A survey of phishing attacks: Their types, vectors, and technical approaches

> 一份调查网络钓鱼攻击类型，载体及其技术途径得报告

1.背景

（1）刊物/会议级别

Expert Systems With Applications CCF C

2018年3月27日

（2）作者团队

Kang Leng Chiew, Kelvin Sheng Chek Yong* , Choon Lin Tan

马来西亚沙捞越大学计算机科学与信息技术学院

（3）论文背景

网络钓鱼始于1995年得美国AOL（America Online）,phishing 是fishing得变体。（网络钓鱼就像是“钓鱼”一样，用“饵料”来获取受害者信息）

定义：网络钓鱼是一种可扩展得欺骗行为，通过假冒自己来获取目标信息

网络钓鱼的两种方式：

- 直接欺骗受害者获取个人信息
- 投递payload，简介获取个人信息

网络钓鱼攻击越来越多，所造成的经济损失也非常巨大。所以了解网络钓鱼攻击的手段对于开发部署反钓鱼技术和系统至关重要。

讨论两种相互关联：（这些关联是每种钓鱼技术的特征）

- 网络钓鱼媒介和载体的关联
- 载体和技术方法的关联

主要内容：

1. 列举了有关当前可用的网络钓鱼方法的文献
2. 根据各自的传播媒介和载体，将网络钓鱼方法分类，并对其具体操作进行说明。
3. 讨论复杂的钓鱼技术的组合形成的更加高级的网络钓鱼攻击

2.主要方法

（1）相关文献

1. Mohammad et al.（2015）将钓鱼策略分为三类：
    - mimicking attack：通过盗用合法账户假冒为工作邮件进行欺诈
    - forward attack（前向攻击）
    - pop-up attack（弹出式攻击）
    - 前向攻击和弹出式攻击涉及使用中间人(MITM)方法，即钓鱼者通过代理网站(前向攻击)或弹出式窗口(弹出式攻击)拦截和检索受害者的个人信息

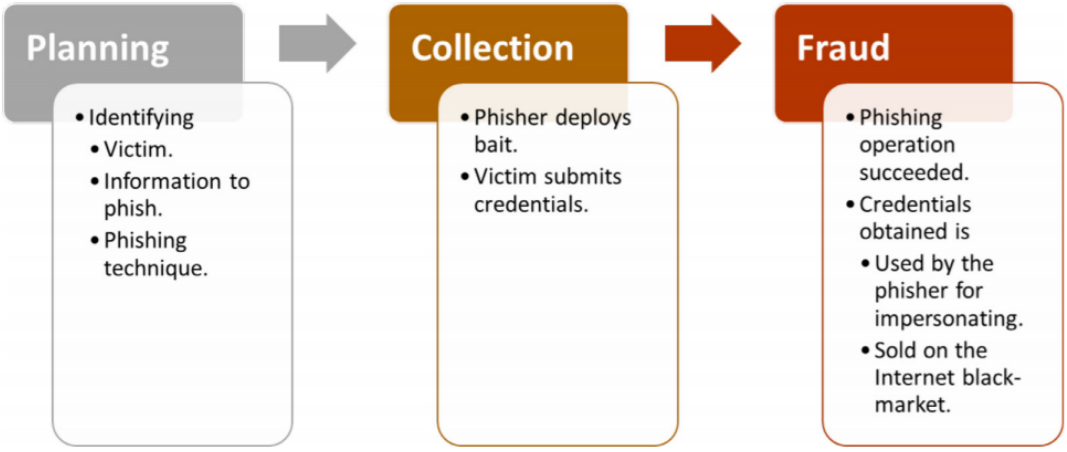


Fig. 1. Lifecycle of a phishing website (Mohammad et al., 2015).

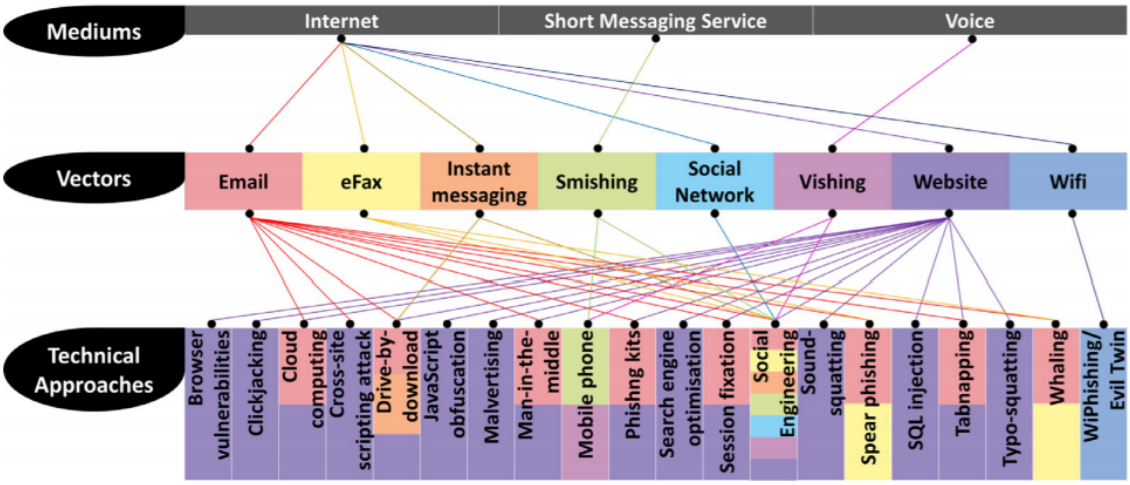
2. Singh（2007）重点研究针对银行部门钓鱼技术进展。相关技术被分为四类：
    - dragnet（网；拖网） method：邮件，网站，弹窗中包含合法组织的logo，合作伙伴名称等诱导受害者进行某些操作
    - rod（棒） and reel（卷轴） method：这种方法包括通过初次接触确定潜在受害者，并利用虚假信息锁定目标，诱导受害者透露他们的个人信息。
    - lobsterpot method："龙虾笼法"是利用一个假冒的网站，欺骗受害者交出他们的个人信息。
    - Gillnet phishing：利用网站或邮件内的恶意代码对受害主机进行感染入侵
3. Rader and Rahman（2013）讨论了现有的和新兴的网络钓鱼攻击载体
4. Sahoo et al.（2017）不局限于网络钓鱼，而是介绍了流行的恶意软件攻击方式。也包含了关于机器学习，特征工程等内容。
5. Patil and Patil（2015）讨论恶意网页中的攻击载体。这些攻击载体不仅限于钓鱼攻击。他们还从文献中讨论了各种恶意网页检测工具，并强调了这些工具中使用的特征和机器学习算法。
6. Almomani et al.（2013）通过电子邮件回顾钓鱼攻击的主题。对网络钓鱼邮件进行了简要概述，重点介绍了网络钓鱼攻击的类型和网络钓鱼邮件的生命周期，以及网络钓鱼邮件的分类和评估方法。详细讨论了网络钓鱼邮件检测中使用的各种特征，并将这些特征分为三类，即基本特征、潜在主题模型特征和动态马尔可夫链特征。随后，进一步讨论了防范网络钓鱼攻击的方法，包括它们的优点和缺点。
7. Ollmann（2004）介绍了网络钓鱼历史，然后详细描述了网络钓鱼威胁的三个方面：
    - 社会工程学因素
    - 网络钓鱼信息的传递机制
    - 网络钓鱼攻击载体

    他还讨论了三个位置的防御机制，即客户端、服务器端和企业级。尽管这篇论文发表于10多年前，但作者所传递的基本信息仍然与当今有关钓鱼攻击的讨论有关。

网络钓鱼攻击最初是通过社会工程学进行欺诈的，伪装成合法账户区欺骗受害者的密码等个人信息。之后网络钓鱼又产生了许多新的更加强大的攻击形式。**相比于网络钓鱼本身的研究，学者们的研究工作更加聚焦在反网络钓鱼方法。然而不彻底详尽地了解网络钓鱼技术，又如何去防范网络钓鱼呢？因此本文作者聚焦于研究网络钓鱼技术本身地特点和类型。**

（2）网络钓鱼组成元素

- 网络钓鱼的媒介：所有的网络钓鱼攻击都需要从受害者到被钓鱼者的互动，而媒介是互动发生的必要条件。钓鱼者可以通过这三种媒介接近他们的潜在受害者:**互联网，语音和短消息服务。**
- 用于传递攻击的载体：
- 攻击过程中的技术方法



（3）网络钓鱼技术途径

【1】浏览器漏洞

利用浏览器漏洞的网络钓鱼通常不容易检测和防御

```
<HTML>
  <BODY>
    <A HREF="http://www.microsoft.com%01@
     phishing.com/as001/mypage.htm">Microsoft
    </A>
  </BODY>
</HTML>
```

【2】点击劫持

“点击劫持”(帕蒂尔,Patil, 2015)，也被称为用户界面(UI)重定向攻击(Akhawe, He, Li, Moazzezi， & Song, 2014)，是对网页UI的操作，导致用户在与受损的UI交互时不知不觉地执行一个动作。

Fig. 4. The UI redressing attack by compromising the pointer integrity.

【3】云计算

云计算是一种在线服务，它包含三种服务模型:软件即服务(SaaS)、平台即服务(PaaS)和基础设施即服务(IaaS)。随着云服务提供商增加更多的服务，云服务的使用正在增加(Weins, 2016)。云服务的安全成为云服务用户关注的第二大问题，仅次于缺乏资源或专业知识(RightScale, 2016)。**由于云服务提供商依赖用户的电子邮件地址作为帐户凭据，钓鱼者可能针对云服务提供商检索用户凭据，并使用这些凭据访问其他帐户使用密码重用攻击**(PhishLabs, 2017)。对云服务的入侵可以通过客户端或提供商发生(Nagunwa, 2014)

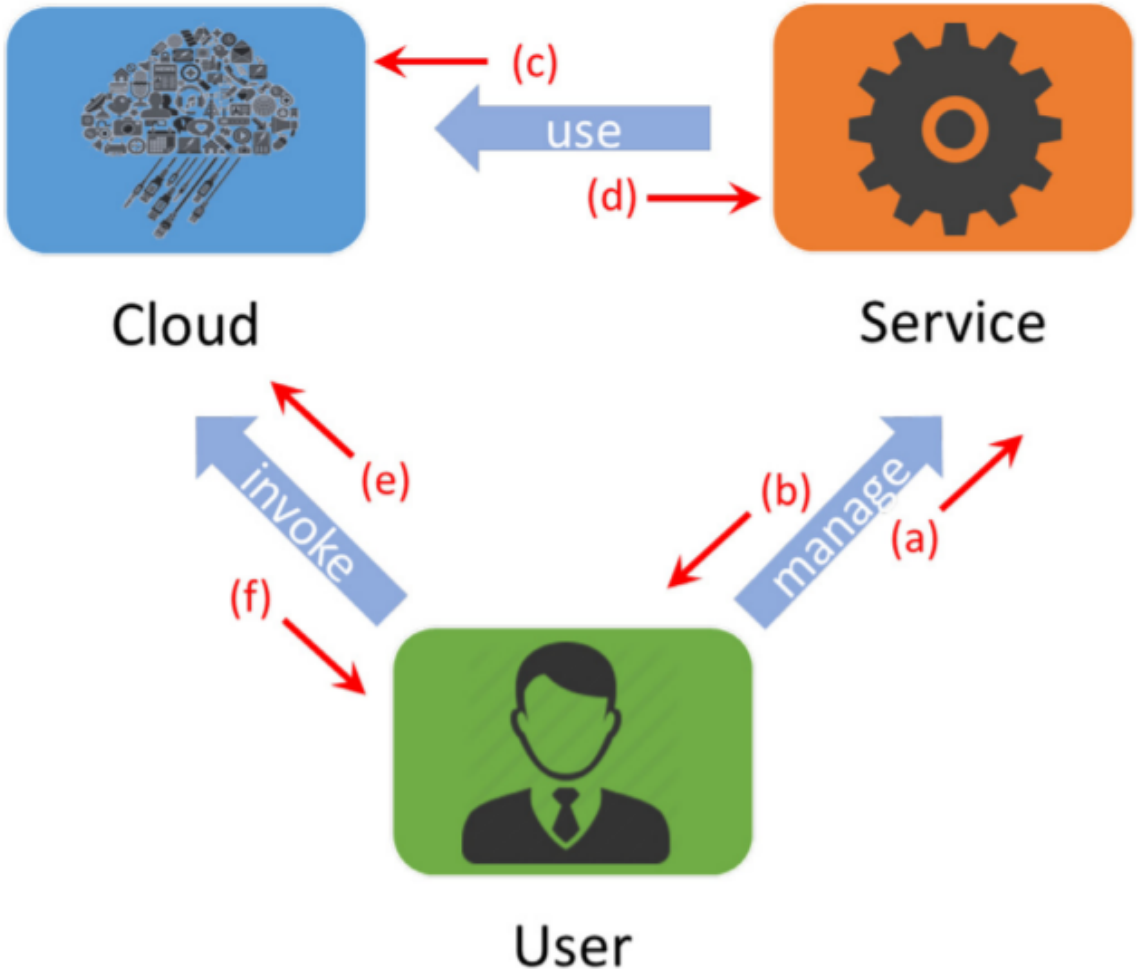


Fig. 6. The relation of the three components in cloud computing, along with the attack surfaces in red (Gruschka & Jensen, 2010). The attack surfaces are (a) service-to-user, (b) user-to-service, (c) cloud-to-service, (d) service-to-cloud, (e) cloud-to-user and (f) user-to-cloud. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

【4】跨站脚本攻击（XSS）

跨站脚本攻击(XSS)是一种利用网站漏洞的漏洞，允许网络钓鱼者向数据字段注入恶意代码或使用自定义URL到网站(DigiCert, 2009;•奥尔,2004)。此类漏洞产生于一个构造糟糕的网站，未能过滤掉外部提供的内容，可能以恶意脚本的形式(Emigh, 2005;雷德,拉赫曼,2013)。XSS攻击是一种规避同源策略(SOP)的方(Ruderman, 2016)。SOP可以防止脚本交互和访问另一个来源的信息。因此，它可以防止恶意网站的脚本在用户访问其他网站时访问个人信息，如登录凭证。

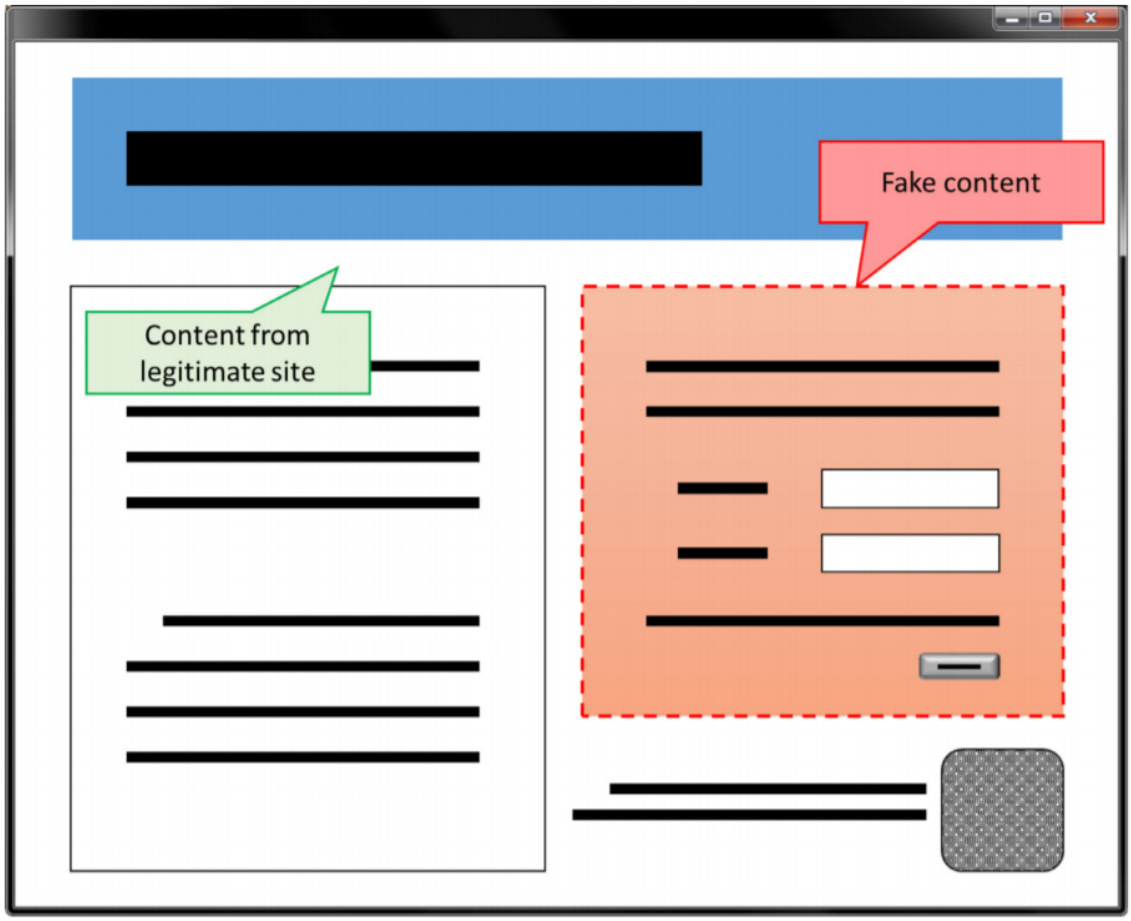


Fig. 7. An example of cross-site script attack on a legitimate website.

【5】Drive-by-download(挂马，路过式下载)

挂马是一种访问一个网站或查看HTML电子邮件就可以把恶意软件，病毒或shellcode注入到目标主机的技术。挂马也可以通过互联网中继聊天(IRC)站点部署(Elledge, 2007)。恶意代码通常是用JavaScript编写的，以攻击浏览器或浏览器插件的漏洞，并驻留在服务器或注入到网站或HTML电子邮件中。

- 特洛伊木马
- 监视软件
- 僵尸网络

【6】嵌入JavaScript

钓鱼者使用JavaScript来掩盖或混淆浏览器窗口的chrome区域。chrome区域包括地址栏、状态栏、工具栏和菜单区，菜单区是内容区周围的区域。使用JavaScript，可以欺骗地址栏或状态栏，使URL看起来合法。此外，钓鱼者还能够欺骗https和锁定图标，使钓鱼网站显示为一个安全的网站。受害者不会意识到，他或她正在访问的网站是一个钓鱼版本的"合法"网站。在地址栏的URL和状态栏的信息的视觉检查将不会标记任何怀疑。这种攻击的形式可以是在钓鱼网站中嵌入JavaScript，受害者访问该网站时执行。也可能是通过一种病毒，在不知情的受害者在地址栏中输入URL后，自动重定向到钓鱼网站，混淆钓鱼网站的真实身份。

【7】恶意广告

恶意广告使用在线广告托管服务作为向受害者分发恶意软件的手段(Nagunwa, 2014)。钓鱼者在广告中嵌入了恶意软件。当受害者点击广告时，一个动态恶意软件将感染受害者的机器，利用机器的漏洞，目的是从受害者那里窃取个人信息。在线广告托管服务的可用性和此类服务的简单申请流程(订阅所需信息最少)使得这种技术对钓鱼者具有吸引力。此外，钓鱼者可以通过合法网站使用广告传播恶意软件，而不需要危害网站。这样，用户在访问广告网站时不会产生怀疑，看到广告是托管在一个合法的网站上。用

户可能不知道广告实际上是由广告网络提供的(Xing et al.， 2015)，也不知道广告内容缺乏验证(Sood & Enbody, 2011)。

【8】中间人攻击(MITM)

在中间人(MITM)攻击中，钓鱼者将自己置于受害者与基于web的应用程序之间的通信中间。

Fig. 11. The Man-in-the-Middle attack.

【9】移动电话

由于移动电话市场的快速发展，透过移动电话进行钓鱼攻击在钓鱼者中越来越受欢迎。随着手机数量的增加，潜在的受害者数量也在增加，钓鱼者可以通过钓鱼者获取他们的个人信息。此外，手机的小屏幕限制了用户界面中可以包含的信息的数量，而且缺少应用程序标识的指示器使得区分恶意应用程序和合法应用程序变得困难。

Felt和Wagner(2011)识别了发生在移动电话中的四种控制转移方式，这些方式可能会被网络钓鱼攻击者利用：

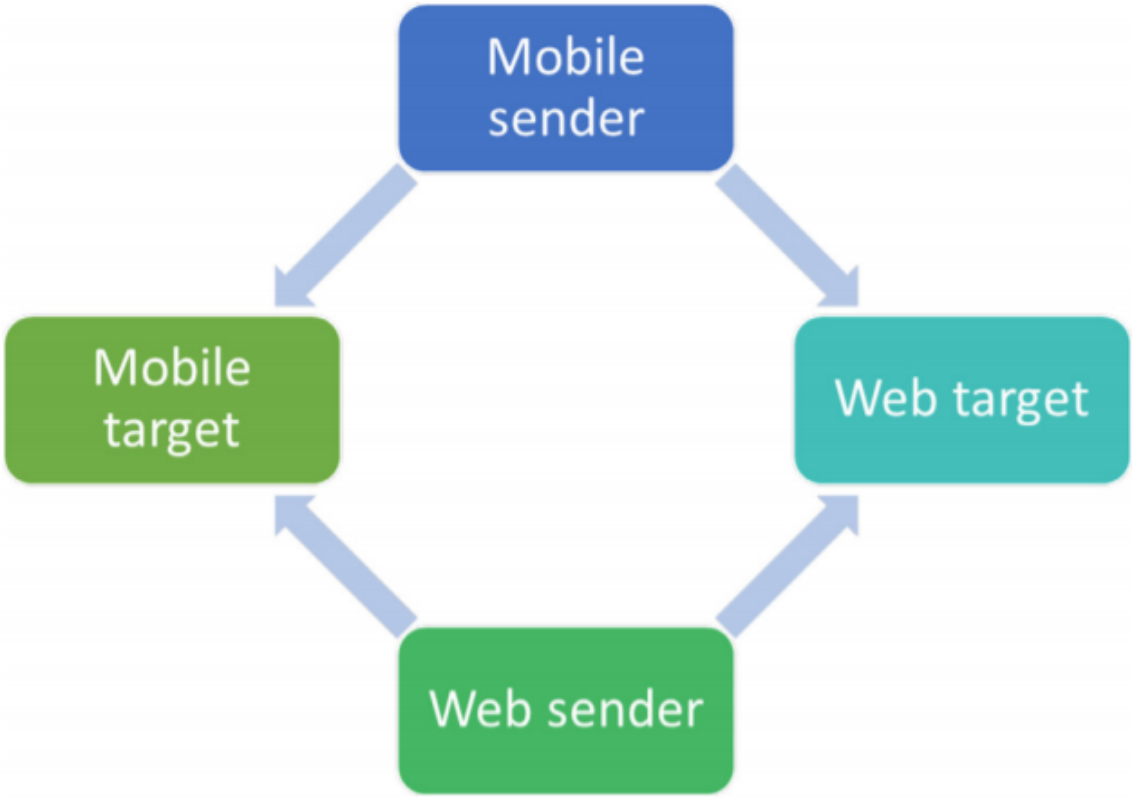


Fig. 16. The four ways of control transfer in a mobile phone.

【10】网络钓鱼工具

钓鱼工具包是使钓鱼者生成钓鱼网站、电子邮件和脚本获取用户输入而不需要任何高级编程技能的工具。这些工具包可以从网络犯罪市场以一定价格(赛门铁克，2016年)获得，也可以由工具包开发人员在地下圈子中免费分发(Cova等人，2010年)。然而，大多数这些免费的钓鱼工具都有后门，会将钓鱼工具用户收集到的个人信息泄露给开发者(Chaudhry等人，2016;Cova等，2010)。网络钓鱼工具在从受害者获取个人信息的网络钓鱼过程中并不起直接作用，但确实有助于部署网络钓鱼攻击。这使得任何具有或不具有编程深度知识的人都可以很容易地发起钓鱼攻击。

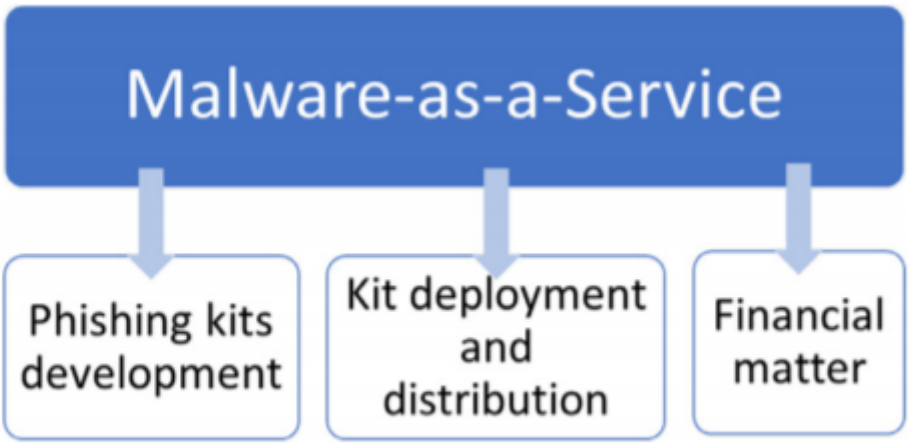


Fig. 17. The components of the Malware-as-a-Service (Moreno, 2016).

【11】搜索引擎优化

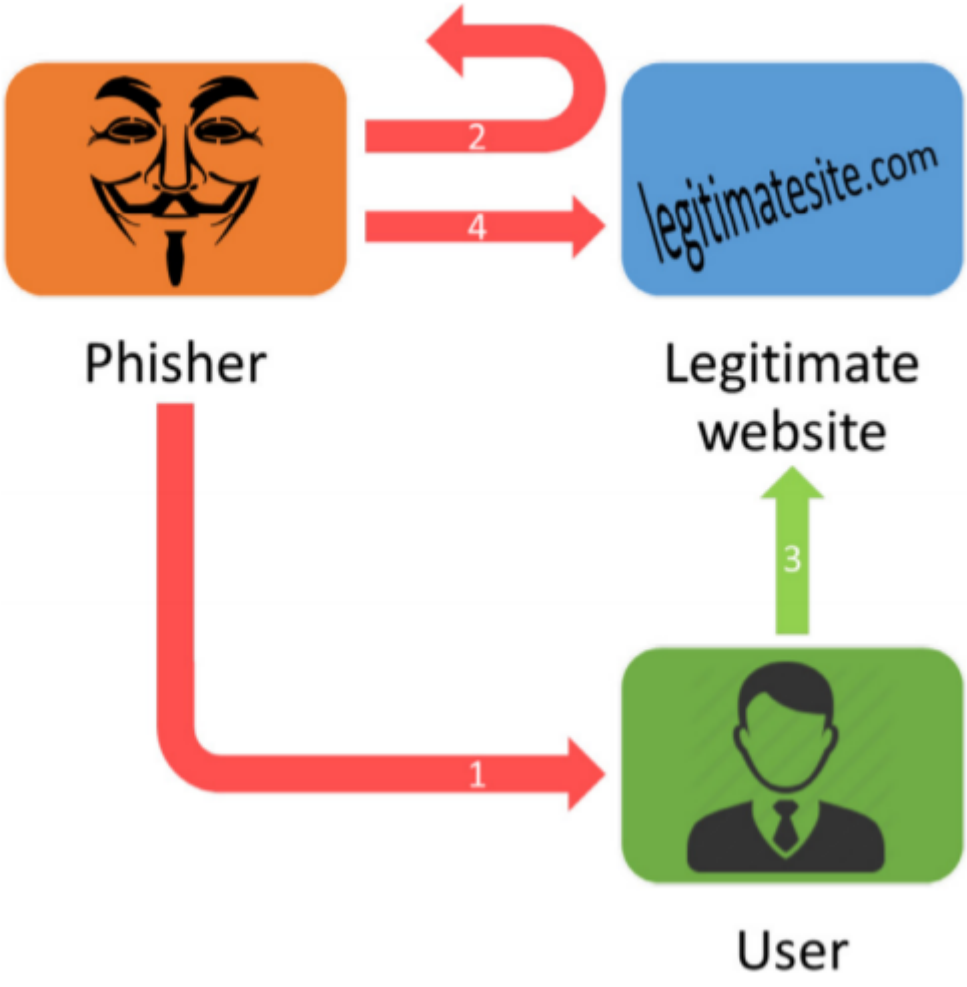
钓鱼网站可透过搜索引擎投递给受害者。**钓鱼者创建了一个钓鱼网站，并优化它为搜索引擎的索引。**潜在的受害者使用搜索引擎搜索某一特定服务或产品供应商的网站时，可能会点击搜索结果中的钓鱼链接，认为该链接将直接指向目标网站。钓鱼者可能会以荒谬的价格提供商品或服务，从而使网络钓鱼攻击更具吸引力和吸引力。Blackhat SEO (Nagunwa, 2014)可能被钓鱼者用来提高钓鱼链接在搜索引擎结果中的页面排名。这是通过在他们的网站中注入流行趋势或事件的关键字来实现的，以确保他们的网站排名作为一个顶级搜索结果。这将进一步增加潜在受害者点击链接的可能性。

【12】Session fixation（Session完成攻击）

对于无状态协议，如HTTP和HTTPS，客户端和服务器之间的通信会话不会被保留，一旦数据传输完成，连接就会丢失。这对正在访问他或她的帐户的用户形成了一个问题，这种协议将不会保持用户当前所在的活动会话。例如，当用户登录到购物网站并浏览商品时，服务器需要有一种方法来维护用户的会话并跟踪他或她的活动，例如将商品添加到购物车中并在稍后结账。

实现这一目的的常用方法是使用会话标识符(sid)。当用户通过身份验证并登录到网站后，一个名为SID的唯一密钥被分配给网站内的用户会话。当用户浏览多个网页并在网站中执行某些操作时，此键将识别用户所处的会话。这个SID可以以cookie、表单字段或URL的形式存储。

钓鱼者能够瞄准状态较差的管理系统中的SID漏洞，并执行会话劫持攻击。这种技术称为会话固定或当前会话攻击(Ollmann, 2004)。这种技术要求用户使用钓鱼者指定的SID对会话进行身份验证，钓鱼者然后能够劫持该会话，以代表用户执行某些操作。



【13】社会工程学

社会工程包括钓鱼者利用受害者的信任、同情或恐惧等情感、帮助意愿和轻信来达到他们的目的(Mitnick &西蒙,2002)。社会工程的基础是使受害者不再做出理性的选择，而导致受害者做出情绪化的选择(Goel, Williams， &Dincelli, 2017)。这些情感的例子包括恐惧、贪婪、好奇、愤怒、友谊、爱国主义、虚荣、利他主义、社区归属感、责任感和权威感。通过操纵和利用受害者的情绪，例如灌输失去有价值的东西的恐惧，受害者会做出非理性的行为，例如向骗子透露他或她的个人信息(Kim &金正日,2013)。这种行为源于人的保护天性，即立即采取预防性行动(Leventhal, 1970)。例如，一个骗子可能会联系他或她的受害者，询问一个可能导致服务中断或帐户暂停的账单问题，需要立即采取行动来解决这个问题。受害者采取的行动将涉及受害者向钓鱼者透露他或她的个人信息。

【14】Sound-squatting

Sound-squatting是一种域名抢注技术，钓鱼者通过注册听起来类似于合法网站的域名来使用。这种发音相似的词叫做同音词。例如air和heir, ascent和assent, base和bass。钓鱼者也可能使用一个数字的单词或数字作为同音词。例如www.highfive.com和www.high5。com。钓鱼者利用用户对同音异义词的混淆和输入错误的单词，但在键入URL时却拥有相同的发音。然后用户会被引导到合法网站的钓鱼版本。钓鱼者可以注册几个与合法域名同音的域名。

【15】鱼叉式网络钓鱼

鱼叉式网络钓鱼是针对个人、团体或组织的定向攻击。鱼叉式网络钓鱼已经成为网络钓鱼者的流行选择(Nagunwa, 2014)，而非传统的网络钓鱼使用大量和随机的电子邮件网络钓鱼。这是因为与传统方法相比，这种方法成功率高(Krombholz et al.， 2015)。鱼叉式网络钓鱼使用特别制作的电子邮件，模仿受害者认识的发送者。电子邮件的内容是与受害者相关的，不会引发任何来自受害者的怀疑。

【16】SQL 注入

结构化查询语言(Structured Query Language, SQL)注入技术是利用数据库中的漏洞，这些漏洞没有正确执行过滤，允许注入和执行数据库命令，从而导致信息泄漏(Emigh, 2005)。这是通过将SQL命令注入SQL语句或通过网页输入查询来改变语句的原始意图来实现的。注入的代码通过用户输入变量与SQL命令连接，然后执行这个动态SQL命令。可以通过利用当前SQL查询或通过多个查询添加新查询来利用此漏洞。

【17】Tabnapping

Tabnapping(苏瑞，托马，&2010年，火狐的创意总监阿扎·拉斯金(Aza Raskin)首次推出。tabnapping这个名字是由Tab(标签)和Kidnapping(绑架)组成的混合词，用来描述在浏览器中劫持标签的攻击形式。这种攻击的操作如图19所示。首先，钓鱼者将钓鱼网站的链接通过电子邮件发送给用户。一旦用户点击该链接，用户浏览器中的一个选项卡将打开，加载钓鱼网站，看起来像一个普通的网站。钓鱼网站内嵌的JavaScript会监控用户的浏览活动。一旦用户导航到浏览器中的其他标签，离开标签与钓鱼网站脱离焦点，标签加载钓鱼登录屏幕，更改favicon和标签的标题来欺骗一个合法的网站，如Gmail。当用户浏览打开的标签页时，注意到钓鱼登录屏幕，用户可能会认为该网站的登录会话已经过期，需要重新登录。因此，用户通过钓鱼登录屏幕提交登录凭证，而不知道这是一个钓鱼网站。Aza Raskin在他的网站上展示了这种攻击(Raskin, 2010)。phisher使用这种技术是因为用户对之前打开的选项卡不那么怀疑，并且不知道之前加载的内容可以使用JavaScript更改，而不是像用户假设的那样保持静态。只有当用户在浏览器中打开多个选项卡时，这种攻击才会成功，并且很容易丢失所有打开的未激活选项卡的内容

【18】Typo-squatting

一种域名抢注技术，钓鱼者通过注册合法域名的拼写错误的域名。有五种可能的域名输入错误，可能是用户意外执行的，它们在表3中给出。这种攻击会影响在地址栏中手动输入URL的用户。当用户文件的URL不小心按相邻键或失踪一个字符,输入错误的URL可能直接用户网络钓鱼网站,可能看起来像合法网站用户试图访问或一个网站,加载一个恶意软件到用户的主机。

Table 3
Examples of domain name typos (Wang et al., 2006) in the URL: www.mybank2us.com.

Typo type	URL
Missing dot typos	wwwmybank2us.com
Character omission typos	www.mybankus.com
Character permutation typos	www.mybank2su.com
Character replacement typos	www.mybanl2us.com
Character insertion typos	www.mybank2uss.com

【19】Whaling（捕鲸）

Whaling（捕鲸）与鱼叉式网络钓鱼在某种意义上是相似的，因为它是一种有针对性的攻击，但目标是由高层管理人员组成(Ollmann, 2004)，他们在一个组织内拥有获取信息或资源的高度特权。捕鲸是通过恶意软件完成的，这些恶意软件给钓鱼者后门进入该组织的系统或部署键盘记录程序。由于这是一种有针对性的攻击，钓鱼者将花费更多的时间通过电子邮件或电子传真来设计他或她的攻击载体，以增加受害者点击链接或下载含有恶意软件的附件的成功机会。捕鲸被用作一种先发制人的攻击，进一步的恶意攻击称为商业电子邮件泄漏(BEM)(联邦调查局，2017)。这封泄露的电子邮件来自CEO等高层管理人员，被用来指示CEO的下属进行未经授权的电汇支付。

【20】Wiphishing/evil twin

一种使用无线网络的网络钓鱼技术。钓鱼者使用如图20所示的非法AP，将自己置于互联网用户和合法无线接入点(AP)之间。首先，钓鱼者会部署一个非法AP，该AP具有相同的服务集标识符(SSID)或网络名，以及某个区域内现有合法AP的无线电频率。有软件可以使笔记本电脑成为无线网络的接入点(truesofsoftware, 2017)。然后,网络钓鱼将这流氓美联社接近用户可能导致用户连接到AP最强的信号或有计算机自动连接到流氓美联社它选择美联社与一群APs的最强的信号相同的名称。最后，钓鱼者能够窃听用户提交和通过用户机器连接的非法AP接收的信息。钓鱼者通常会将目标锁定在有免费热点的公共场所，如咖啡馆、机场、酒店等(Song et al.， 2010)。

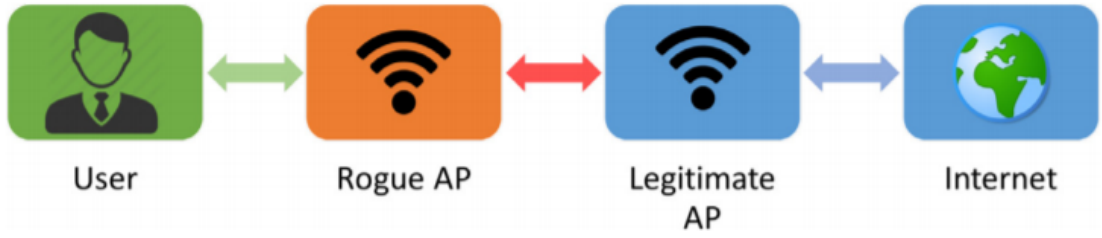


Fig. 20. The WiPhishing/Evil Twins attack.