解决可视性缺口

使用思科 StealthWatch 可视性评估保护您的网络

随着网络不断壮大和日趋复杂，组织在保护自身应对日益复杂的威胁发起者时，显得捉襟见肘。攻击常常数月未被发现或报告。要检测和缓解安全风险，您需要能够了解您的网络中正在发生的情况。

为了帮助您实现此目标，我们提供思科 Stealthwatch™ 可视性评估。它旨在评估您的内部网络可视性和整体安全状态。

我们评估了数百个组织，即刻便发现以往未检测到的未知主机和恶意网络活动。对环境中攻击者行为和位置的深入了解，可帮助您防止安全事件演变为大范围的数据泄露。

内容提要

Stealthwatch 可视性评估对 10 个与恶意活动或安全风险相关的主要标准进行评估。本白皮书涵盖以下内容：

- 十个您需要可视性的关键区域
- 思科 Stealthwatch 如何帮助您监控这些区域
- NetFlow 如何提供端到端网络可视性

内部受监控网络

内部可视性对了解您的网络状态至关重要。思科 Stealthwatch 技术可持续监控和保护内部资产，观察服务器和互联网之间传输的数据，并处理流量。这些指标和其他内容可帮助安全和网络人员量化网络中的主机、系统和资源，从而确保不会出现任何未知的内容。他们还可以确定关键资产、验证策略、审核和验证合规性，帮助您基于数据做出更明智的决策。

Stealthwatch 可视性评估可确定您的网络中活跃通信的主机数量。

服务器消息块风险

有些威胁会使用服务器消息块 (SMB) 协议对主机进行控制。由于有许多组织使用该协议，所以攻击者可以用它隐藏恶意活动迹象。具有破坏性的定向恶意软件（例如 Conficker）还会利用 SMB 漏洞部署代理工具、安装后门、破坏数据，并导致服务器离线。

在我们评估的组织中，有一半存在恶意 SMB 流量。

即便 SMB 是常用协议，我们也能通过可视性和正确分析轻松区分善意与恶意 SMB 行为。例如，如果存在异常多的 SMB 会话（尤其是网络主机与互联网主机之间存在异常多的 SMB 会话），很可能是恶意软件传播迹象。

当 FBI 来敲门

一家国际油田服务公司收到 FBI 的通知，被告知其网络遭到中国网络犯罪者的攻击。

公司安装了思科 Stealthwatch 系统后，在一周内确定了漏洞来源。一名看上去是从中国登录的本地用户，竟试图一次窃取数千兆字节的重要文件。但实际情况是，攻击者窃取了该用户的访问凭证，获得了对敏感数据的特权访问权限。

如果该公司当初具备适当的网络可视性，就能尽早识别并修复此行为，从而避免数据丢失。

高风险国家/地区的流量

大多数组织的业务范围仅限于特定地理区域。识别来自这些区域以外的流量是检测威胁的有效方式。例如，如果在某个仅为美国中部居民提供服务的公共设施公司中，发现了大量来自东欧或亚洲的流量，就很不寻常。

检测来自与大量威胁活动关联的区域的流量，尤为重要。在我们评估的组织中，有 50% 已经受到来自高风险国家/地区攻击者的影响。

如果组织能够监控来自可疑国家/地区的流量，就能在其系统受到影响之前发现攻击，并加以阻止。

DNS 风险

DNS 服务器用于将主机名转换为相应的 IP 地址，因此对网络正常运行（尤其是互联网访问活动）不可或缺。使用未经批准的 DNS 服务器，可能是恶意活动或违反策略的迹象。在我们评估的组织中，有 70% 以上表示他们的网络中存在未经授权的 DNS 使用的情况。

许多组织依赖自己的 DNS 服务器执行策略，例如阻止对违禁网站的访问。一些经验丰富的用户会利用未经授权的 DNS 服务器来规避此类策略。如果用户访问不安全的网站或违反公司关于 Web 内容的政策，势必会将组织置于危险境地。

更让人不安的是，据《思科 2016 年度安全报告》显示，91.3% 的恶意软件在攻击中使用了 DNS。恶意软件通常会重新配置受感染的计算机，使其使用恶意 DNS 服务器。这些恶意服务器会将用户重定向到利用漏洞或钓鱼获取访问凭证的网站，从而使组织面临威胁和数据丢失的风险。

代理违规

大多数组织使用代理服务器阻止已知恶意网站、不当内容和数据泄露，同时使用这些服务器保存用户互联网活动日志。用户可能会尝试绕过这些代理服务器，以避开策略，而且配置错误的设备可能导致意外不合规。这两种情况都会使组织面临数据丢失和遭受攻击的风险。借助于端到端网络可视性和监控，思科 Stealthwatch 可持续代理策略审核，并在检测到违规行为时发出警报。

远程访问漏洞

远程网络访问正在迅速成为大多数公司的标准业务活动。让移动工作人员可以随时随地访问公司资源至关重要，但同时这些服务也很容易被攻击者利用。如果成功入侵，远程访问服务将能够为攻击者提供与合法用户相同的权限。

接受评估的组织中大约有 38% 曾因远程访问遭到某种漏洞攻击。因此，获得远程访问流量的可视性对识别可疑活动来说非常重要。

欺诈服务器活动

欺诈服务器是指企业网络中设置的不受管理员控制的服务器。攻击者可以利用这些服务器获得网络的永久访问权限。在最近的一个案例中，我们发现某个组织的内网中有 30 多个未知和未授权的服务器正在使用中。在这些服务器中，很多都未应用最新的补丁和安全标准，因此容易被利用，导致组织暴露于危险之中。

欺诈服务器通常最初是由员工出于良好意图设置的（比如工程师希望构建一个快速测试环境以方便工作）。安全团队通常并不知晓这些服务器的存在，因此无法保证对它们采取了适当的保护措施。如果员工忘记在完成测试后禁用服务器，那么情况会变得更糟。

攻击者会在已入侵的网络内部设置他们的服务器。这些服务器将成为他们在网络内部横向移动的基地，或成为他们转移被盗数据的中转站。

自定义恶意软件

在思科 Stealthwatch 的一次评估期间，一家大型技术公司发现其几乎半数的终端用户工作站受到专门针对其网络编写的自定义恶意软件的感染。

该恶意软件已偷偷窃取他们的数据很长时间了。这种情况无迹可寻，但是通过行为分析，我们可以检测到恶意软件在整个网络中的扫描、连接和传播操作，从而加以制止。

行为分析

当今的网络庞大且复杂，为威胁发起者提供了许多入侵途径。更令人担忧的是，大多数攻击者非常擅于利用弱凭证、默认凭证或窃取的凭证，来伪装成合法用户。要区分入侵者与他们模仿的用户，一个重要途径就是对网络活动进行监控，识别异常或者与攻击相符的行为。

例如，扫描网络的主机可能是在执行侦测，但也有可能是在传播恶意软件。同样，如果营销部门的某个用户通常每天只访问几兆字节的网络资源，但突然有一天下载了上千兆字节的工程材料，那么很可能是有不法之徒准备将数据泄漏到网络之外。

就我们评估的组织而言，他们的网络中都存在可疑和异常行为。

保护有风险的资产

每个组织的网络均存在部分需要密切关注和更多防御的高度敏感数据。保护这些“皇冠上的珍珠”可能是网络安全战略最重要的一部分，因为它们常常是威胁发起者的最终目标。借助思科 Stealthwatch 技术，组织可以密切监控这些宝贵资源是否存在恶意活动、策略违规行为和错误行为的迹象。当出现内部主机或从外部互联网访问这些数据的情况时，思科 Stealthwatch 可对其进行检测，并将可视性扩展到敏感系统（例如数据中心）内及敏感系统之间的流量上。

Telnet 风险

Telnet 是一种不安全的旧协议，使用此协议可能会导致凭证受到攻击以及数据丢失。Telnet 可以在计算机之间建立通信，但大多数版本没有有效的加密功能，因此也就成为网络安全攻击报文窃听的主要目标。当数据以纯文本格式传输时，攻击者可以进行拦截，从中获取密码和其他敏感信息。

大多数组织认为他们没有使用此协议，但是我们的评估发现，67% 的组织网络中存在 Telnet 流量。

存储敏感数据、财务程序和客户信息的大型主机和其他系统通常会运行 Telnet，因此很容易暴露在攻击之下。自 1994 年以来，软件工程研究所 CERT 部门便一直推荐使用纯文本验证（例如 Telnet）之外的方式。

要确保 Telnet 不会使组织处于危险中，安全操作人员必须能够在企业网络中的任何位置检测并响应 Telnet 活动。

照亮网络中的黑暗区域

获得对这些区域的可视性，对有效保护您的网络和数据至关重要。幸运的是，大多数网络都内置监控功能，我们只需要一种方式对这些功能善加利用。

在包括路由器、交换机和防火墙在内的大多数网络基础设施设备中，都存在网络流量元数据（如 NetFlow）。思科® Stealthwatch 可以收集并分析这些数据，对所有网络流量（包括 IP 地址、端口、用户、设备和应用等信息）建立审计追踪机制。思科 Stealthwatch 可存储数月甚至数年的流量数据，而且无需占用过大的存储空间。

借助 Stealthwatch，安全专业人员可以获得深入的网络见解，从而：

- 实时发现可疑的攻击行为
- 对曾经发生的攻击尝试进行调查，确定根本原因
- 从攻击追溯到特定用户、设备、位置和时间范围
- 改善其组织的安全状况

Stealthwatch 可视性评估开启您的网络明灯，评估您的内部可视性和整体安全状态。可视性评估包括 Stealthwatch 管理控制台和流量收集器，可收集超过 14天 的网络遥测数据。随后，向您提供包含详细信息和当前安全风险分析的可视性评估报告。

有关详细信息，请访问 www.cisco.com/go/stealthwatch-free-assessment。

C11-738293-00 12/16