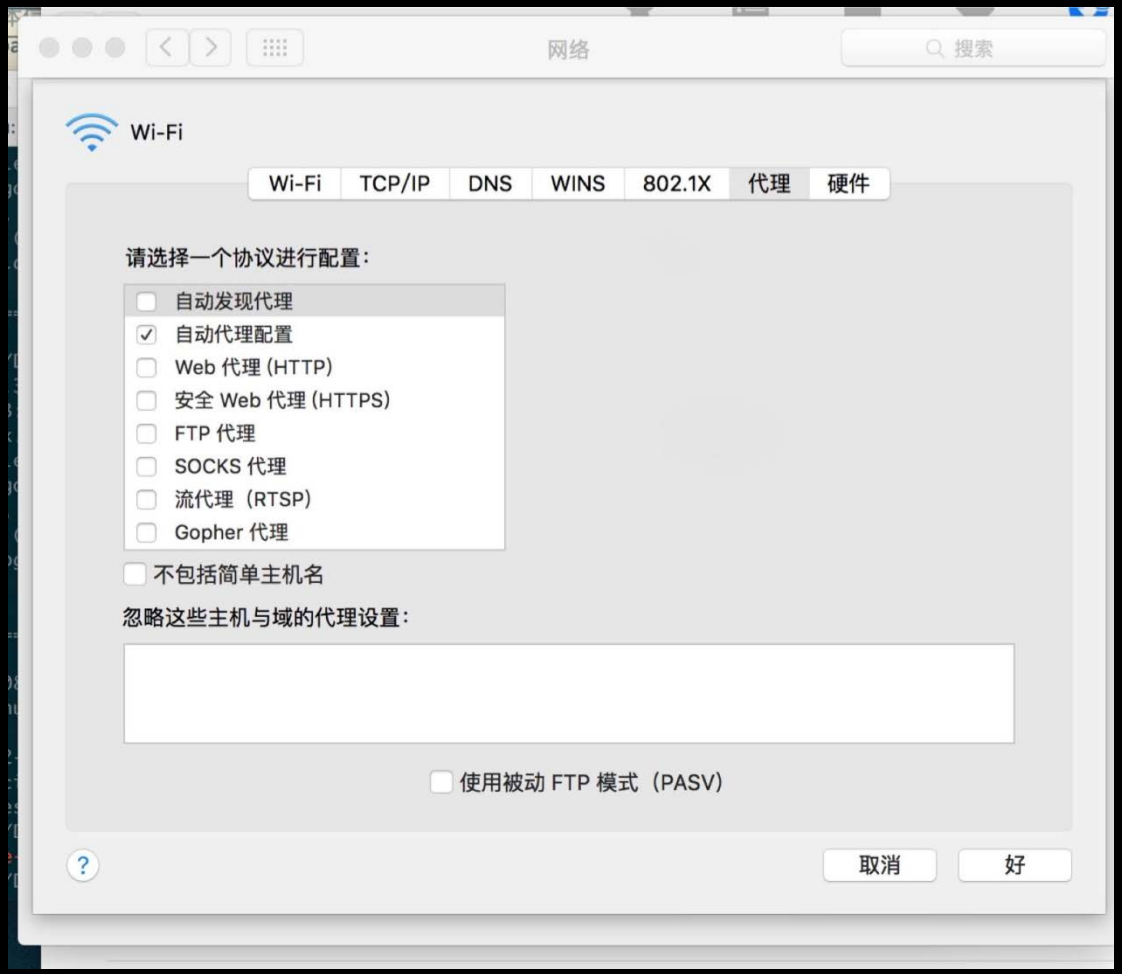

命令提示符
>>ping wpad
正在 Ping wpad [10.18.25.211] 具有 32 字节的数据:
来自 10.18.25.211 的回复: 字节=32 时间<1ms TTL=64
来自 10.18.25.211 的回复: 字节=32 时间<1ms TTL=64
来自 10.18.25.211 的回复: 字节=32 时间<1ms TTL=64
来自 10.18.25.211 的回复: 字节=32 时间<1ms TTL=64
10.18.25.211 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 0ms, 最长 = 0ms, 平均 = 0ms
C:\Users\wangyongtao>
111 http://notify3.note.youdao.com GET /pushserver3/client?ClientVer=5...
112
Request
Raw Params Headers Hex
GET
/pushserver3/client?ClientVer=500000000000&GUID=PC4
name=CAONONGJIAN-D1&device_type=PC&dic
ornew=website&ver=0 HTTP/1.1
Accept: */*
USER-ID: lmin
User-Agent: Ydrive client
Host: notify3.note.youdao.com
Pragma: no-cache
Cookie: OUTFOX_SEARCH_USER_ID
JSESSIONID=aaah6SJZWn8pA
YNOTE_SESS=v2|TmjGOMymzuu64nLGnPMlY0qB0MQFRMJL0JZhLpBG4gn0P4nHTLRLqB0gKhHTunkQFRPK64UAGLgLRwFk4JK64eW0GhMgFkff40
Connection: close

影响平台

window


chrome://settings
Chrome
设置
网络内容
网络
Google Chrome会使用您计算机的系统代理设置连接到网络。
更改代理服务器设置...
语言
下载内容
HTTPS/SSL
Google 云打印
无障碍
系统
重置设置
高级
常规
数据反馈
网络
更新
证书
连接
配置 Firefox 如何连接至国际互联网
使用系统代理设置(U)
http://www.apple.com/
Mac
iPad
iPhone
Watch
局域网(LAN)设置
自动配置
自动配置会覆盖手动设置。要确保使用手动设置，请禁用自动配置。
自动检测设置(A)
使用自动配置脚本(S)
地址(R)
代理服务器
为 LAN 使用代理服务器(这些设置不用于拨号或 VPN 连接)(X)
地址
端口(T):
80
高级(C)
跳过本地地址的代理服务器(B)
确定
取消
局域网(LAN)设置
LAN 设置不应用到拨号连接。对于拨号设置，单击上面的“设置”按钮。
局域网设置(L)

Mac os

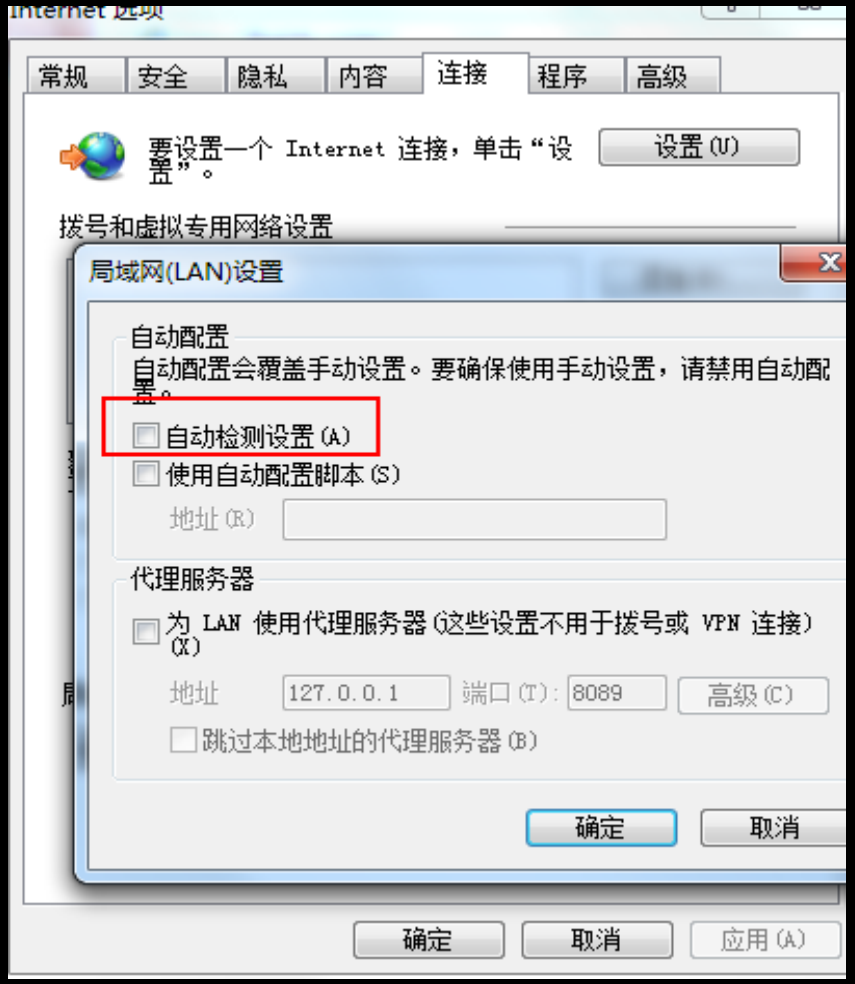

网络
搜索
Wi-Fi
Wi-Fi
TCP/IP
DNS
WINS
802.1X
代理
硬件
请选择一个协议进行配置：
自动发现代理
自动代理配置
Web 代理 (HTTP)
安全 Web 代理 (HTTPS)
FTP 代理
SOCKS 代理
流代理（RTSP)
Gopher 代理
不包括简单主机名
忽略这些主机与域的代理设置：
使用被动 FTP 模式（PASV)
?
取消
好

Case分享

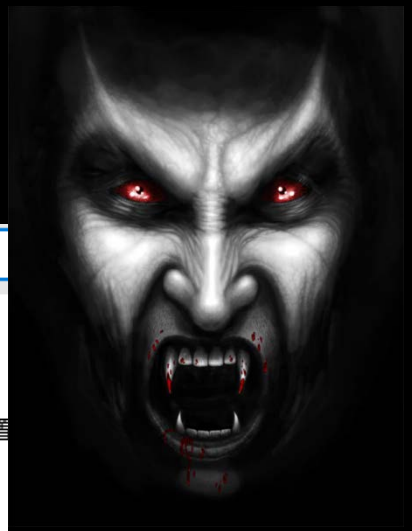
1.用手机从锁定的计算机中偷取凭证信息
http://www.freebuf.com/news/120174.html
2.使用恶意USB设备解锁任意锁屏状态Windows、Mac
http://bobao.360.cn/learning/detail/3005.html
3.仅使用5美元设备，在锁定的计算机中植入Web后门
http://bobao.360.cn/learning/detail/3203.html

修复方案

Windows 7, Vista, XP



Win10、Win8.1、Win8



网络和 INTERNET

查找设置

数据使用量

VPN

拨号

以太网

代理

自动设置代理

将代理服务器用于以太网或 Wi-Fi 连接。这些设置
连接。

自动检测设置

开

使用安装程序脚本

关

脚本地址

保存

手动设置代理

将代理服务器用于以太网或 Wi-Fi 连接。这些设置
连接。

Mac os


Wi-Fi
Wi-Fi
TCP/IP
DNS
WINS
802.1X
代理
硬件
请选择一个协议进行配置:
自动发现代理
自动代理配置
Web 代理 (HTTP)
安全 Web 代理 (HTTPS)
FTP 代理
SOCKS 代理
流代理（RTSP)
Gopher 代理
不包括简单主机名
忽略这些主机与域的代理设置:
使用被动 FTP 模式（PASV)

剧终