应用于网络安全遥测的花蜜通证 (NCT)

PolySwarm

2021-05-17

摘要

我们为 PolySwarm 的花蜜通证 (NCT) 引入了一种新的用途：用来奖励那些提供安全相关遥测 (telemetry) 数据的大众用户。现在，遥测数据提供者（即用户）将根据提供的遥测数据价值获得奖励，并通过对全世界的遥测数据网络做出贡献，获得全球 PolySwarm 网络的集体保护。质押者和遥测数据聚合者参与到网络中，协助判定最有用的遥测数据来源和减少网络上的垃圾信息，他们也将因此获得一部分 NCT 奖励。最后，遥测数据用户得以接入一个真正的全球网络，找到他们需要的安全数据，以识别和应对新出现的威胁。

简介

在本白皮书中，我们为普通用户介绍了 PolySwarm 的花蜜通证的一种新用途：作为提供安全相关数据遥测数据的奖励，这些安全相关遥测数据包括：日常电脑使用中遇到的 TLS 证书、DNS 解析 (resolution) 和潜在恶意文件等。虽然上述某些遥测数据源已有反病毒服务商在用户设备上收集，但实施过程中存在着严重的问题，例如：信息是如何被收集的？用户如何获得公平的报酬？最终信息是如何共享的？等等。

通过重新设想这个市场的工作方式，我们可以增加收集的透明度，公平地给市场中的所有参与者发放报酬，以及最重要的是，创建一个更统一的、能更好保护全球用户的安全遥测数据源。

项目目标

统一的遥测数据源

我们在最初的白皮书中，讨论了杀毒软件市场的分裂现状，以及这种分裂怎样给市场上用户带来更糟糕的结果。然而，这种分裂并不仅仅局限于安全扫描服务商的世界：它也影响到安全行业的许多其他领域。我们在构建 PolySwarm 市场时，意识到我们的客户想要得到的各种不同的安全信息常常是已经存在的，但是市场的碎片化导致实际操作中这些信息不可获取。

为了解决这个问题，我们正在建立一个统一的安全遥测数据市场。我们的愿景是打造一个统一的平台，让全世界的用户、安全公司和黑客都可以在这个平台上安全、可靠、公平的分享和访问这些遥测数据。

公平报酬

在当前的市场上，用户向他们的安全服务提供商提供数据是几乎得不到任何回报的。事实上，很多人根本没有意识到这些数据正在被收集。安全公司使用这些信息来探测新型的潜在威胁，但它们的能见度从根本上受到用户数量和地域限制，所以为了得到全面的信息，它们必须从数据转卖人那里购买信息，或设法避开自身的盲区。

通过创建一个市场，让用户能够真正的因提供的有用信息和保护其他用户得到回报，我们能够极大地提高全球安全信息的可用性，并且保证用户的宝贵贡献能够获得合理的回报。同时，安全服务提供商也能从这种模式中大大获益，因为现在他们有办法拓展自己的威胁能见度，而不必与中间人进行交易。

信息收集透明度和安全性

对于任何需要采集用户信息的系统，合乎道德的数据收集是一个绝对要求。我们的市场设计方案十分注重向遥测数据聚合方出售数据的隐私性和安全性，并确保资料被适当的匿名化和保护。通过给予用户对自己提供数据的更多的控制权，并对他们自愿贡献的数据提供奖励，我们希望为整个安全社区创建一个更开放、更有效的数据源。

参与者

遥测数据提供者（Telemetry Providers)

遥测数据提供者即普通用户，他们只需安装一个小的浏览器插件(v1)或监控守护程序(v2)即可加入网络。这些用户可以按照自己的意愿向自己选择的遥测数据聚合方提供自己选择分享的信息。作为回报，这些用户会根据其对网络的贡献的价值而得到报酬。此外，他们还可以在遇到潜在的恶意程序时及早得到预警。

遥测数据用户（Telemetry Consumers)

遥测数据用户是用户数据和聚合者信息洞察服务的主要买家。他们持续使用 NCT 向一家或多家聚合方购买信息查询或数据更新汇总服务。

PolySwarm 平台上专注于网络安全的用户们已对平台上的遥测数据洞察增值服务表示了浓厚的兴趣，此服务的基础则是平台上每天超过 75 万条的恶意软件信息。传统市场上，这些信息都是零散的，没有集中的中央市场及共享机制，分散于反病毒和威胁遥测数据机构中。PolySwarm 协助遥测数据用户更好地获取数据，并能突出恶意软件的来源和行为。通过观察到的 URL 和 IP 的分布以及其他感染点位信息，可以初略定位出目标人群的地理位置。而 DNS 类被动数据可以突出标记新的恶意域名及其他“快速流动”基础设施。

遥测数据聚合者（Aggregators)

遥测数据聚合者处在市场的中心：他们接收遥测数据提供者的数据，经过分析和综合，向用户提供遥测数据的汇总以及从中得到的对新威胁的洞察。聚合者采用 PolySwarm 的去中心化遥测数据模型，能以更低成本、更直接的方式收集更大范围的威胁信息，从而为用户提供更好的遥测数据，并为自身创造更多的机会。

通过为遥测数据提供者的数据提供一个单一的、自动化的、能创造被动收入来源的市场，聚合者可使遥测数据提供者受益。而遥测数据用户则得益于这些数据中所蕴含的洞察，他们既可以从聚合者处得到经过滤的威胁遥测数据动态，同时也能在同一个地方查询海量的遥测数据。

市场设计

这个新市场的 V1 版本设计专注于三个主要的目标：易于参与、平衡激励和最小化链上交易。

遥测数据收集

成为遥测数据提供者参与到网络中是非常简单的，只需要下载和安装 PolySwarm 开发的遥测数据收集程序。我们的 V1 设计专注于为用户提供一个易用的的信息收集方法，其中包含安全合理的隐私默认设置。遥测数据将遵循用户的隐私偏好收集，并采用隐私敏感的数据结构提供给聚合者。

这些数据结构由聚合者以去中心化的方式查询和维护。这样用户可以保有对其数据及其收入的控制权，同时仍然允许聚合者标记遥测数据中的数值，例如 IP、URL 和文件哈希值等。

遥测数据聚合

聚合者有三个主要功能，分别是：从提供者处收集广泛的遥测数据、奖励遥测数据提供者，以及通过分析遥测数据为遥测用户增添价值。因此，聚合者最终交付的是两类服务：信息查询和动态订阅。当用户(a)发起一个动态订阅，或者(b)获得聚合者的数据查询结果时，该聚合者可以赚取 NCT。

聚合者在 PolySwarm 平台上完成注册后，PolySwarm 遥测数据收集软件中会对应增加一个对应该聚合者的用户“数据目的地”选项。在 V1 中，PolySwarm 团队将设计、创建和运营第一个聚合者。我们在下文“贡献者报酬”部分涵盖了聚合者应该如何进行遥测数据奖励的话题，并计划发布公开的实例给到其他聚合者作为起步阶段的参考。

聚合者提供的查询服务很好理解：首先假设，用户已经用 NCT 从聚合者处购买了包含一定查询条数的服务包。用户用遥测数据参数(例如 IP 地址范围)在一到多个聚合者中发起查询。聚合者给出查询结果，并且记录查询者对特定数据的兴趣，以便后续给相关数据提供者计算每期报酬。

同样，聚合者的动态订阅服务也是非常直接的。每隔一段时间，聚合者会收集一定数量的遥测数据，这些数据是安全动态的原材料。例如，在 PolySwarm，我们每天生成一个收录观察到的勒索软件和元数据动态，来帮助我们的用户侦测和拦截可能带来感染的入侵。

作为一个聚合者，我们将通过以下方式为动态服务增添价值：(a) 每日按照在外探测到的感染情况，对威胁进行排名 (b) 将衍生遥测数据及强化的 DNS 和 IP 地址信息附加到样本家族中。

有了威胁等级排名，用户，尤其是网络安全响应团队便可以对任何热门勒索软件发布预警进行优先级排序。而在遥测数据中附加进一步的 IP/DNS 信息，使用户能够有信心的快速、自动地阻止来自恶意软件的命令并控制 (command and control)流量，因为控制基础设施已被多个独立的遥测数据供应商观察到。

动态订阅为网络安全防护者和用户带来了直接的价值，而我们将在下文“提供者报酬”章节中介绍一种新型的抵押模式，以帮助把最有价值的信息置于第一位。

遥测数据使用

网络安全遥测数据对许多行业的客户来说都很有价值，例如：管理安全解决方案提供商(MSSPs)、反病毒服务商、端点检测和响应产品(EDR)提供者，以及企业安全运营中心等。在我们的市场设计中，我们试图捕获这些不同的用户分配给遥测数据的“价值”，来奖励聚合者和广大遥测数据提供者。系统内的价值通过 NCT 从用户向聚合者传递，当聚合者订阅动态或执行按次付费的查询时，NCT 流入各聚合者中。

贡献者报酬

遥测数据提供者报酬

遥测数据提供者获得的报酬取决于他们提供信息的质量，由聚合者根据使用模式来判断。而聚合者会公布他们的整个周期的总奖池总额。在网络的 V1 版中，这种报酬通过聚合者的非公开计算得出，而在 V2 版中，我们期望设计和部署治理机制让聚合者参与者决定奖励的计算公式。这部分设计部分灵感来自于 Uniswap 的流动性常数产品公式，但有一个额外的变化，即随着遥测数据提供者和押注者为聚合者增加价值，他们可以让计算公式得到进化。

每个聚合者都可以实施不同的、独立的奖励策略。首先，以我们自主的 PolySwarm 聚合者的计划详情作为遥测数据奖励计算的例子：

V1 PolySwarm 聚合者将每天获得 X NCT 的资金，该资金将根据 NCT/美元的汇率和活跃参与者的平均数量进行调整。随着其他聚合者的加入，NCT 的总报酬应该增加。

NCT 的奖励在每个时间周期结束时，根据以下公式分配给遥测数据提供者：

$$NCT_t = f(R_p, t, S_p)$$

其中 Rp 代表在该时间段内提供的遥测情报的相关性，t 代表数据提供者持续提供数据的时长，Sp 代表在该遥测数据提供者上押注的 NCT 金额。最初，我们计划将每天用于遥测数据的 NCT 资金的 75% 用于奖励创造了价值的贡献。剩下的 25%分配给贡献者，以鼓励那些可能不是立即产生回报的遥测数据的增长。

奖励公式的结果很简单，代表该时间段内总奖励的百分比份额。在网络的第一个版本中，这个公式将完全由聚合者自己定义，但我们打算在以后的版本中追求更加去中心化的治理。

最初，在上述提到的 V1 版本网络中，相关性参数(Rp)由两个属性决定：

1) PolySwarm 用户/客户的兴趣，和

2) 威胁的严重性

一个提供有价值的遥测数据的用户预计将根据以下公式，从该奖励池中获得 NCT 奖励：

$$R_p = \sum_{i=0}^{n} \frac{1}{Ni} \times W_i$$

其中，*Ni* 是同样提供了匹配遥测数据的其他用户数量，而 Wi 是聚合者分配给这一观测项的权重。请注意，PolySwarm 的聚合者计划用来计算观测项权重的方式，近似于计算在多个时间周期内此遥测数据目标对遥测数据用户和社区的观测价值。最初，这将会是用我们的 PolyScore 和相关性数值进行综合计算的结果，而他们取决于用户的查询和动态订阅情况。

多个周期的评估是尤为重要的，特别是当动态更新的遥测数据在较长时期内保持相关性，或者威胁的严重性持续上升的情况下。2021 年导致 Colonial Pipeline 公司关闭成品油管道的勒索软件 DarkSide，就是这个现象的一个绝佳例子。PolySwarm 早在 2020 年 8 月就检测到了此勒索软件的变种，但是早期已经开始跟踪此软件的“金丝雀”遥测数据服务商应该能在 2021 年 5 月看到其相关性和严重性的猛增。

这就是为什么要将遥测数据提供者贡献时长纳入 NCT 奖励方程的主要原因：在需要获取真正的遥测数据背景来比对一项威胁的历史及当前严重性时，长期的观察是有价值的。

聚合者报酬

聚合者的报酬将从信息查询和动态订阅费用中抽取。对聚合者的用户而言，费用的计算是透明的，占每期奖池中奖励的一定百分比。这些费用激励聚合者用最相关的、精心包装的、专注于特定网络安全领域和垂直行业的遥测数据吸引用户的订阅和查询，例如：针对金融行业提供与银行业相关的威胁遥测数据。

押注报酬

为了帮助防止垃圾信息和更好地分配奖励，系统将提供功能，允许用户可以对包括自己在内的遥测数据提供者身上进行 NCT 押注。NCT 质押为聚合者提供了一个重要的信号，即某信息提供者的可信度，同时为奖励计算公式提供了 *Sp* 值。在每个奖励周期，押注用户会分得遥测数据提供者收益的约 20%作为奖励。然而，押注者承担的风险是，如果某个提供者被发现是恶意的、或提供

了无效的遥测数据信息情况下，聚合者可以向网络提议销毁押注，而押注资金将于遥测数据提供者的市场信任一同归零。

质押奖励由如下公式定义：

$$NCT_s = S_t \times NCT_t \times S_s$$

其中，*St* 是遥测数据提供者希望给到押注者的总收益的百分比，*NCTt* 是遥测数据提供者在这一时期获得的 NCT 总和，而 *Ss* 是当前押注者在总押注中所占的份额。

时间表和评论

我们计划于 2021 年 7 月 19 日发布一份路线图，详细列出本白皮书中讨论的高层次构想的开发时间表。我们欢迎大家通过 info@polyswarm.io 或 PolySwarm Telegram 频道对提出的想法进行讨论和反馈。

总结

这个新的信息交易市场为所有参与者提供了直接的好处。用户对他们的数据有更多的控制权，并为他们提供的价值得到实际的报酬，也会收到关于他们所遇到的威胁的提前预警。聚合者的数据不再受限于自身的安装量，并能通过提供查询计算能力，和验证遥测数据获得 NCT。质押者帮助网络确定最有用的遥测数据来源，并帮助减少网络上的垃圾信息威胁，他们也会因此获得一部分 NCT。最后，用户现在将能够访问一个真正的全球网络，找到他们需要的数据，以识别和打击新出现的威胁。

在 PolySwarm，我们的使命是让全球的安全社区和用户一起抗击恶意软件。通过利用以太坊的全球去中心化网络，我们的新交易市场将极大地推进我们的努力，把这些群体团结在一起，通过赋能（和激励！）每个人来解决这个困难的问题。

免责声明

本文件仅供一般参考之用。它不构成投资建议或购买或出售任何投资的建议或怂恿，也不应被用于评估做出任何投资决定的好处。不应将其作为会计、法律或税务建议，或投资建议的依据。本文反映了作者当前的观点，不代表 PolySwarm 或其附属机构，也不一定反映 PolySwarm、其附属机构或与 PolySwarm 有关的个人的观点。本文所反映的观点可能会有变化而不被更新。