年度热点威胁报告

2019年策略及工具回顾

CISCO

目录

2019年网络威胁目标及工具分析

有些网络犯罪分子在制定攻击计划时，会以特定的组织为目标。不管出于哪种原因，他们都很清楚两件事：攻击目标和潜在回报。一旦明确了攻击目标，几乎没有什么能阻拦他们。看看今年全球发生的定向勒索攻击事件就能发现，这些攻击之所以能够造成极具破坏性的结果，部分原因便在于这些组织由于防护不足，极易成为恶意攻击者专门选取的攻击对象。

而其他网络犯罪分子则更像是沉迷于一场数字游戏。他们不管被攻击的对象是组织还是个人，只是希望尽可能扩大被攻击者的数量，前提是他们能够获得他们想要的最终结果。

例如，在今年首次出现的 DNS 劫持事件中，恶意攻击者正是通过控制部分特定的 DNS 条目来发动攻击。恶意攻击者通过这种方式，能够悄无声息地将无防备的访问者从合法系统重定向到恶意系统，以期对方安装恶意软件或拦截保密资料及凭证。

从远程访问木马到将藏匿在加密流量中的威胁，恶意攻击者为规避先进的检测技术也在不断更新着自己的威胁方案。

本文旨在带您了解我们在过去一年内所开展的调研工作，以及我们最关注的六种主要威胁。请浏览我们在“每月热点威胁”博客上发布的更为深入的分析性文章，并注册订阅，随时了解有关2020年威胁发展趋势的最新信息。

如果您在未来几个月内组织任何以安全为主题的董事会会议或业务规划会议，本报告结尾处给出的建议可作为回顾性资料，针对您需要用到的工具和流程给予指导。它可以帮助您更好地阐明当前的安全防御机制是如何应对恶意攻击的，并找出相应的安全漏洞，比如了解遇到上述六种威胁时的响应速度？获知威胁的及时性？以及加快响应速度的必要措施。

1. DNS 劫持

DNS，全称域名系统（Domain Name System），用于将人类可读的域名（例如 www.example.com）转换成机器可读的 IP 地址（用点隔开的若干位数字，例如 208.67.222.222）。使用 DNS 的过程与图书管理员帮您找书的过程非常类似；您首先输入一个文本名称，然后由 DNS “图书管理员”将其转换为一个 IP 地址，再在书架上搜索相应的 IP 地址，而后带您返回至要查找的目标网站。

威胁场景

上午9点，您准时登录公司网络，边喝咖啡边浏览行业新闻。您打开浏览器，单击书签，想要打开您收藏的新闻网站。

只可惜这次您打开的网站并非是您最近一次访问过的网站。

思科的威胁情报研究团队 Cisco Talos 一直密切关注 DNS，而且我们在今年也发现了多起利用 DNS 劫持发起的恶意攻击。

然而 DNS 攻击的关键在于，它们不会直接面向指定目标（坐在办公桌旁的您）发动攻击，而是将图书管理员作为攻击对象（在本场景中即您想要边喝咖啡边浏览行业新闻的网站）。图书管理员没有将您带到目标书籍的正确存放位置，而是把您带去一个完全不同的地方。最糟糕的一点在于，您可能根本不知道自己去到了一个错误的位置。您打开的钓鱼网站，或者是您从书架上取下的书，看上去跟您想要寻找的目标非常类似，但实际上却大相径庭-比如您本来要找的是一本儿童读物，实际拿到的却是《无政府主义者的烹饪手册》。

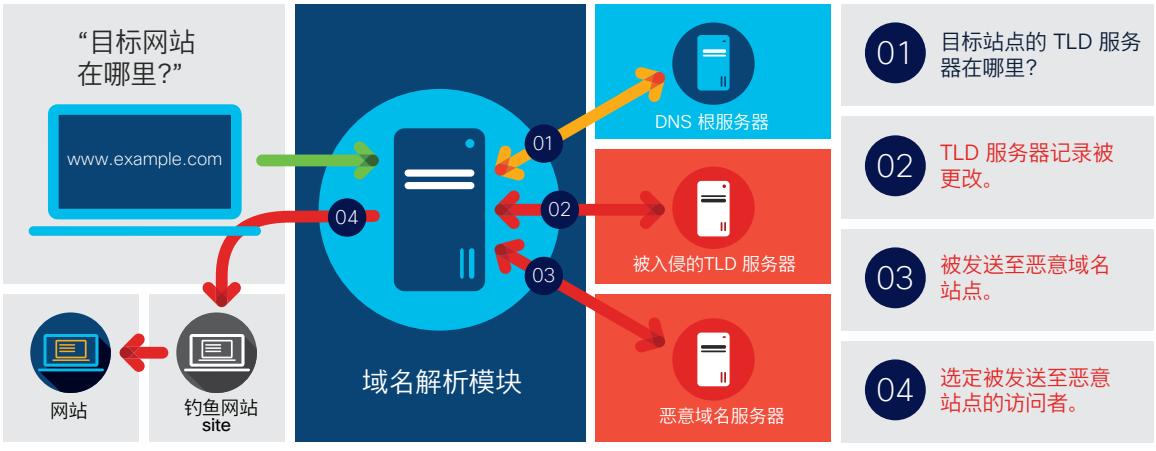
整个攻击过程通过网络犯罪分子将指向合法网站的路径更改至恶意网站而实现。虽然您输入的是计划访问的指定域名的IP地址，但是由于 DNS 记录被篡改，所以您打开的实际是一个恶意IP地址。当您在毫无防备的情况下抵达恶意服务器后，便会马上成为任由恶意攻击者摆布的受害者。恶意攻击者可能会尝试安装恶意软件，收集您的用户名和密码，或者隐蔽地充当恶意站点和合法站点之间的中间人，并拦截您出于其他目的（即身份盗用、勒索...）而访问的所有数据。

“海龟”开始肆虐网络

Sea Turtle（“海龟”）便是由控制 TLD（顶级域）的组织发起的一种DNS劫持案例。案例中的恶意攻击者正是利用多个系统漏洞控制了整个域的域名服务器。

这样一来，恶意攻击者便能对根据 DNS 请求返回的 IP 地址施加控制。它在完成一台恶意域名服务器的设置后，就能选择何时将针对特定域名的请求发送至合法站点或恶意站点。

图 1　Sea Turtle（“海龟”）攻击流程图



除此之外，网页邮件服务器的 DNS 记录也已被更改，这也属于 Sea Turtle 攻击的一部分。恶意攻击者由此便可以拦截用户登录网页邮件系统的连接，这样一来，他们不仅可以捕获用户凭证，还可读取网页邮件系统和用户之间所传递的所有数据。

DNS 劫持是一种非直接攻击案例，对隐藏在幕后的恶意攻击者来说，他们的真正目标并非某个特定的组织，而是整个互联网的基础设施。

在报告结尾，我们虽然就如何应对 Sea Turtle 之类的网络攻击进行了讲解，但首先还是需要考虑通过一些特定的技术来防止 DNS 被盗用，例如通过监视被动 DNS 数据以及寻找域名记录更改数据来判断是否存在DNS被恶意篡改的情况。

2020年态势分析

今年，“海龟” DNS劫 持行动的幕后黑手并没有放慢脚步。Talos 团队发现的一些新细节也暗示出这些恶意攻击者在我们发布有关 Sea Turtle 的初步发现后已经重整旗鼓，并且针对新的基础设施方面发动了更为强烈的攻击。许多恶意攻击者在被发现之后便会暂时放慢攻击的步伐，但是这个团体却异常明目张胆。针对这种情况，我们建议重点关注 DNS 安全技术和多因素身份验证技术，以落实更为严格的身份认证流程。

阅读有关 DNS 劫持的更多内容。

來源: https://blog.talosintelligence.com/2019/04/seaturtle.html

特别关注:
定向勒索病毒

今年，全球发生了许多起备受瞩目的定向勒索软件攻击事件。当然，勒索软件早已屡见不鲜，但我们所关注的地方在于，伴随着新的攻击形式层出不穷，旧的攻击手段也绝不会销声匿迹。我们通过下述几个勒索软件攻击案例就能看出，这些恶意攻击活动一旦成功，所产生的破坏性结果将有多么严重，尤其是在关键服务被中止时。

今年5月，美国巴尔的摩市遭受了大规模勒索软件攻击，市政府大楼中有7,000名用户均收到了严重影响。尽管政府拒绝支付赎金，但在借助多种全手动操作系统，并开展多次数据丢失调查之后，该事件最终约给全市造成超过1000万美元的损失。

第二个案例同样发生在美国，犹他州的莱克城和佛罗里达州的里维埃拉海滩，也遭受了类似的勒索软件攻击，但这两场攻击最终以支付黑客总计100万美元比特币告终。目前，这两个城市仍然面临着解密被盗数据这项艰巨任务。

再看英国，一家名为 Eurofins Scientific 的公司遭受了定向勒索软件发起的大规模攻击，而这家公司也是为全国警队提供法医服务的公司。这家公司每年处理的刑事案件数量超过70,000宗，但在遭受如此大规模的网络攻击之后，许多诉讼案件被迫休庭，与此同时警队也不得不寻求其他供应商提供服务。

请阅读有关定向勒索软件的更多信息，包括 Talos 团队关于如何应对勒索需求的论述。

2.远程访问木马 (RATs)

攻击场景

您目前就职于一家知名的科技公司，公司即将面向公众发布一款能够灵活应对市场变化的全新产品。您希望在产品公开发布之前严守相关机密信息。但遗憾的是，您准备已久的惊喜就要被泡汤。

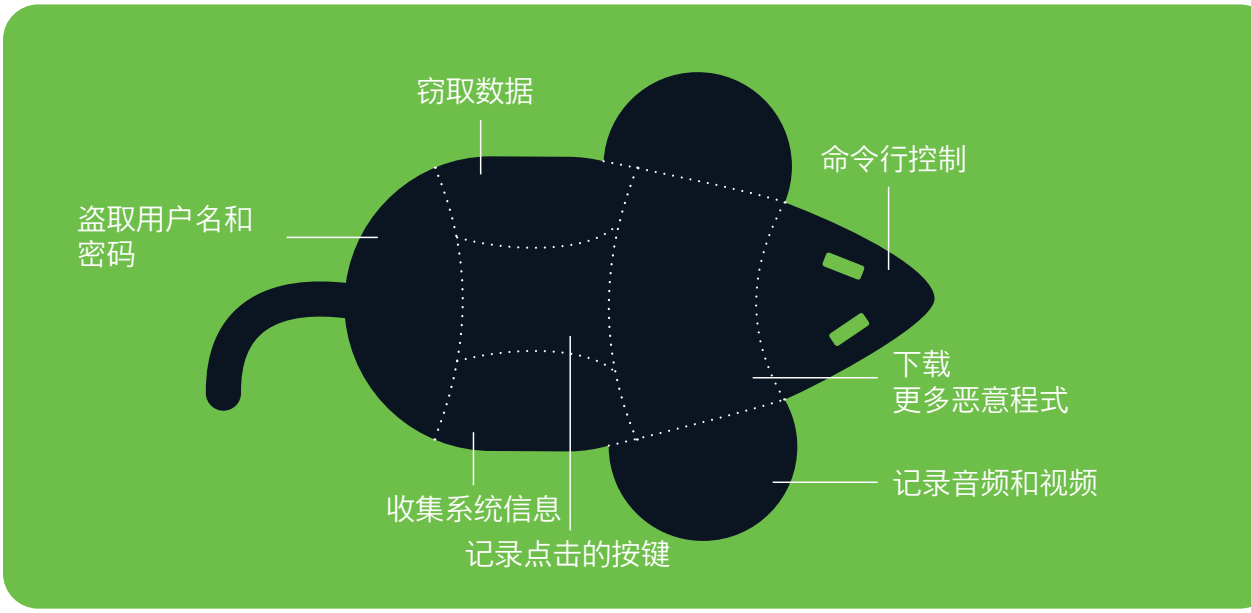
有人入侵了您公司的系统，并盗取了与这款即将上市的关键产品相关的敏感数据。

可被恶意攻击者用来盗取知识产权数据的有力武器可能有很多种。下载程式、管理工具以及资讯盗窃程式很多时候都是催生此类攻击的重要原因。但在类似上述攻击场景中，恶意攻击者通常会在一种简称为“RAT”的远端控制木马程式的协助下发起攻击。

如何借助RAT发动恶意攻击

身为一种工具，RAT 所具备的功能可谓丰富至极。举个例子，如果恶意攻击者的目标是窃取财务数据，那么他们可以借助一个RAT，通过一台被入侵的计算机获取银行信息，或者通过安装键盘记录程式来收集信用卡账号。

图 2　RAT 程式的组成部分



许多 RAT 都能获取到用户已保存和缓存的密码，一旦掌握了用户名和密码，恶意攻击者便能试着登录到共享服务器。

谨记一点，大部分 RAT 程式都能对已被入侵系统的命令行进行访问。恶意攻击者可借助相应的管理权限来控制 RAT，让它执行恶意攻击者计划执行的任何操作，例如安装和删除文件或安装键盘记录程式。

RAT 入侵系统的方式并不存在任何特殊之处。RAT 的分布方式与其他类型的恶意软件大致相同：它们都与其他常见的攻击媒介一道以电子邮件为发送载体，被植入程序植入系统，并被设置为漏洞攻击工具的有效载荷。

2020年态势分析

2020年恰逢中国十二生肖中的“鼠年”，这或许也是种巧合。近期在威胁环境中常见的一些RAT包括 Orcus RAT 和 RevengeRAT。Talos在今年夏天就发现了这样一个恶意攻击者：它在针对政府实体、金融服务组织、信息技术服务商和咨询公司发起的各种恶意软件分发活动中，一直在不断地利用 RevengeRAT 和 Orcus RAT。

他们发现了与这些活动有关的几种独特战术、技术和程序（TTP），包括：

- 使用与“无文件”恶意程式存在最普遍关联的持久性技术
- 旨在掩盖 C2 基础架构的迷乱技术
- 旨在绕过自动分析平台（如恶意程式沙箱）的规避手段

由于网络犯罪分子会继续扩展 RAT 的用例范围，因此它们在来年势必构成威胁。

3. 藏匿在加密流量中的威胁

攻击场景

为了将威胁成功散布到目标系统和网络，恶意攻击者一定会竭尽全力。一旦成功入侵目标组织，他们最不想遇到的情况就是自己的流量被网络监控工具监控到。所以现在的很多威胁都会借助加密流量来防止自己遇到这种情况。

从恶意功能的角度来看，威胁加密的手段也十分繁多。从命令控制（C2）通信到数据的盗取，恶意攻击者都会通过加密来隐藏恶意流量。

如何检测恶意加密流量

用于捕捉恶意加密流量的其中一种方法即流量指纹技术。这项技术能够监控您网络中的加密数据包，并寻找与已知恶意活动相匹配的攻击模式。

但是，由于恶意攻击者能够轻而易举地将随机或虚拟数据包嵌入其流量，以掩盖可能留下的指纹，所以这项技术不足以捕捉所有恶意加密流量。在这种情况下如果要准确识别出恶意流量，您就需要求助其他检测技术，例如可识别更复杂恶意连接的机器学习算法。但是威胁可能仍然会想尽各种办法来规避一些机器学习检测方法，因此我们建议用户采用分层方法，综合多种技术。

2020年态势分析

通过加密流量发动的威胁持续加剧。根据思科收集到的数据资料，在Cisco Stealthwatch发现的所有威胁事件中，有63%是在加密流量中发现的。由于整个行业不太可能放弃使用https技术，因此企业千万不能轻视这项加密技术，因为它很可能会成为被一些网络犯罪分子进行尝试并有效利用的一种策略。有关网络分析的用途，我们将在结语部分予以探讨。

有关藏匿在加密流量中的威胁，请阅读更多内容。

图 3　银行木马对其正在窃取的数据进行加密。

4. Office 365 钓鱼攻击

攻击场景

您正在通过您的 Office 365 帐户与一位同事进行邮件沟通。邮件主题是关于您准备提交给董事会的一篇报告，最终版本由您的同事发送给您。

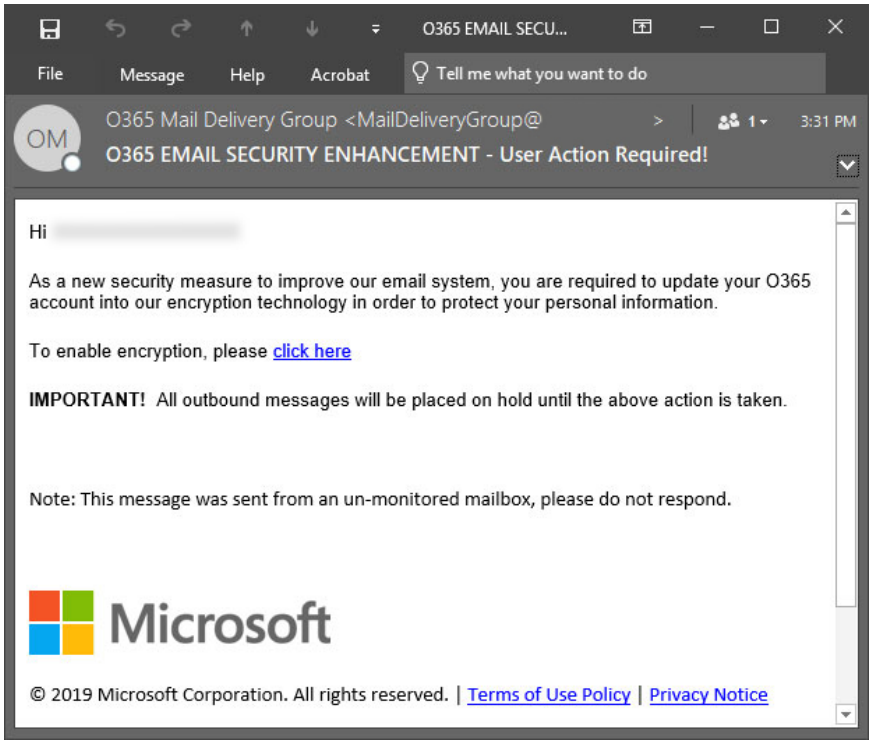
除非对方不是您的同事，发送的不是您要的报告，否则你们的对话内容恐怕已经被恶意入侵者所掌握，因为他们已经成功破坏了企业 Office 365 的正常使用。他们会拦截并回复您发送给 “colleague @ yourcompany.com” 的电子邮件，目的就是让对话朝着他们计划好的方向发展，以便他们掌握更多信息。

连锁反应

恶意攻击者用来获取 Office 365 帐户访问权限的方法通常简单粗暴。网络钓鱼攻击通常以貌似来自 Microsoft 的电子邮件为载体。这种电子邮件中包含一个登录请求，包括提醒用户重设密码，最近是否登录过账户，或帐户存在问题，需要他们注意。邮件中还包含一个 URL，邮件阅读者为了解决提到的问题，很可能会点进去。

在成功发起的 Office 365 网络钓鱼攻击中，用户输入的登录信息会被恶意攻击者盗取。整个伪造的网页上没有任何有用的信息，只是提示用户登录信息错误，或将用户重新带回到真正的 Office 365 登录页面。

图 4 Office 365 钓鱼邮件示例



在完成这一系列操作之后，大多数用户都不会知道自己的登录信息已被盗取。

为了让局面更加复杂，恶意攻击者经常会使用一种“会话劫持”的伎俩，就像前面提到的攻击场景一样，攻击者正是通过对已进入被攻击收件箱的电子邮件进行回复，来释放他们的恶意有效载荷。

2020年态势分析

ESG 代表思科展开的一项最新研究表明，超过80%的被访者都提到了自己就职的企业都在使用类似 Office 365 的 SaaS 电子邮件服务。但是，仍有43%的被访者反映，在使用此类服务之后，他们反而需要通过一系列二次安全技术来支撑他们的邮件防御系统。

思科CISO基准研究报告显示，对用户行为的关注（例如点击邮件或网站中的恶意链接）仍然很高，且已成为 CISO 关注的首要问题。只有51%的被访者认为自己能够很好地处理好与安全相关的人力资源问题，具体就是根据综合的员工入职流程和其他适用流程来处理员工调动和离职问题。此外，Verizon在其发布的《 2019年数据泄露调查报告》中也提到，网络钓鱼是迄今为止成功率最高的一种威胁载体。过去一年，网络钓鱼在几乎三分之一（32%）的数据泄露事件中都扮演主要的攻击武器。

特别关注：Magecart 卷土重来

2019年，我们见证了 Magecart 恶意网站通过盗取信用卡详细资料的撇油器卷土重来。Magecart对最近几个月内几起关注度极高的数据泄露事件负责，包括针对航班预订和在线票务服务的攻击。

这次回归有一点值得我们注意，那就是在若干起供应链攻击事件中也出现了 Magecart 的身影。比如在一月份那场供应链攻击中，受影响的电商网站多达数百家，他们主要销售化妆品、医疗保健品、服饰及上述行业产品。

Magecart 之所以能在此类攻击中产生重要作用，原因就在于恶意攻击者将这些品牌用于其电商服务的第三方网站作为目标，这样一来他们就能扩大攻击范围并成功窃取更多数据，而无需逐个攻破。

1. Mark Bowker 和 Adam DeMattia, 解决方案展示: 思科邮件安全机制, ESG, 2018年10月。

图 5 销售商品和服务的恶意攻击者示例。

5. 社交媒体和网络黑市

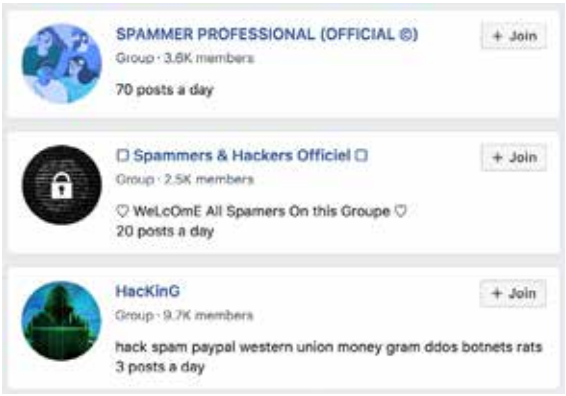
您可能以为网络犯罪行为都发生在互联网深处的隐秘角落里，他们所依托的网络经过严格加密处理，需要通过复杂软件和广泛授权才能访问。然而事实并非总是如此。网络犯罪活动有时也会出现在公开程度极高的场所，例如社交网络。

Talos 的研究人员在2019年初就发现了包含数十万名成员，且以 Facebook 为公开活动平台的多个网络犯罪群组。这些群组通过社交媒体平台与其他犯罪分子进行联系，共享并出售各种工具、技术以及盗取的数据，而且这些犯罪分子之间有时也会互相讹诈。经过广泛的研究和分析，Talos 研究人员发现，通过 Facebook 群组共享的部分工具可能与 Talos 此前监视过的恶意活动存在一定的关联。

关注度丝毫不减的热点问题

我们必须搞清楚一点，社交网络并非在最近才成为帮助网络犯罪分子开展非法活动的工具。截至本文撰写之时，在我们发现的 Facebook 群组中，有些已存在长达八年之久。而他们的活动也已经不是第一次成为公众关注的焦点问题。网络安全研究员 Brian Krebs 最近就曝光了120个具有类似性质的网络群组，成员总数大约在30万名。虽然这些群组名义上已经停止活动，但从Talos在2019年汇报给 Facebook 的群组数量来看，这似乎并没有影响此类活动成员数量的增长。

图 6 有关 Talos 针对社交媒体和网络黑市的调查，请阅读更多内容。



在这种情况下，如果用户在此类社交媒体活动中并非直接目标，那么还存在一线希望。社交媒体平台不仅已经成为犯罪分子共商犯罪大计的重要场所，还变成了犯罪分子买卖工具的交易市场，包括针对如何发动攻击提供相应的培训。

2020年态势分析

2019年底，我们在 Facebook 上快速检索了几个比较明显的群组名称，例如“ Spam professional（垃圾邮件专家）”，“ Spam and hackers（垃圾邮件和黑客）”，发现这些群组仍然存在，而且每天都有好几条新的发帖记录。作为一个网络安全社群，我们不仅将继续向 Facebook 报告这些群组的存在，还会与 Facebook 联手，实现更多突破。

6. 数字勒索诈骗

攻击场景

您突然收到一封标题包含您用户名和密码的电子邮件。但真正让您感到慌张的却是这封邮件的正文内容。

发件人在邮件里写道它已经入侵了一个色情网站，而且您访问过这个网站。诈骗者会告诉您他们已经控制了您的显示器和网络摄像头，记录了您的个人资料和色情资讯，然后对这两段视频流进行了同步处理。

除此之外，诈骗者还声称他们已经通过您的社交媒体帐户和电子邮件收集了所有联系人信息，这才是最令人不安的地方。而且在邮件结尾，诈骗者还会巧妙地暗示您，如果他们将视频发给这些联系人，结局将会多么难堪。

接下来，诈骗者会说自己并非不近人情，想要清除这些内容也并非难事。您只需支付价值1000美元的比特币，诈骗者就能让这些令人难堪的内容全部消失。

虚张声势

如果这看起来像是敲诈，那是因为它的目的就在于此。但是也不排除虚张声势的成分。

在这个案例中，电子邮件所声称的内容都是虚假的：他们并没有入侵任何网站，没有控制您的网络摄像头，也没有盗取任何联系人资料，而是在巧妙地利用人类的复杂情绪以及内心深处的罪恶感。除此之外，还有另外一大批网络钓鱼活动，他们的目标则是通过诱骗大量收件人来帮助敲诈者获利。为了让增加邮件的真实感，他们会在邮件里加入真实的用户名和/或密码。其实，敲诈者的真实意图则是想通过之前窃取的数据牟利。

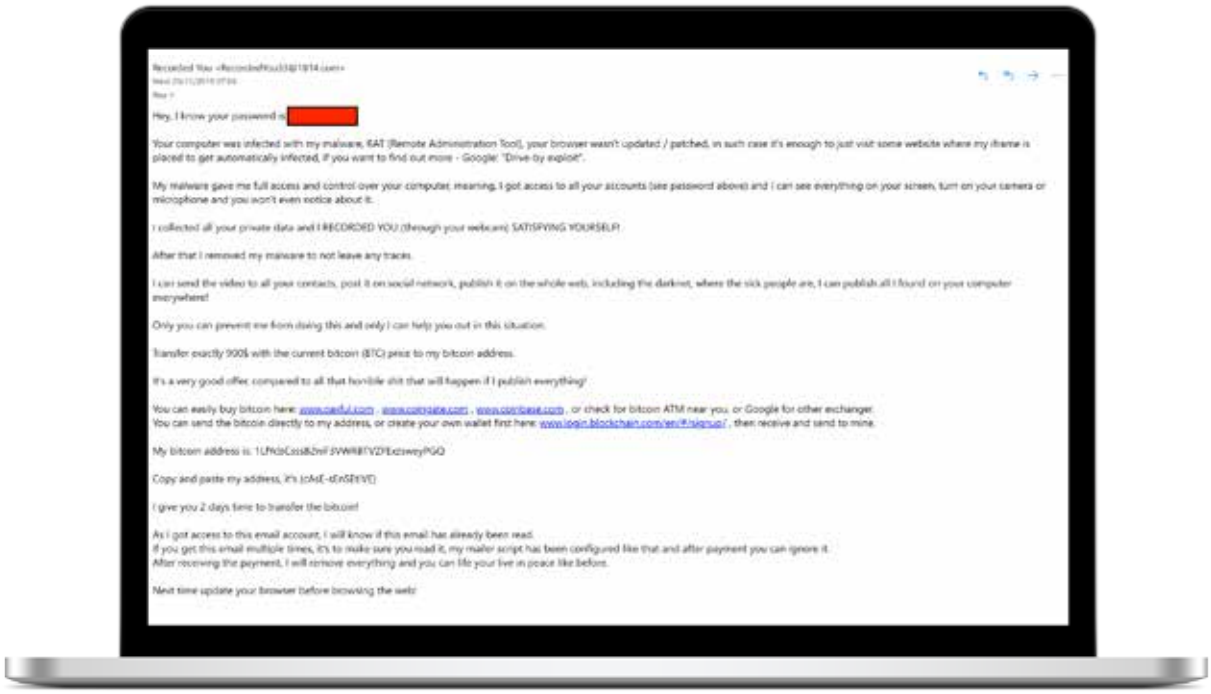
这些邮件中还包含大量技术行话。这并不是说远程访问您的桌面或网络摄像头是不可能发生的事（但它的确发生了），而是根据诈骗者所描述的方式，他们想要访问您桌面活网络摄像头的可能性还是微乎其微的。

如果您收到了类似的邮件，请注意您的个人数据可能已经遭到外泄。如果这个密码还用在其他地方，请立即更改。如果您想搞清楚自己的邮件地址是否已经外泄，请查看相关服务，例如“ Have I Been Pwned”，并将此类情况是否出现以及出现的地点一一列出。

2020年态势分析

即使胜算很低也能获利，因此数字勒索仍然是当下常见的一种攻击模式。图7就为我们展示了最近出现的一个数字勒索案例。

图 7　近期出现的数字勒索邮件示例。



思科的威胁应对之道

正如任何一种威胁解决方案，思科专门针对关键基础设施威胁而设计的纵深安全防御机制，将为有效保护企业的网络安全提供强大助力。

建議1：及時更新系統，定期下載補丁。比如在 Sea Turtle 這個案例中（DNS劫持），正是由於存在漏洞，包括一些已存在10年之久的漏洞，惡意攻擊者才得以成功入侵使用者的系統。

应对威胁的关键在于能否充分利用威胁情报作为制定威胁防御策略的基础。思科网络安全产品将帮助您充分利用 Talos 威胁情报的强大力量，而这种力量蕴藏在思科的每一个系列里，每一款产品中。

下面的内容不仅列出了构成分层防御机制的部分解决方案，同时也突出强调了每个方案旨在应对哪种威胁。

监控 DNS 记录并阻止恶意域名

Umbrella Investigate 是一个支持互联网域名、IP 及文件相互关系及演变过程完整视图的 DNS 检测平台，旨在帮助用户查明恶意攻击者的基础架构，准确预测后续威胁，并帮助用户快速查找对 DNS 记录所做的更改。能否顺利连接 C2 域名，是许多威胁实现其功能的关键。Cisco Umbrella 通过 DNS 阻止针对所有端口和协议的威胁，甚至可以阻断IP直连，以此来防止用户连接到恶意攻击者的服务器。

此方案针对的威胁包括： DNS 劫持、RAT 威胁、定向勒索软件、以及藏匿在加密流量中的威胁

采用切实可行的终端保护解决方案

随着入网设备的数量不断增加，用户必须清楚地知道自己的终端设备正面临哪些攻击，然后积极主动地进行防御，并在防御机制出现漏洞时快速响应。面向终端的思科高级恶意软件防护体系 (Cisco AMP for Endpoints) 可将恶意软件的入侵定格在入侵起点，然后针对这些高级威胁采取相应的检测、控制和补救措施。

此方案针对的威胁包括： RAT 威胁

借助多因素身份验证（MFA）

思科的 MFA 解决方案，比如 Cisco Duo（双因素身份认证），旨在验证用户身份，洞察每台设备，并通过实施自适应策略来确保应用程序访问的安全性。如果恶意攻击者盗取了用户的登录信息，MFA 还能阻止他们登录用户系统。

此方案针对的威胁包括： RAT 威胁、定向勒索软件、以及 DNS 劫持

监控网络流量

监视未授权活动是一项非常重要的工作。作为一种网络流量安全分析解决方案，Cisco Stealthwatch 以来自现有网络基础设施的企业遥测数据为基础，赋予用户最全面的信息可见性。Stealthwatch 还包含加密流量分析（Encrypted Traffic Analytics）功能，可帮助用户找到那些藏匿在加密流量中的狡猾威胁。

此方案针对的威胁包括： RAT 威胁，以及藏匿在加密流量中的威胁

邮件安全机制

除垃圾邮件、病毒、恶意软件防御等基础措施外，在保障邮件安全方面，用户还可采用更高级的网络钓鱼防护措施，比如通过机器学习来分析和验证邮件身份及行为关系，以及时阻止更先进的网络钓鱼攻击。

此方案针对的威胁包括： Office 365 钓鱼攻击、RAT威胁、以及数字敲诈

识别恶意文件行为

类似的解决方案，比如思科 Threat Grid，旨在搜寻恶意文件，然后将通知自动下发至所有思科网络安全产品。

Threat Grid 将高级沙箱与威胁情报整合到一套统一的解决方案中，旨在保护企业免受恶意软件的侵害。

此方案针对的威胁包括： 定向勒索软件、RAT 威胁

平台化方案

平台化方案，例如思科威胁响应（CTR）平台，能够面向多种攻击载体和受影响系统，对新的病毒感染、漏洞传播和数据泄露情况实施全方位阻断。CTR 平台可自动完成并加速主要安全操作功能，包括检测、调查和修复。它也是思科集成安全架构的关键支柱。

此方案针对的威胁包括： 所有威胁类型

事件响应

此类方案旨在提升用户面对各类攻击的准备水平和响应能力。借助 Talos 事件响应服务，用户可直接访问与思科相同的威胁情报，从而帮助您针对安全漏洞进行准备、做出响应并从中恢复。我们的专家会与您共同评估现有计划，制定全新计划，并在您最需要的时候提供及时快速的帮助。

思科网络安全系列报告简介

过去十年间，思科面向关注全球网络安全态势的网络安全专家发布了大量具有权威性的安全及威胁情报信息。这些综合性报告不仅详细描述了相关的威胁态势以及它们对企业的潜在影响，还列出了能够有效抵御数据泄露所产生的不良影响的最佳实践。

作为我们提升思想领导力的一项全新方案，思科安全团队以“思科网络安全系列报告”为主题，不断发布一系列基于研究的数据导向型报告。我们专门增加了标题的数量，以涵盖具有不同关注点的网络安全专家所撰写的不同类型的报告。依托网络安全行业中诸多威胁研究人员和创新者深邃且广泛的专业知识，思科在2019年成功发布了数据隐私基准研究、威胁报告、CISO 基准研究等一系列网络安全报告。

了解更多信息，并查看所有报告和存档文件，请访问:
www.cisco.com/go/securityreports

北美总部
Cisco Systems, Inc.
加州圣何塞

亚太总部
Cisco Systems (USA), Pte. Ltd.
新加坡

欧洲总部
Cisco Systems International BV Amsterdam,
荷兰

思科在全球拥有超过200个办事处。您可登陆思科官网，查看各办事处的地址、电话和传真，具体链接为: www.cisco.com/go/offices

2019年11月发布 THRT_08_1219