VirusMap 白皮书 1.0

Written by: maldiohead@outlook.com

Twitter: @ma1fan

概述

对于反病毒与威胁情报产业来说，virustotal 为产业提供了最大的样本检索和检测平台，对于整个网络安全领域来说有着重要的作用，形成了厂商，virustotal,普通用之之间的共赢，但是随着谷歌对平台的垄断，厂商往往需要付出很大的代价，才能获取其平台的数据，一个企业账号，需要支付每年 100w 美金(2017 年数据)，对于厂商来说是一笔不小的数目，对于普通用户来说，提交样本，也并没有获取任何的回馈，更不用说，去获取平台的任何数据。我们可以看到谷歌利用其平台的巨大便利性和巨大流量，形成垄断，榨取提交的样本的数据价值，而且并没有回馈社区，这对厂商。

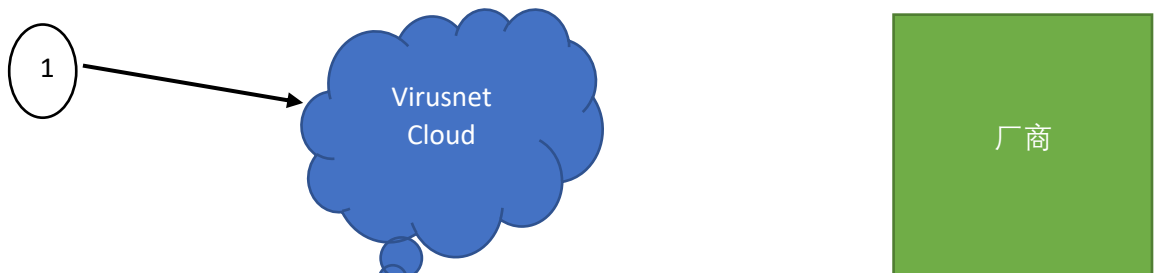
VirusMap，利用区块链技术，将会改变现有的这种模式，让社区真正获得收益，让厂商不必再付出沉重代价，普通用户也可以通过上传样本来获取回馈，从而形成正向的循环，改善现有的状况，打破巨头垄断。

通过 VMT(VirusMap token),普通用户通过提交样本或者威胁情报，从而获取 VMT，作为回报。厂商通过购买 VMT 来获取自己所需的数据，如果厂商提交自己的引擎，成为 VirusMap 超级节点，可以获取 VMT，然后购买用户提交的样本，或者威胁信息。

VirusMap 不仅可以告诉您给定的防病毒解决方案是否将提交的文件检测为恶意文件，还可以显示每个引擎的检测标签（例如 I-Worm.Allaple.gen）。

技术架构

1.0



普通节点

普通节点主要是为了给 VirusMap cloud 提交样本，然后 VirusMap cloud，根据人工智能算法会奖励相应的 VMT 发送给普通节点。形成一次 SSFM（submit sample for minning），普通节点主要包含,web 界面，浏览器插件，移动 app，erc20 钱包等。

任何用户都可以使用其浏览器从计算机中选择文件，然后将其发送到 VirusMap could。 VirusMap 提供了许多文件提交方法，包括主要的公共 Web 界面，本地上传软件，浏览器扩展和 WEB API。在公开可用的提交方法中，Web 界面具有最高的扫描优先级。可以使用基于 HTTP 的公共 API 以任何编程语言编写脚本。

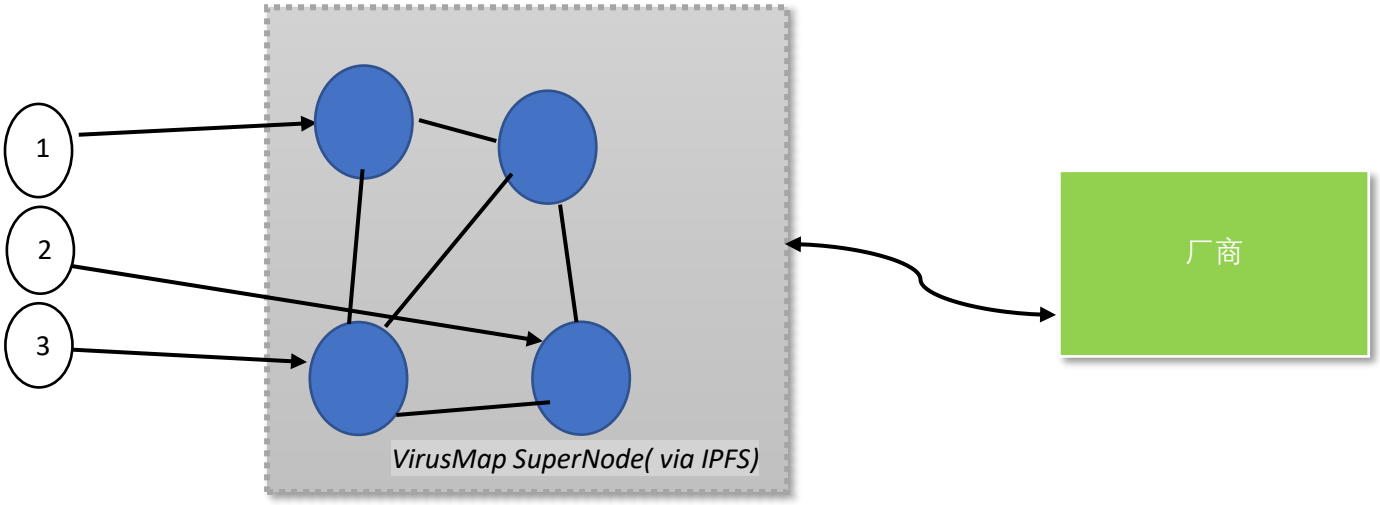
VirusMap Could

virusmap could 主要包含以下功能: 加密存储样本，利用防病毒扫描程序给出样本鉴定结果，大数据处理，获取样本大数据信息，存储样本大数据信息，相应厂商请求并完成(厂商所需样本，威胁情报，样本元数据，等其他大数据信息)请求，收取厂商 VMT 代币，奖励普通节点 VMT 等。

厂商

包括 web 页面，移动 app，厂商通过这些客户端，与超级节点通信，完成购买，请求数据，获取相应数据的过程。

2.0



与 1.0 最大的不同是，virusmap could 演变成 virusmap SuperNode，这些节点有社区投票产生，来使社区更去中心化，更加稳定，不会因为某一个节点崩溃，造成 virusmap 出现 DOS.选出来的超级节点，通过将样本加密存储在 ipfs 节点上，实现数据安全，数据分布式存储。到 2.0 社区回更加壮大，virusmap 网络更加健壮，SSFM 更加合理，厂商费用会更低，样本规模，威胁情报，安全大数据会更丰富，从而促进信息安全领域更加美好，互联网更安全，互联网更去中心化，趋向互联网本来的精神内核。

VirusMap 提供的服务

反病毒扫描结果

反病毒扫描器是用来鉴定文件是否为恶意还是正常程序的主要手段，VirusNet 将不断与各大全球知名防病毒公司合作，更多扫描程序的加入会让 VirusNet 更加强大。

威胁情报

数字技术是当今几乎每个行业的核心。他们提供的自动化和更高的连通性彻底改变了世界的经济和文化形态。但它们也以网络攻击的形式带来了风险。威胁情报是使您能够预防或缓解这些攻击的知识。威胁情报植根于数据中，可提供上下文（例如谁在攻击您，它们的动机和功能是什么以及要在您的系统中寻找哪些妥协指标）来帮助您做出有关安全性的明智决策。

网络威胁情报解决方案可以解决所有这些问题。最好的解决方案使用机器学习来自动化数据收集和处理，与现有解决方案集成，从不同来源获取非结构化数据，然后通过提供折衷指标（IoC）以及策略，技术和程序的上下文来连接点（TTP）的威胁参与者。

VSNT 将通过动态分析，机器学习，以及传统的方式来收集，获取威胁情报，并且普通节点也可以提交威胁情报，来产生威胁情报。为政府，金融公司，大型企业提供服务。

url 检测

url 检测主要是来判断 url 是否包含恶意信息和数据，比如钓鱼网站，仿冒网站，包含恶意代码的网站，挖矿 url 等信息。提前预知潜在的威胁。

样本数据

对于企业，厂商我们将会提供样本数据，提供给一些信息安全公司，大型企业等

我们的愿景

通过区块链，我们不仅可以解决信息安全领域的目前存在的一些技术问题，同时改变了现有的经济模型，从而促进互联网更加趋于平等而不是少数垄断信息安全公司利用互联网数据获利，而忽视数据提供者的利益，我们希望通过 virusmap 让网络安全等级提高一个层次，更加开放，平等，自由。

团队

团队成员在网络安全领域深耕多年，具有丰富的经验和行业顶尖的专家，团队成员来自国内顶级安全公司和团队。

VIRUSMAP TOKEN

我们将发行 VirusMap Token 即 VMT。我们将会发行固定数量的 token。 在 token 销售期间未售出部分的 token 将被销毁。一旦 VirusMap 完成全面发售，这些 token 将可用于购买样本数据及其威胁情报信息。VMT 将成为 VirusMap 网络的关键组件，因此，token 可以被客户用来购买样本数据和威胁情报。 大部分 token 都将分配给节点的矿工（提交样本及威胁情报，及 IPFS 节点），一小部分给开发者和支持者。使用 VirusMap 服务，所有费用将 VMT 计算，未来会根据供需变化而变化。与典型的区块链不同，挖矿将是奖励上传样本及其提供威胁情报信息。因此 Token 的目的是为了促进 VirusMap 网络的增长。形成正向的网络安全经济模型。促进产业，行业持续发展。