中国计算机行业网
www.ciw.com.cn

http://www.ciw.com.cn/h/2562/408536-22820.html
It is difficult to measure the high cost of protecting network from malware
17/10/16

防护网络恶意软件的成本高昂难以衡量

出处：中国计算机行业网 日期：2016-10-17

毫无疑问，对消费者、员工和企业而言，勒索软件的攻击非常可怕!受害者必须付出可观的代价从勒索攻击中复原。美国有线电视新闻网(CNN)报道，根据美国联邦调查局2016年4月的报告，“通过敲诈企业和机构来解锁计算机服务器，网络犯罪在2016年的前三个月就收获了2.09亿美元。”典型的勒索软件可能要求支付10,000美元或更高的金额;比如好莱坞长老会医疗中心在二月份就支付了超过17,000美元的赎金。

同样重要的是，我们对从勒索或其他网络攻击中恢复的成本已经相当了解。但我们应该考虑的是一个组织应该花多少钱来防止这些攻击?首席执行官和其他领导们都承认他们必须投资在保护网络上。但要如何判断那笔花费是否明智而非出于恐惧过度?我们需要更聪明地花钱，以获致更好的安全形势。

先让我们来看看现代企业面临的最大攻击的提供恶意软件(包括勒索软件)的网站。

网站如何能造成严重破坏

我们检查网站有两个原因;首先查看目前市售的解决方案风险如何被降到最低甚至消除。其次，网站是最常见的一种恶意软件载体(与恶意电子邮件一起)，它可以提供许多其它类型黑客攻击的入口点。只要能阻止恶意软件访问网站，整体网络安全的风险就降低了。

AV-TEST报道，已经有超过5.5亿个恶意软件变种，而且每天都可以辨识出39万个以上新的恶意程序。这是一个令人难以置信的数字。以下是恶意软件进入最终用户计算机的一些方式，恶意软件从哪里开始无限制地访问该计算机的一切事物及业务网络上的其他资源：

- 用户点击普通的网络钓鱼电子邮件内或高度定制的鱼叉式网络钓鱼电子邮件内的一个链接，从而打开一个包含恶意软件的网站。

- 用户打开了包含一个链接的文件，而该链接打开一个包含恶意软件的网站。

- 用户点击了社交媒体(如脸书或推特)上的一个链接，从而打开一个包含恶意软件的网站。

- 用户点击了受信任的网站(如新闻/媒体网站)上的链接，从而打开一个包含恶意软件的网站。

- 不良行为者感染一个受信任的网站，即使这些访客没有点击任何链接，它就可以将网站编程传送恶意软件给访客。

- 不良行为者危害内容交付网站、行为追踪器，或其他网站的组件，并将他们编程后再传播恶意软件给访客。

许多情况下，最终用户即使没有做错事，仍不免被感染。

阻止访问这些未分类的网站可以降低被恶意软件感染的机会，但也会造成一些问题和隐性成本，比如更多的帮助台派工单。允许访问未分类的网站会将组织置于更大的风险中，并增加安全警报的数量，以至于管理者处于两难的情况。

允许访问未分类网站带来的问题

• 风险：允许访问未分类网站而带来恶意软件的风险是显著的。一家财富50强的大型金融服务机构委派了他们的安全研究小组用三个月的时间来分析恶意软件感染的来源。他们的内部报告显示，超过60%的感染来自未分类的网站。这些感染带来昂贵的成本，一家大企业每星期平均可以花上近600小时在恶意软件围堵控制上。考虑到每个SOC(安全运营中心)工程师小时是82美元，一年52周，每周 600小时，光是在这一个任务上的花费每年就得超过250万美元。

• 消毒受感染机器的成本：消毒受感染的机器可以说是相当昂贵的。在亚洲的一家大型服务提供商被迫每周为平均八台的端点设备重新做映像，因为他们不再相信他们能成功地消毒使用传统防病毒解决方案的机器。其内部分析表明，这种做法让他们每年在IT和生产力损失上付出3至4百万美元的代价。

• SOC成本：允许未分类的网站意味着更多的安全警报。在日本，以及全球范围内最规范的行业，来自每一个安全产品的每一个警报必须充分分析其可能的端点危害。根据Ponemon协会的分析，因为错误的情报，安全人员应对恶意软件警报所花费时间的三分之二是浪费的。它每年让组织平均花费127万美元在浪费时间应对错误或不准确的恶意软件警报。

• SOC周转：SOC工程师的平均就业期限大约是一年，他们多半因为应对这些安全警报的重复工作不堪疲劳而辞职。越来越难雇用到合格的SOC工程师，由于应届毕业生被吸引去构建app应用软件，而不是学习具有陡峭的学习曲线和复杂性专业知识的安全和取证科学。

假设以年薪170,000美元的基本工资和典型的25%的招聘成本来填补这些职缺。若一个5人团队中有40%流失率，其招聘成本每年就达85,000美元。如果考虑两位现有的SOC工程师花费他们25%的时间来训练两名新进员工的机会成本，每年成本还需增加额外的85,000美元。综合以上，每年员工周转总成本约为170,000美元。

拒绝未分类网站的问题

故障派工单数目：拒绝未分类网站创建了重新分类请求数量的激增。对于一家全球性的投资公司而言，每天为了全体25万员工重新分类产生的派工单请求数量约为2000个。75%以上的这些请求是与工作无关的，例如兽医研究、学校、少年足球联赛…等等。若有超过5名专职人员解析这些请求，每年就要花费850,000美元。

重新分类专家：重新分类是一个手动过程。当一家欧洲保险公司和一家大型日本制造商开始阻止访问未分类网站时，很容易被这样的请求淹没。这个问题还因为另一个事实而雪上加霜，这个事实就是他们的安全web网关无法帮助他们确定有问题网站的安全状况。上述两家组织分别有16名和5名安全分析师专注于分析重新分类前的网站。另一家全球金融服务公司有20名员工在世界各地，用他们自己的话说，在“重新创建雅虎的索引”。就以5名SOC员工来保守估算，这个团队每年让企业花费超过300万美元。

用另一种方式来看：阻止未分类的网站防止了用户访问合法的内容，因而危害了生产力，并且会产生对屏蔽内容重新分类的请求。同时，允许访问未分类的网站意味着更多的恶意软件和网络钓鱼攻击会到达用户，这样就会通过数据盗窃和欺诈行为导致破坏和重大损失。除了用户的问题，IT人员追逐未分类网站所产生的所有警报是非常昂贵的(通常是不可能的)，会导致高昂成本和降低安全性。我们就是无法用传统的方法取胜。

一个更有效的策略：隔离

隔离技术，就其性质而言，是不打开终端用户台式机、笔记本，或移动设备上的网站，而是打开基于云的平台上的安全虚拟容器内的网站。最终用户是通过能呈现与直接访问无分别的用户体验的技术来与网站互动。借由执行远离端点的会话，并且只提供安全呈现的信息给设备，用户就避免了恶意软件和恶意活动的攻击。

恶意软件没有到达端点的路径，而合法的内容不需因安全的利益而被阻止。管理者可以开放更多的互联网给他们的用户，同时消除了攻击的风险。

“隔离”终结了他们昂贵的两难局面：

- 风险：没有活跃的web内容到达端点，从而未分类的网站存在零风险。
- 消毒感染机器的成本：隔离消除了网站成为恶意软件威胁的载体，大大减少了需重新映像的机器的数量。降低了为每个浏览器和插件漏洞制作修补机的紧迫性。
- SOC成本：隔离会在传统解决方案检测到威胁之前就阻止了威胁，消除了错误或不准确的恶意软件警报。
- SOC周转：警报疲劳与SOC员工流失一起都被最小化。
- 故障派工单数目：员工生产力更高，且现在可以自由安全地探索网络而不需提交重新分类请求。
- 重新分类专家：通过消除重新分类的请求，需要昂贵专家的需求被消除。

有超过5.5亿的恶意软件变种，以及每天成千上万新的恶意软件被发现，传统检测恶意软件的方法在时间上，在人才上，并在人员配备上，以及在购买和维护安全产品的成本上有许多隐性成本。隔离，不需安装任何软件在最终用户的台式机、笔记本，或移动设备上，不仅节省IT的时间和金钱，而且还消除了关于更新最终用户软件的担忧。