每月热点威胁报告：藏匿在加密流量中的威胁

加密技术与Web流量

Web诞生伊始，通过互联网发送密码、信用卡交易等敏感信息是存在很大风险的。为化解这一风险，网络流量加密技术应运而生，人类从此进入受保护的通信时代。

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，用户就能对敏感的交易信息和通信内容感到更加放心。

恶意攻击者竞相效仿

在成功渗透到组织内部之后，恶意攻击者们最不想遇到的情况便他们的一举一动会被网络监控工具捕获。如今，为防止这种情况的出现，许多攻击者都选择对其流量进行加密处理。

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。

延伸阅读

- 思科ETA 白皮书
- RAT威胁齐发动：通过可窃取信息的RAT威胁在PC中植入后门
- 加密货币挖矿：是羊还是狼
- 思科 Stealthwatch
- 思科 Umbrella

僵尸网络&RAT威胁

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实现自我隐蔽。
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络传输的内容，例如Orcus RAT、RevengeRat、以及Gh0st RAT的几种变体。

银行木马&加密货币挖矿

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

加密货币矿工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。

思科 Stealthwatch

- 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

- 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。

07/19