探究加密流量背后的重重威胁

Ben Nahorney

曾几何时，网络是一个完全开放的空间。人们在通过早期网络进行文字性交流时，并未采用任何具体的方式对交流内容加以防护。这就意味着，那些在网络设备之间传输的数据很容易被恶意拦截和读取。

如果被恶意拦截或读取的是类似密码认证信息或信用卡交易等敏感数据，那么情况则会变得更加糟糕。为化解通过web传输此类数据时所面临的风险，流量加密技术应运而生，受保护的网络通信时代从此开启。

如今，超过半数的网站都在使用 HTTPS 技术。实际上，根据 Stealthwatch（思科推出的网络流量分析解决方案）背后基于云的机器学习引擎 - 思科认知性智能提供的数据来看，目前已有82%的 HTTP / HTTPS 网络流量会经过加密处理。

流量加密技术的应用对于提高网络安全性和隐私性起到了很大的推动作用。采用这一技术后，用户可以对敏感的交易和通信内容更加放心。然而加密流量也存在一个缺点，那就是我们将更难区分善意行为和恶意行为。随着加密流量的应用程度日益提升，网络数据的隐藏程度也在加深，因此恶意攻击者更容易将恶意活动隐藏在此类流量中。

加密流量简史

Netscape 为解决网络流量的安全性和隐私性问题，于1995年首次推出了安全套接字层（SSL）协议。在发布了若干个版本之后，互联网工程任务组（EITF）接管了该协议，并以“传输层安全性”（TLS）的名称发布了后续的更新版本。 虽然在非正式情况下，SSL 一词仍然经常被用来指代这两个术语，但 SSL 协议的确已被弃用并被 TLS 代替。

TLS 协议可直接与现有协议配合，并对网络流量进行加密。这就是HTTPS等一系列协议的起源 - 超文本传输协议（HTTP）是通过 SSL / TLS 传输的。尽管 HTTPS 是迄今为止通过TLS 实施保护的最常见协议，但其他常用的协议，例如 SFTP 和 SMTPS，甚至一些等级较低的协议，例如 TCP和 UDP，都可以对该协议加以利用。

竞相效仿的威胁主体

为了让威胁入侵系统和网络，恶意攻击者们一定会煞费苦心。在成功渗透到组织内部之后，他们最不想遇到的情况便是他们的一举一动会被网络监控工具捕获。如今为防止出现这种情况，许多威胁主体都选择对其流量进行加密处理。

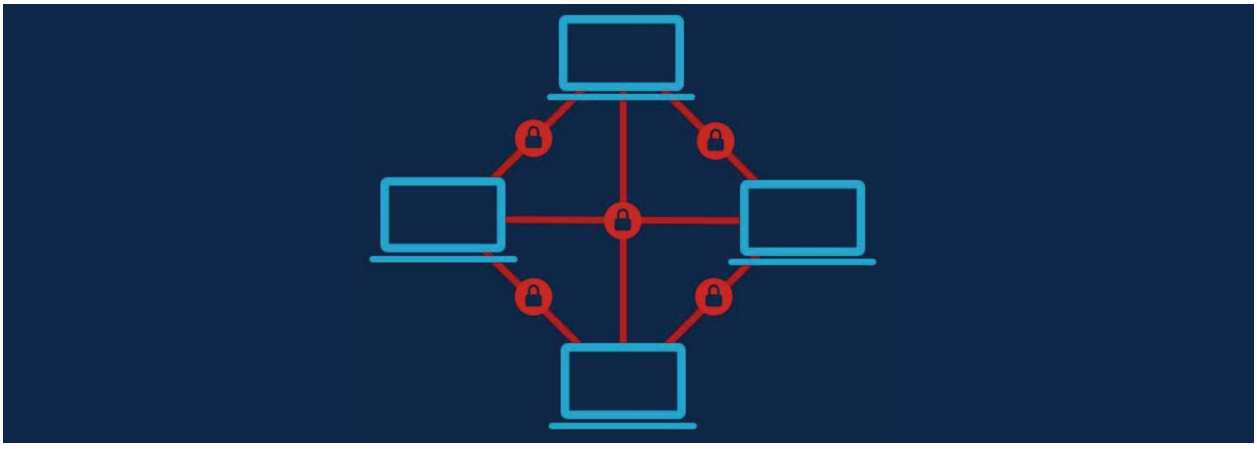
虽然标准化的网络监控工具可能足以快速识别并阻止未加密的流量，但 TLS 却能对威胁的通信内容进行伪装。根据思科认知性智能提供的数据可以发现，Stealthwatch 检测到的所有威胁事件中，有63%是在加密流量中被捕获的。

就恶意功能来说，威胁用来自我加密的方式有很多种。从命令控制式（C2）通信到后门程式，再到数据泄露，攻击者自始至终都会通过加密手段来隐藏他们的恶意网络流量。

僵尸网络

从定义上看，僵尸网络是一组通过互联网相互连接、且已经遭到破坏的系统。僵尸网络中的系统通常采用客户端-服务器配置或点对点配置。但是无论采用哪种配置，恶意攻击者通常都会以 C2 系统为杠杆，以便将恶意指令顺利传递至受损的系统。

像 Sality、Necurs 和 Gamarue / Andromeda 等常见的僵尸网络在进行 C2 通信时都会通过加密技术来持续自我隐蔽。僵尸网络的恶意活动包括下载其他恶意有效负载、传播至其他系统、实施分布式拒绝服务（DDoS）攻击、发送垃圾邮件以及其他一系列恶意活动。



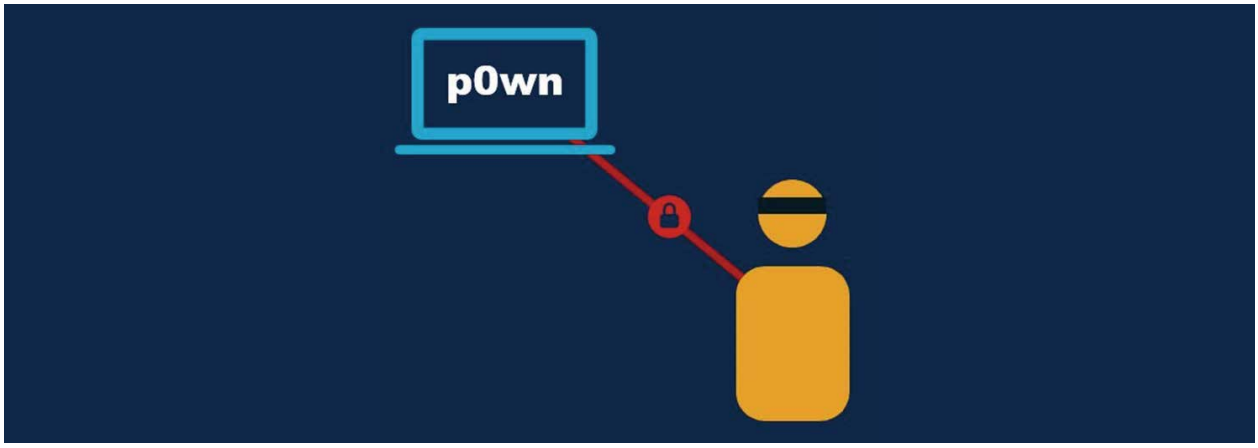
僵尸网络通过加密手段隐藏 C2 流量

RAT 威胁

RAT 的主要目标即帮助恶意攻击者实现远程系统监控。RAT 一旦设法将自身植入某个系统，就需要通过回拨的方式来获取进一步行动指示。RAT 需要定期或不定期地连接互联网，而且经常借助 C2架构来实施恶意活动。

RAT 常常会试着对计算机施加后台管控和/或从中盗取信息，无论是密码、截屏还是浏览历史。之后它便将盗取的数据发回至恶意攻击主体。

如今，大部分 RAT 恶意软件会通过加密手段来隐蔽通过网路传输的内容，例如 Orcus RAT、RevengeRat、以及 Gh0st RAT 的几种变体。



RAT 威胁通过加密手段对计算机施加控制

加密货币挖矿

加密货币矿工会在其运行的计算机和服务器之间建立 TCP 连接。计算机通过这条通道定期接收来自服务器的工作任务，对其进行处理，然后将其发回服务器。要进行加密货币挖矿活动，就必须维持这些连接。因为如果失去了这道连接，计算机就无法对其工作情况进行验证。

考虑到这些连接的长度、重要性以及被发现的几率，恶意加密货币挖矿者通常会对这些连接进行加密处理。

值得注意的是，这里提到的加密适用于任何类型的加密货币挖矿行为，无论是蓄意的还是恶意的。就像我们之前在 Threat of the Month（每月热点威胁）博客中发布的一篇有关恶意加密货币挖矿的文章中提到的，这两类采矿行为最大的区别在于是否获得许可。

加密货币矿工在服务器之间来回传输工作任务

银行木马

银行木马程序的运行依赖于对受感染计算机上的 web 流量所实施的监控。为此，一些银行木马程序会通过恶意代理采集 web 流量或将数据窃取至 C2 服务器。

为防止恶意流量被发现，一些银行木马程序也会采取流量加密手段。例如一个名为 IcedID 的银行木马程序会利用 SSL / TLS 发送窃取的数据。还有一个名为 Vawtrak 的程序，则是通过一种特殊的编码模式来隐藏它的 POST 数据流量，以增大解码和识别的难度。

银行木马会对他们要窃取的数据进行加密

勒索软件

勒索软件使用加密手段的最广为人知的一种情况即通过加密私人文件来要挟对方。但是，勒索软件威胁也经常在网络通信过程中使用加密技术。有些勒索软件家族甚至会对解密密钥的分布情况进行加密。

如何准确捕获恶意加密流量

流量指纹识别技术便是其中一种用于捕获恶意加密流量的方法。对这项技术加以利用的前提，即对网络中传输的加密数据包进行监控，并寻找与已知恶意活动相匹配的指纹模式。例如，与熟悉的 C2 服务器创建的连接会产生一种独特的模式，也就是所谓的指纹。这同样适用于加密货币挖矿流量或比较常见的银行木马。

然而，恶意攻击者只需将随机数据包或伪装包嵌入其流量，即可掩盖可能出现的指纹，因此这项技术不足以帮助您捕获全部的恶意加密流量。为了能在这种情况下将恶意流量一一识别出来，我们需要用到其他一些检测技术来识别流量，例如可识别复杂程度更高的恶意连接的机器学习算法。由于威胁仍有办法躲过某些机器学习检测方法，为此我们建议采用涵盖一系列不同技术的分层法。

除以上内容外，以下几点也值得考虑：

- Stealthwatch 包含加密流量分析功能。这项技术不仅可用于采集网络流量，且无需解码，即可通过机器学习和行为建模来检测各种各样的恶意加密流量。
- 思科 Umbrella 所采用的 DNS 防护技术可用来阻断与恶意域名之间的连接，从而在威胁尚未建立加密连接之前就将其成功阻止。
- 高效的终端防护解决方案（例如面向终端的AMP）对于在威胁开始行动之前便对其实施阻止也能起到很大的作用。

您是否喜欢阅读"本月威胁"系列博文？ 请订阅"本月威胁"系列博客，您将在第一时间收到新博文发布提醒。

关键词: #NCSAM | 本月威胁 | 面向终端的AMP | 思科安全 | 思科Stealthwatch | 加密流量 | 加密流量分析 全国网络安全宣传月（NCSAM） | Stealthwathch | 本月威胁
