VirusMap White Paper 1.0

Write by maldiohead@outlook.com

Twitter: @ma1fan

Overview

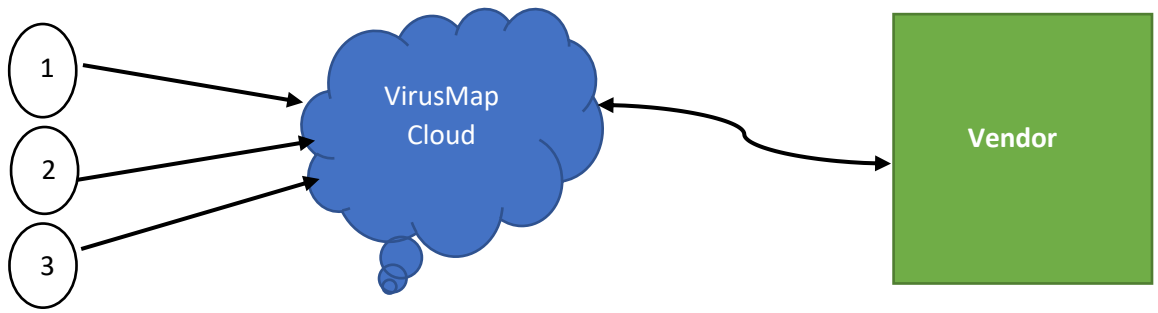
For the anti-virus and threat intelligence industry, virustotal provides the industry with the largest sample retrieval and detection platform, and plays an important role in the entire network security field, forming a win-win situation between manufacturers, virustotal, and common users. However, with Google's monopoly on the platform, manufacturers often need to pay a high price to obtain data on their platform. An enterprise account needs to pay more than $1 million per year (2017 data), which is a lot of money for manufacturers. Number, for ordinary users, submitting samples does not get any feedback, let alone get any data on the platform. We can see that Google takes advantage of the huge convenience and huge traffic of its platform to form a monopoly, squeezing the data value of the submitted samples, and does not give back to the community, which is for the manufacturers.

VirusMap, using blockchain technology, will change the existing model and allow the community to gain real benefits, so that manufacturers no longer have to pay a heavy price. Ordinary users can also get feedback by uploading samples, thus forming a positive cycle. Improve the existing situation and break the monopoly of giants.

Through VMT (VirusMap token), ordinary users can obtain VMT by submitting samples or threat intelligence in return. Manufacturers obtain the data they need by purchasing VMT. If a manufacturer submits its own engine and becomes a VirusMap super node, it can obtain VMT and then purchase samples or threat information submitted by users.

VirusMap can not only tell you whether a given antivirus solution detects the submitted file as malicious, but it can also display the detection label of each engine (for example, I-Worm.Allaple.gen).

Technology Architecture



1.0

Normal node

Ordinary nodes are mainly to submit samples to VirusMap cloud, and VirusMap cloud will reward the corresponding VMT to the ordinary nodes according to the artificial intelligence algorithm. SSFM (submit sample for minning) is formed once. Common nodes mainly include web interface, browser plug-in, mobile app, erc20 wallet, etc.

Any user can use their browser to select a file from the computer and then send it to VirusMap could. VirusMap provides many file submission methods, including the main public web interface, local upload software, browser extensions and WEB API. Among the publicly available submission methods, the web interface has the highest scanning priority. You can write scripts in any programming language using HTTP-based public APIs.

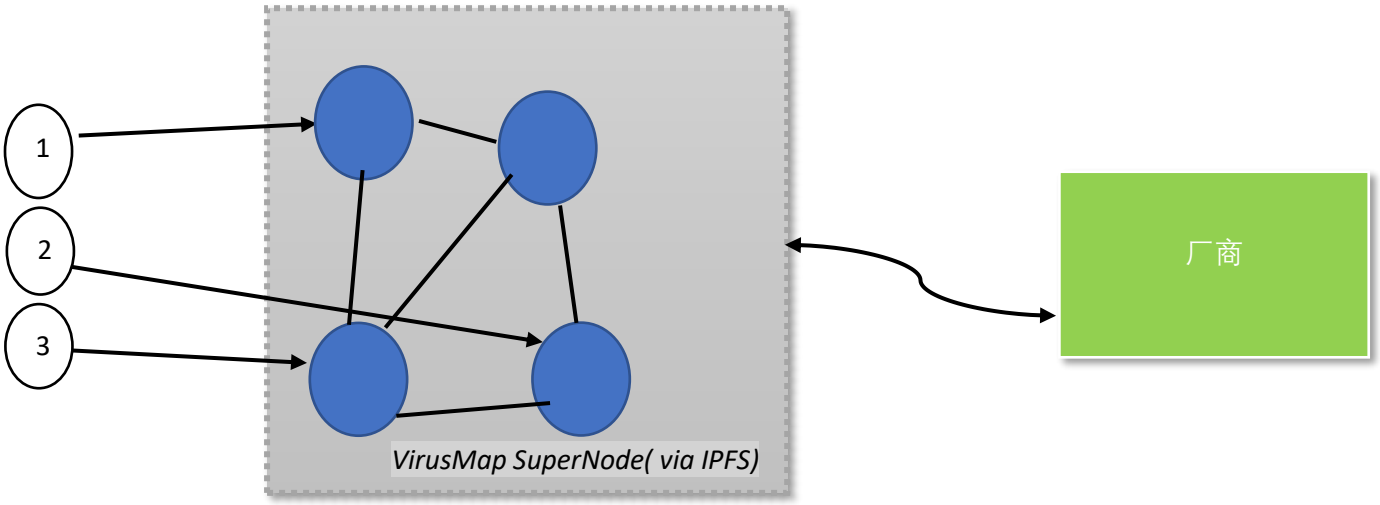
VirusMap Could

The virusmap could mainly include the following functions: encrypting and storing samples, using anti-virus scanning programs to give sample identification results, big data processing, obtaining sample big data information, storing sample big data information, and completing the corresponding manufacturer's request and completion (the samples required by the manufacturer, threat Information, sample metadata, and other big data information) request, collect vendor VMT tokens, reward ordinary nodes VMT, etc.

Vendor

Including web pages, mobile apps, vendors communicate with super nodes through these clients, complete purchases, request data, and obtain corresponding data.

2.0



The biggest difference from 1.0 is that virusmap could evolve into virusmap SuperNode. These nodes are voted by the community to make the community more decentralized and stable, and will not cause virusmap to appear DOS. Supernodes selected by the virusmap due to a node crash. , By encrypting the sample and storing it on the ipfs node, data security and distributed data storage are realized. The 2.0 community will grow stronger, the virusmap network will be more robust, SSFM will be more reasonable, vendor costs will be lower, sample size, threat intelligence, and security big data will be more abundant, thereby promoting a better information security field, a safer Internet, and a better Internet Centralization tends to the original spiritual core of the Internet.

Services provided by VirusMap

Anti-virus scan results

Anti-virus scanner is the main method used to identify whether a file is malicious or a normal program. VirusNet will continue to cooperate with major global anti-virus companies. The addition of more scanners will make VirusNet more powerful.

Threat intelligence

Digital technology is at the core of almost every industry today. The automation and higher connectivity they provided have completely changed the economic and cultural patterns of the world. But they also bring risks in the form of cyber attacks. Threat intelligence is the knowledge that enables you to prevent or mitigate these attacks. Threat intelligence is rooted in data and can provide context (such as who is attacking you, what their motives and functions are, and what compromise indicators to look for in your system) to help you make informed decisions about security.

Cyber threat intelligence solutions can solve all these problems. The best solutions use machine learning to automate data collection and processing, integrate with existing solutions, obtain unstructured data from different sources, and then connect the points by providing indicators of compromise (IoC) and the context of strategies, technologies, and procedures (TTP) threat actors.

VSNT will collect and obtain threat intelligence through dynamic analysis, machine learning, and traditional methods, and ordinary nodes can also submit threat intelligence to generate threat intelligence. Provide services for the government, financial companies, and large enterprises.

url detection

URL detection is mainly to determine whether the URL contains malicious information and data, such as phishing websites, counterfeit websites, websites containing malicious code, mining URLs and other information. Anticipate potential threats in advance.

sample

For enterprises, manufacturers will provide sample data to some information security companies, large enterprises, etc.

Our vision

Through the blockchain, we can not only solve some of the current technical problems in the information security field, but also change the existing economic model, thereby promoting the Internet to become more equal instead of a few monopolistic information security companies using Internet data for profit. Ignoring the interests of data providers, we hope that through virusmap, the network security level will be raised to a level, more open, equal, and free.

team

The team members have been deeply involved in the field of network security for many years, and they have rich experience and top experts in the industry. The team members come from top domestic security companies and teams.

VIRUSMAP TOKEN

We will issue VirusMap Token or VMT. We will issue a fixed number of tokens. During the token sale period, the unsold part of the token will be destroyed. Once VirusMap is fully sold, these tokens will be used to purchase sample data and threat intelligence information. VMT will become a key component of the VirusMap network. Therefore, the token can be used by customers to purchase sample data and threat intelligence. Most of the tokens will be allocated to node miners (submitting samples and threat intelligence, and IPFS nodes), and a small portion will be given to developers and supporters. Using VirusMap service, all fees will be calculated by VMT and will change according to changes in supply and demand in the future. Unlike a typical blockchain, mining will reward the upload of samples and provide threat intelligence information. Therefore, the purpose of Token is to promote the growth of the VirusMap network. Form a positive economic model of network security. Promote the industry, the industry continues to develop.