白皮书：反网络钓鱼最佳实践思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/590/2021_2022__E7_99_BD_E7_9A_AE_E4_B9_A6_EF_c101_590360.htm 目前，每个月都会上演成千上万次目标锁定于全球金融机构的网络钓鱼攻击，对金融机构而言，采取具有前摄性的措施，保护自己及客户免受网络钓鱼和其他高级威胁的攻击是非常重要的。一个组织减少网络钓鱼所造成的影响，保护其自身品牌、客户和资产的唯一最有效的方法就是关停具有欺诈性的网站。尽管另外也有其他的保护机制，并且应该被加以利用，但是屏蔽网络钓鱼网站就可以很简单地阻止攻击的发生。这可以确保受网络钓鱼邮件欺骗而点击进入具有欺诈性的网站的消费者真正受到欺诈的人数达到最少。 然后就出现了这样的问题：关停具有欺诈性网站的最有效的方法是什么?本白皮书确立了几个最佳实践，金融机构(或面临网络钓鱼攻击的任何组织)可以通过这些实践有效地屏蔽具有欺诈性的网站，并在对抗网络钓鱼的时候探索创建有效的指挥中心的重要性。 创建有效的指挥中心的重要性 对抗网络钓鱼的方法有很多。最适合的方法会同时把几种措施、技术和服务结合在一起，以便于尽快减轻网络钓鱼的攻击。不管一个金融机构是选择利用自己的资源开展反网络钓鱼的措施，还是选择一种外包服务，对抗网络钓鱼都是一个需要网络钓鱼和在线金融欺诈领域的专家意见的过程。 在行业内，对抗网络钓鱼的最普遍的方法包括创建或合伙成立一个指挥中心，用于处理从初始探测到最终被关停的攻击。有人可能认为，创建一个指挥中心是非常简单的，主要是有关物流和资源的事情，但是，对抗网络钓

鱼的本质是速度和效率一个缺乏经验的指挥中心和一个有效率的指挥中心之间的区别，可以很容易地通过一次攻击所造成的受害者的数量和损失的金额来体现。 因此，在创建指挥中心或寻求已经存在的指挥中心来关停网络钓鱼站点时，最为关键的是要把指挥中心的经验和追踪记录作为考虑要素。可以通过简单地对指挥中心进行测试来验证它的效率。指挥中心检测到攻击的速度有多快?指挥中心如何关停正在进行的网络钓鱼攻击?在分析攻击的时候，指挥中心揭示了多少受连累的信息和情报? 需要考虑的其他事情包括该中心已经有效抵御的攻击的数量，网络钓鱼攻击处理流程的有效性，以及该中心所支持的机构的数量。同样重要的还有指挥中心具体的反欺诈经验。既然网络钓鱼只是在线欺诈的一种类型，因此在处理网络钓鱼的时候，经验和金融服务的专业知识，以及反欺诈措施是极为重要的。一个有效的指挥中心应该由富有经验的欺诈分析员构成，他们要接受关于新的诈骗技术和金融欺诈方法的广泛培训和不断进行的教育。 指挥中心被创建和运行起来之后，可以i采用几种最佳实践惯例来确保其运行的有效性。 典型攻击的流程 对抗网络钓鱼攻击是一种耗费时间的资源密集型过程，包括取得成功所需要的各种技术和工具。如上描述，在对抗网络钓鱼攻击的时候，首要的建议是建立一个指挥中心或使用一个现有的指挥中心。 在关停网络钓鱼攻击的过程中，可以采取多个步骤。需要采取的第一个步骤是检测除非你知道攻击正在发生，否则你不可能关停它。越早发现攻击，你就可以越快地去屏蔽它。检测网络钓鱼攻击最有效的方式是利用多种来源。例如，可以与每天扫描大量电子邮件的反垃圾邮件提供商合作，也可以让用户报告

他们收到的可疑网络钓鱼邮件。 一旦识别出一次攻击，接下来要采取的步骤就是关停具有欺诈性网站的过程。这通常是通过联系网站所在的虚拟主机提供商来完成。关停过程要使用好几种工具，并分为几个步骤，包括：确定相关的虚拟主机提供商，找到正确的联系信息和正确的联系人，使用正确的语言有条理地解释事情的来龙去脉，并寄送要求关停具有欺诈性网站的合法的停止和终止表。尽管这听起来很简单，但是，获取虚拟主机组织的信任关系对于关停的速度和成功至关重要，而这种信任关系只有通过一定的时间才能建立起来。在钓鱼网站离线后，还要对其进行不断地监控，以确保它不会卷土重来。 屏蔽网络钓鱼站点的最佳实践 接下来是有助于创建指挥中心和快速检测及关停具有欺诈性网站的其他几种最佳实践惯例。这些建议来源于RSA的防欺诈指挥中心(AFCC)所获得的经验。防欺诈指挥中心是一个24x7的全天候“ 作战室 ”，为全世界200多个组织检测、监控、跟踪和关停网络钓鱼、网址嫁接欺骗和特洛伊木马攻击。由 40多位经过训练的欺诈分析员组成的防欺诈指挥中心，迄今为止已经关停了40，000多次攻击，并且是关于网络钓鱼和新兴在线威胁的信息的主要行业来源。 1. 建立全球经营 网络钓鱼网站存活的时间越长，金融机构的客户泄露他们的个人信息和受到其诈的风险越大。时间是关键一个指挥中心必须提前为攻击和实际关停做好尽可能充足的准备。它还必须拥有在全球水平上应对网络钓鱼攻击的资源和专家。例如，由于网络钓鱼是一种全球现象，全世界130多个国家已经遭受过攻击，所以一个指挥中心必须拥有多种语言能力。这可以通过雇佣具有多种语言能力的欺诈分析员或提前翻译用于网站关停的文件

来实现。如果指挥中心处理网络钓鱼攻击、网址嫁接欺骗攻击和品牌滥用攻击，并提交了停止和终止文件作为关停流程的一部分，然后，它还应该为每一种类型的攻击准备好文件，并翻译成相关的语言，以便于在关停流程启动时，欺诈分析员可以获得相关信息。 另一种提前准备和实现全球覆盖的工具是一个立即响应翻译公司，直接在与世界各地的虚拟主机提供商的电话中现场翻译。寻找可以掌握150种语言的欺诈分析员是不现实的，但是，让分析员联系一个实时的翻译公司，并与世界上任何地方的虚拟主机提供商召开电话会议则是切实可行的。 一个指挥中心应该拥有所有事先准备好的标准的沟通信息，像电话脚本和电子邮件模板欺诈分析员不应该在每一次遇到一个新的虚拟主机提供商时都从头开始重新打一遍关于网络钓鱼的界定。简而言之，事先所做的准备越多，欺诈分析员的分析过程就越简单，网站被关停的速度越快。 2. 使用24x7全天候威胁反应 当关停网络钓鱼攻击时，随时保持警惕是非常关键的。网络钓鱼关停服务必须是24x7全天候运行的。欺诈者推出网络钓鱼的目的是获得金钱。他们会寻找他们所能找到的一切脆弱之处，包括在人们最没有想到的时候发起攻击。例如，有人可能会在营业时间之后或在周末发现汹涌而来的网络钓鱼攻击，而这时候金融机构和服务器主机提供商要么不上班，要么人员不足。这会导致关停流程变慢，从而扩大了欺诈者的“ 机会之窗 ”。此外，在某一个国家的法定节假日期间，业务都在缓慢进行的时候，发生在这个国家的攻击通常会增多。建立一个24x7全天候的指挥中心可以降低发生攻击的风险，并减少攻击所造成的损害。 3. 与服务器主机所在地联系，建立并保持关系 当网络钓鱼

在2003年首次出现在国际互联网上的时候，关停一个网站即使不需要几周，也需要几天的时间。由于不了解问题，服务器主机提供商在被要求关停一个欺诈性网站的时候，会有所怀疑和犹豫。毕竟，一个提供网站服务的ISP要保护自己的声誉，不能因为一时兴起就简单地拆除其顾客的网站。如今，随着发生范围的普及和全世界对网络钓鱼的危害性的认识越来越高，与虚拟主机提供商的沟通变得更容易了。因此，一个已经与虚拟主机提供商建立了关系的指挥中心在迅速关停网站的过程中更具优势，更容易成功。 网络钓鱼攻击虚拟主机提供商有很多类型从ISP开始，到免费的和商业化的网络虚拟主机公司，注册商和国家互联网电子邮件提供商，像MSN Hotmail 和 Yahoo!。在试图关停网络钓鱼网站时，熟悉国际互联网的运转和错综复杂是非常重要的，这样才能了解网站位于哪里，并在关停的过程中联系正确的实体。 关停具有欺诈性的网站不是一门精确的科学，因此，从经验中学习，并将所学东西记入日志信息是至关重要的。例如，只要虚拟主机提供商符合他们的需求，欺诈者就会一次又一次地使用同一个虚拟主机提供商，因此，指挥中心的欺诈分析员一旦找到了虚拟主机提供商的正确的联系人，并成功地关停了在这家虚拟主机上寄存的网站，那么他们就应该保留所有的联系信息和任何在将来与这家虚拟主机提供商打交道的其他窍门。一个关于虚拟主机提供商信息和有用小窍门的大型数据库，可以大大缩短在后来的攻击中关停一个网站所花费的时间。随着指挥中心越来越有经验，当他们与一家熟悉的虚拟主机提供商打交道的时候，他们可以实现非常高的成功比率，在几分钟或几小时内关停一个网站。理想的情形是，拥有在特

定虚拟主机提供商工作的最相关之人的电话和电子邮箱地址，简单地发送一个关于具有欺诈性的URL的快速请求，然后这个网站就会被立即屏蔽。 保持与不同的虚拟主机提供商之间建立起来的关系也非常重要。毫无疑问，如果在虚拟主机提供商中有一个熟悉指挥中心，并认可其专家地位和专门知识的团队，此提供商将会更合作，更有帮助，从而能提高关停的成功比率。 与处理计算机安全和在线欺诈的各种法律执行机构和计算机安全事故反应团队(CSIRT)建立联系并维持关系也至关重要。这是对抗一般的在线欺诈的最佳实践惯例，不过对于关停网站也非常有用。在有些国家，当由法律执行部门或联邦机构提出屏蔽具有欺诈性的网站的请求的时候，虚拟主机提供商一般都更加合作。因此，一个拥有这些关系的指挥中心在关停位于遥远的国家的网站时将更加省事，也更容易成功。 4. 关注新的攻击和欺诈技术建立不断前进的专家团队 在创建一个指挥中心和关停网络钓鱼网站的一开始，寻找并利用富有才能和经验的欺诈分析员非常重要。尽管这看起来像是一项简单的任务，只需要坚持和良好的沟通技能，但是，经营一个指挥中心还需要最开始的专家经验，以及不断进行的培训、教育和情报收集。 欺诈分析员的重要背景信息和特征包括：计算机科学和计算机工程学领域的教育，国际互联网(连网、基础设施、TCP/IP协议、软件和硬件选择)的技术环境方面的广泛经验，以及提供技术支持的经验。如果每位欺诈分析员都是双语的，也会非常有帮助。在正确的分析员团队确立之后，对他们进行广泛的培训和不断的教育将保证指挥中心保持效率。 网络钓鱼和在线欺诈是不断演进的。欺诈者每天都变得越来越复杂，通过在线欺诈者论坛

和社区进行大量的信息分享。对于一个指挥中心而言，必须关注不断发展的欺诈和网络钓鱼趋势，检测它们的变化并缩短攻击的存在时间。开展与时俱进的教育研讨会和每两周一次的会议上，让团队成员共享信息和“ 战斗故事 ”，监控欺诈者社区和对网络钓鱼攻击及它们的基础结构的最新分析，都可以帮助保证欺诈分析员不断地更新知识和有效地工作。
5. 同步工作 在对抗在线欺诈的时候，会存在许多难题从攻击的探测，到分析、关停、通过ISPs和反垃圾邮件合作商屏蔽、用于收集资料和受连累信息的先进的取证，还有更多。最有效的防网络钓鱼服务会利用尽可能多的技术和方法。尽管有如此多的最佳实践惯例，但有时候还是会花费几个小时，甚至几天的时间才能关停一个网络钓鱼网站。同时，还应该同时做一些其他的事情来减轻攻击所造成的危害。 一个可以在网站关停过程中同步实施的关于网络钓鱼防范措施的范例是网站屏蔽。通过与ISPs和反垃圾邮件提供商合作，指挥中心可以把具有欺诈性的URLs提供给屏蔽合作伙伴，他们会反过来阻滞客户访问网络钓鱼网站。换句话说，如果一个指挥中心把一个网络钓鱼网站提供给主要的ISP，然后使用那个ISPs互联网浏览器的所有成员都将不能访问网络钓鱼网站。即使他们之前点击过网络钓鱼邮件中的链接，他们也将收到一条信息，告知他们该网站已被屏蔽，因为它会引导你到包含恶意信息的网络钓鱼网站。在指挥中心努力地完全关停网站期间，这种屏蔽过程可以保护许多用户免受危害。 