A Survey of Network Flow Analysis for malware detection

Sameera Bammidi#1, Jash Pithadia#2

*Department of Computer Science, Volegnau School of Engineering*

*George Mason University*

*Fairfax, VA, USA*

1sbammidi@masonlive.gmu.edu

2jpithadi@masonlive.gmu.edu

***Abstract—* In this article, we presented a survey of network flow analysis for malware detection in various realms. DNS spoofing, Denial of Service and Malvertisements are some of them. We focused on network flow analysis tools for detection of malware, identification of malware distribution infrastructure and its dynamics. An overview of flow analysis for malware detection in different realms like Peer to Peer networks, Android malware, and Botnet detection and Internet of Things. We also discussed how malware attacks could be prevented by following some preventive measures.**

1. MOTIVATION

While learning about computer networking – the protocols and infrastructure that allows computers to communicate and all the things that depend on the internet, we also learned how security is an important aspect of it. All the commerce and applications that depend on the internet operate with the assumption of enough security that gains outweigh risks. However, security is a constantly evolving dimension. It is a game of catching up with the latest threats where both the attacks and the prevention methods keep getting more complex. From our initial search for literature in the aspect of security from a networking perspective we found that “flow” is a concept that is present in many levels – i.e., when communications are analyzed for finding malicious intent it is better to isolate flows from all the communications which represent data at the right granularity for analysis. We present in this paper how the concept of flow is present in several seemingly different works in malware detection.

1. INTRODUCTION [9]

*Network flow*, also known as traffic flow or packet flow is a sequence of packets sent from a source to any desired destination. Flow is also defined as a set of packets traversing certain point in the network during a certain time. *Flow*, also called a five-tuple IP flow, is a series of packets which share the same source IP address and destination IP address, source port and destination port, and IP protocol. All traffic in a flow is in the same direction.

A *flow record* is a summary of information about flow. It has the information about hosts communicating with each other, how the traffic was transmitted, and other necessary information about the network conversation. Flow records tell us what kind of traffic is filling the internet, what the client end system is doing, and what types of errors are reaching the server.

A *flow analysis* system collects flow information and then creates and reports statistics from the flow updates. It gives us a system to search, filter, and print flow information.

We can capture, analyze, and reconstruct everything that traverses the network, i.e., which websites user visits, what files the user downloads, what the user transmits back to the site, and any usernames and passwords used in the exchange. Flow records do not contain this data; they simply tell the network administrator that a client visited a website running at which IP address, how many connections the user made to that site, how much data was exchanged, but not the contents of those exchanges.

A typical flow-based management system has three components:

1. Sensor (or sensors),
2. Collector, and
3. Reporting system.

These components can be combined as well.

A *sensor*, also known as a probe listens to the network and captures traffic data. The sensor can be a switch, router, firewall with integrated flow export capability, or a piece of software listening to an Ethernet tap, etc. The sensor tracks network connections. Once a connection is established, or a timeout is reached, the *sensor* transmits the data.

A *collector*, which is a software, receives records from the sensor and writes them to the disk. The collector is a critical piece of flow-based management infrastructure.

The *reporting system* reads the collector files and produces human-friendly reports. The reporting system must understand the file format used by the collector.

Network flow analysis is useful in load planning, network security such as *malware detection,* i.e., detecting if the flow is directed to blacklisted IP addresses or whitelisted ones, accounting, forensics, and counterterrorism.

Malware: *Malware* (which is short for Malicious software) is a set of computer programs, which is designed to subvert and damage the user’s computers, without user’s consent. Malware is the generalized term for various threats to an end system. A common example of malware are viruses, worms, torjan horses, keyloggers, spyware, rootkits, etc. These can be of contagious threat, masked threat or financial threat to the end system users. [11]

1. FLOW ANALYSIS VS PACKET ANALYSIS [1]

*Flow analysis* is done at the networking layer. As mentioned earlier, a flow record contains typically the IP addresses of two hosts communicating with each other, their network ports, the network protocol they adapt, the amount of data sent through this connection, time when the flow has occurred and a few miscellaneous flags. Data traversing the routers and switches is captured and analyzed. It is easy to set the tracking up on the routers, switches, and other devices that operate at networking layer. It doesn’t require cabling. The presence of malware such as viruses, worms, and DDoS (Distributed denial of Service) attack on a network can be detected by analyzing these exported *flow records* and looking for anomalies.

*Packet analysis* is associated with mirrored ports where exact packets are mirrored. It is based on the raw packets which are captured while traversing the network links. Packets can be captured by configuring a spanning port at devices such as router or switch or installing a network tap directly connecting the cabling infrastructure. Metadata of app or website names is extracted with deep packet inspection(DPI). In contrast to the flow data, packet data contains information about what is contained in the *packet payloads*. Packet analyzers can see the actual packets that are involved in the host to host conversations even when dynamic port numbers are used.

Following are some advantages of network flows: [15]

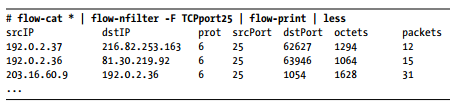
* Without investing time to analyze large packets (by sniffing and storing every data), flow reports reveal detailed information about a network conversation.
* When the connection is encrypted, a flow analyzer can recognize when, where and how much data went by looking at the flow data.
* Previous flows can be used as a baseline for detecting dangerous and anomalous traffic.
* The source (such as router or switch) that generates the flow data is an uncompromised source which is not in the attacker’s target.
* Data can be captured from various points on the network which allows a distributed view. This can be used to determine how an attack began and how deep the containment is.

1. PREPARATION BEFORE ANALYZING THE FLOWS [15]

To deal with a network flow, flow should be enabled and captured with the information needed by the flow analyzer. For capturing a flow, a collector should be installed, configured and tuned for the environment. Then it can be used to assist the incidents.

A collector should be selected by considering factors such as its flexibility, scalability, performance, and cost. Then it should be installed and configured on a router to generate flows. It should be ensured that the flows are being received by the flow collector for a network device (switch or router).  After it is made sure that the flow collector is functional, a baseline should be established from the normal network traffic. Establishing a baseline is important for the flow analyzers to understand.

Following is the screenshot of a flow record which shows only the flows with the protocol 6 (Transport Control Protocol) and the source port is 25:



1. ANALYZING NETWORK FLOWS TO IDENTIFY INCIDENTS [15]

        After collecting the data from different critical points in the network infrastructure, an analyzer uses flow analysis techniques to detect malware infected end systems and systems that are compromised and participating in a botnet. Flows can also reveal attackers’ targets or even better, the attackers. Knowing information about a security breach narrows down an approach to proceed with the attack.

1. *Hunting for bots*

Rise of botnets is one of the biggest security threats to the recent information security. Using the compromised end systems in a botnet, attackers can command account numbers, passwords, send spam messages or launch Distributed Denial of Service attacks. With a properly deployed network flow collection, bot-infected systems can be detected. Using the signs left by the bots, analyzers can identify bots in the network and limit their effect on the damage.

1. *Spotting other malware infestations*

    Home PCs being infected with a wide range of malware can be identified using the network flows. Viruses and worms which typically spread spam through mass e-mails (use Simple Mail Transfer Protocol) and spread infection to other end systems can also be detected using network flow analysis.

1. *Finding attackers and their targets*

    After initially identifying potential security threats through numerous sources, the deployment of flow collection can help network flow analyzers to define the full scope of the attack. This helps in the containment of further attacks.

1. *Pinpointing potential data leaks*

        Using the network flow records which have the data of all conversions among the hosts in a network, analyzers can establish a baseline for normal network activity. This helps in identifying the abnormalities in the network and identifying the security breach.

1. *Use of network flows while eradicating and controlling the malware*

Using network flows information necessary for the containment can be revealed, like:

* What ports or addresses to be firewalled,
* What network segments need incident handlers’ attention, or
* Which DNS names to blacklist.

        They are also useful while cleaning up the mess caused by the attackers. Flows can be generated and analyzed to verify the cleanup progress.

1. NETWORK FLOW ANALYSIS FOR MALWARE DETECTION IN DIFFERENT REALMS
2. *Network flow analysis for malware detection in Android*

There are two approaches to mobile malware detection as follows:

*Host-based*

This approach uses limited resources and leads to drainage of battery. Example: The malware resides inside the host(android device) and may or may not be injected via an application. The host-based approach uses limited resources such as API for contacts, Storage or hardware features that can cause harm to the system.

*Network based*

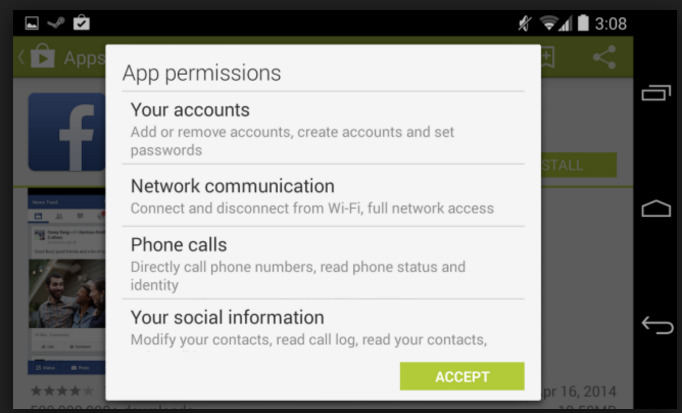
This approach is unable for malware detection where malware does not create network traffic. The network traffic is analyzed, and an analysis of network behavior is tracked to the back-end server. Example: The application uses the Internet has interaction with the back-end sever. This approach tracks the network based traffic flown from the application to the back-end server.

*Usage of public sandbox for network flow analysis* [22]

A sandbox is basically a security mechanism for running and debugging untrusted program or code. The use of a public sandbox will generate an online report. By using a sandbox, you will get an online report that will give you a detailed overview of the network requests. We will discuss two types of a sandbox, by using the public sandbox, the online report gives you an overview of the detailed network requests.

Following are the two types of sandbox:

1. *VirusTotal* is a free/paid subsidiary of Google. VirusTotal is used for analysis of files and URLs. VirusTotal provides interface and API. VirusTotal checks if there is any malware uploaded on the device. Functions of VirusTotal and the detection result is supported by antivirus engines. Detailed network requests are obtained by the online report.
2. *Anubis* is a product by a company called International Secure Systems Lab. Same as VirusTotal it used for analysis of files and URLs. It supports two types of files .exe(Windows) and. apk (Android). It is different from VirusTotal in a way that Anubis provides network capture in pcap format and detects whether malware is communicating with any specific device path.



**Figure 1**

Following are top few kinds of malware which can infect an android device:

1. Ztorg: This is a trojan which used the Android root permission and downloads applications on the mobile phone without user’s knowledge.

2. Triada: This is a modular backdoor which gives super-user privileges to the downloaded malware. Triada is also used as spoofing URLs. Triada used Linux debugging tools and used its Dynamic Link Library into the Android processes. These processes are used to open any standard Android browser. When the user opens the browser, user is directed from standard web page or search engine to malicious website.

3. HummingBad: This Android malware is used by enterprises, and it installs applications which are used for stealing credentials

Application level:

* Malware can be injected while downloading apps from Google play store or 3rd party app stores. The user should be careful while downloading apps from application stores.
* We can see that from figure 1 while downloading the app the user accepts the list of permissions listed by the developer. The device might be hacked if the fake developer gets essential information from the mobile device by misusing the permissions.
* The user device can be misused or hacked by several different types of malware functions such as Android activity monitoring and data retrieval, unauthorized dialing, breach of contacts, storage, payments or by using unauthorized network

Per a study by Juniper Networks, malware on the Android computing platform grew 3,325 percent in 2011 alone. [23]

1. *Network flow analysis for malware detection in P2P*

P2P (Peer to Peer) is a distributed networking application architecture. Communication and data are exchanged between two hosts via a network.

There are two types of P2P applications as follows:

1. General purpose P2P, example BitTorrent.
2. 2.Specific purpose P2P, example, skype and Spotify.

Network flow analysis in P2P includes a research which comprises of following data sources

1. Payload Analysis: Analysis of the actual data is important, and the payload is part of transmitted data, and it consists of the actual message which is intended for the user. Malware resides in the payload, and it has an overhead code which is used for spreading itself or avoiding deletion.
2. Geolocation of P2P network: Geolocation is used to determine the physical location of the user. Websites use this location to provide better service which can be used by some attacker.
3. Reputation: The reputation of point in P2P network, for example, an email id can be checked by validating the email id. If a particular email id is present in public blacklist or spam list, then interaction with this email id should be avoided.
4. *Botnet detection*

* A botnet is a network of computers that are infected by malware and controlled without the knowledge of the user.
* Many Network devices are not protected. Network devices such as routers, TV, cameras should be protected; Netflow can monitor all such devices in a network. We can find network behavior analysis using Netflow.
* Automatic algorithms are used by botnets throughout their life cycle to perform various tasks.
* Some of the bot families such as IRC-based, HTTP based and DNS-based have specific characteristics and how bots react to those instructions.
* A botnet is a group of hijacked PCs, which are employed under command and control mechanism administered by a bot master. The botnet has evolved from IRC(Internet Relay Chat) based centralized botnet to using common protocols such as HTTP with decentralized architectures and then peer-to-peer designs. IRC packets are unencrypted and have a long period in transmission. This is the reason why botnets have evolved from IRC. [25]

1. *Web Security:*

* Web security deals with providing security to websites, web applications and web services.
* Small businesses and large corporations use websites for various purposes. Attacks on any website can be made with different motives depending on the security of the website.
* Website monitoring and traffic analysis are essential to tackle these attacks.

Resources needed for network flow analysis in web security are firewalls and anti-malware software.

1. DIFFERENT TOOLS USED FOR NETWORK FLOW ANALYSIS

There are three major types of network flow analysis tools

* SNMP (Simple Network Management Protocol) is mainly used for remote management and configuration.
* A packet sniffer is used where a device is attached.
* NetFlow-like information is very useful for detailed analysis but has such as high cost and privacy concerns.

We will discuss few popular tools for network traffic flow monitoring and analysis

1. Netflow

* Netflow designed by Cisco is used to generate network flow records.
* These records can be exported in UDP (User Datagram Protocol) or SCTP (Stream Control Transmission Protocol) packets to NetFlow collectors.
* The network flow information obtained from Netflow is useful in understanding the network behavior.
* The popular flow tools used by Netflow are cflowd and flowd. [26]

2. Tcpdump

* tcpdump is used as a packet analyser and is used as a common command line argument.
* User can display TCP/IP packets transmitted or received using Tcpdump.
* Tcpdump can read packets from network interface card and write packets to the output file. It can also use saved packet file for this purpose.
* Consider a user with privilege to a router or gateway. If Telnet or HTTP traffic passes through this router or gateway, the user can use tcpdump to view many details such as login credentials, websites views by the user and any unencrypted data flowing through the traffic.

3. Pcap

* pcap (packet capture) has an application programming interface(API) for capturing network traffic. -Unix-like systems use pcap in the libpcap library whereas Windows uses WinPcap which is a port of libpcap.
* Softwares that analyse and monitor data traffic over the network capture packets using libpcap/ WinPcap. -Recent versions also allow transmission of packets on a network at the link layer. They also fetch a list of network interfaces for possible use with libpcap or WinPcap.

4. AutoFocus

* AutoFocus is used for traffic analysis and visualization.
* AutoFocus is used to analyze the traffic pattern. It is also used to provide reports which are measured in bytes, packets and flows and time series plots.

5. Fluxoscope

* Fluxoscope is used to collect accounting data for network flow analysis.
* Fluxoscope is used in the offline and real-time analysis of report generation and graphical representation based on time.

6.FlowScan

* It is used to generate the online report in HTTP format.
* Flowscan is used for UDP data. IT  receives UDP NetFlow data from routers and passes them to "cflowd," which writes them to storage disks.
* FlowScan deals with buffer management and thus it helps with a very high traffic and flood-based DOS attack.

1. TAXONOMY

There are numerous network traffic analysis and monitoring tools available for free as well as for commercial use. These can be classified into following categories:

1. Free Tools
   * Hardware or software on which the tool runs.
   * The input to the tool and output from the tool.
   * Activity performed by the tool: monitors, captures or analyses the flow.
   * Whether functions online (Real time) or offline.
2. Commercial Tools
   * Primary use.
   * Operating system on which it runs.
   * Price range.

A detailed survey is represented in a table format present in the following link: <http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors3.pdf> [6]

Following are few of the commercial tools used for netflow reporting:

TABLE I

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Product Name | Primary Use | Primary User | Operating System | Starting Price Range |
| Cisco NetFlow  Collector | Traffic Analysis | Enterprise, Service  Provider | Linux, Solaris | Medium |
| Cisco CS-Mars | Security Monitoring | Enterprise, SMB (Server Message Block) | Linux | Medium |
| AdventNet | Traffic Analysis | Enterprise, SMB | Windows | Low |
| Arbor Networks | Security/ Traffic Analysis | Enterprise, Service Provider | BSD | High |
| CA Software | Traffic Analysis | Enterprise, Service Provider | Windows | High |
| HP | Traffic Analysis | Enterprise, Service Provider | Linux, Solaris | High |

1. CURRENT RESEARCH

Network flow analysis is used for several reasons such as policy violation, bot nets, malware in IoT devices, etc. In order to protect the network there is research going on several domains for network flow analysis in several models such as P2P, client side or remote device location. Network flow analysis is very useful to determine many aspects of a network such as availability, security, performance capability and integrity.

*A. IoT and Network flow analysis*

The number of devices connected to the internet was 25 billion in 2015, and it might increase to 50 billion in 2020 as estimated by CISCO

* We have seen an increase in the growth of IoT devices and also a growth in DDoS attacks.
* Botnets usually are faced with DDoS attacks. The hacker uses botnets and floods a website with tremendous traffic that the website crashes
* In October 2016 Dyn DNS, this internet performance management company was under DDoS attack.
* This company manages smart devices. But these smart devices such as cameras, surveillance cameras, thermostats all the IoT devices were hacked.
* One of the easiest targets for hacking are PCs for DDoS attacks.
* PCs are mostly turned into "bots" for DDoS attacks.
* The fact about several of these IoT devices is that they don’t run any traditional security software for protection and thus they are easy targets for hackers and get converted to bots.
* Recently Cisco and Symantec are said to be a prospective buyer for FireEye which has a partnership with ForeScout which is a network security tools and management company to counter IoT-based attacks.

*B. TLS and Network flow analysis*

* The TLS connection is secure, and the messages flowing at Transport layer are encrypted.TLS uses symmetric key cryptography to ensure the data is encrypted. But still, by using machine learning and using classifiers, we can detect malware without exposing client and sever.
* At the Transport layer, messages cannot be analyzed using network flow analysis tools.TLS has its own features which can be employed for network flow analysis for malware detection. The messages are encrypted at the transport layer. While we cannot analyze the data flow at TLS but there some observable attributes which can be used for analysis of messages at Transport layer.
* To identify threats in network flow analysis, flow-based metadata. This flow-based metadata can give us high level information of the flow such as number of packets and bytes. This high level information is typically exported to Netflow like tools.[28]

*C. Network Behavior Anomaly Detection(NBDA) and Network flow analysis*

* NBDA can be used by network flow analysis tools. NBDA can be a real time analysis and is continuously monitoring the network traffic.
* NBDA monitors all the attributes in real time and triggers if there is any threat to the network.
* NBDA can be used along with a firewall and other tools and applications which can enhance the network flow analysis.
* Some of the commercial products for network analysis are as follows:

1. [NetFlow](https://en.wikipedia.org/wiki/NetFlow) - FlowNBA
2. J[uniper Networks](https://en.wikipedia.org/wiki/Juniper_Networks) - STRM (Security Threat Response Manager)
3. [Lastline](https://en.wikipedia.org/wiki/Lastline)
4. [McAfee](https://en.wikipedia.org/wiki/McAfee) - McAfee Network Threat Behavior Analysis
5. MALWARE DISTRIBUTION INFRASTRUCTURE, THEIR DYNAMICS, AND THEIR PREVENTION

Malware can be distributed to the end systems in many ways. Following are few popular ways in which end systems can be attacked by the attackers, and their prevention:

1. **DNS Spoofing**

*DNS spoofing* is a technique where a malicious party impersonates the DNS (Domain Name System) server and reroutes a specific domain name to a different IP address. Attacker intercepts the outgoing DNS request and sends back a response with a spoofed IP address.

When a vulnerable user attempts to browse to a website residing at legitimate IP address, the packets are sent to a fake IP address with the same browser name created by the attacker to steal the user’s confidential information.

Examples of spoofed webpages include banking websites, e-mail web pages, etc. These spoofing attacks are usually made to spread viruses and worms and cache the attacked user’s confidential information. [18], [19]

***Consequences***

Attackers can continue to breach the security of vulnerable users for an extended period without being noticed especially in the case of competing companies. Attackers might launch a product in the market with similar properties as that of the other competing businesses that may destroy their opportunity to be creative. They cause economic and security threats which are not yet realized by many innocent users. [20]

***Prevention***

To prevent the sources of Internet attacks, some of the measures we can follow are:

* Packet filtering: Use packet filters to inspects traversing through a network. They can be useful in the prevention of the spoofing attack since they block packets with conflicting source address information.
* Avoid trust relationships which use IP addresses for authentication.
* Use spoofing detection softwares like XArp, intrusion detection systems(IDS) and intrusion prevention systems(IPS).
* Use secure technology like DNSSEC which allows only digitally signed DNS records to be published on DNS servers.
* Encrypt data when sending and authenticating that the data is received.

1. **Malvertising**

Malvertising is injecting malware into the legitimate online advertisements. The infected internet advertisements are called malvertisements which can infect the current end systems with malware. Compromised computers are used to create powerful [botnets](http://searchsecurity.techtarget.com/definition/botnet) that can be used to carry out any illegal activity. [12]

Malvertisements which are displayed on a webpage are of two types:

***Legitimate advertisements:***

Malvertisers (Criminals who inject malware into the ads) initially place a good amount of malware-free advertisements on a reputed and trusted website. In order to establish a good reputation and gain their confidence, the malvertisers leave them alone for a long time. After several months of stalling, the malvertiser will inject a malicious [payload](http://searchsecurity.techtarget.com/definition/payload) into the advertisement, and infect as many computers as possible within a short period before any action is taken on either removing the malicious code or discontinuing the ad. This kind of attack is often run on the websites that run third-party advertisements.

***Pop-up advertisements:***

Pop-up advertisements deliver a malicious payload as soon as the viewer opens the webpage containing the advertisement with malware. When the viewer sometimes chooses to click on the “X” symbol to close the pop-up add and the malware will be executed. By sneaking into popular syndicated online ad services, malvertisers can infect thousands of sites at a time.

***Prevention***

Following are some measures we can follow to protect ourselves against the malvertisers: [21]

* *Enable Click-to-Play Plug-ins*: When a web page containing a Flash or Java object is visited, it won’t run automatically unless it is clicked. This protects the users from being attacked since most of the malvertisers use these plug-ins. When a *click-to-play* plug-in is enabled, the browser loads a placeholder image which when clicked downloads the actual content.
* Uninstall or disable unwanted browser plug-ins. This reduces the user’s attack surface and reduces the chance of attackers to target potentially vulnerable software.
* Update the plug-ins regularly to make sure the security patches are installed on the end system. Google Chrome, Microsoft Edge, Internet Explorer on Windows 8, 8.1, and 10 automatically update Adobe Flash. Adobe Flash should be set to automatically update on the Internet Explorer on Windows 7, Mozilla Firefox, Opera, and Safari.
* Keep the web browser updated and do not disable automatic updates. Activate windows update on Internet Explorer.

1. **Denial of Service Attack** [18, 26, 27]

        DoS (Denial of Service) attack is an incident when an attacker tries to prevent a user from accessing websites, email, online banking, and other online accounts. When the user types a URL to access a website by sending a request to the server’s webpage, the website cannot process the request.

This happens since the attacker floods the network by overloading the server with requests.

        Also, the attackers consume the space of user’s e-mail account by sending a huge number of spam e-mails or large messages to the user’s account. This prevents the user to receive any legitimate emails.

        A distributed DoS (DDoS) is a process where the attacker launches multiple attacks from many vulnerable end systems on a legitimate server.

***Determining an attack*** [19, 20]

Following are few symptoms which determine if the users end system is under DoS attack.

* Slow performance of the network while accessing webpages or opening files.
* Any website is unavailable.
* Unable to access any legitimate internet site.
* Anomalous increase of spam in the user’s e-mail.
* These symptoms may be seen although there is not a DoS attack but because of network problems or network maintenance.

***Prevention***

* Install Anti-virus software.
* Install firewall and configure the settings to restrict the incoming and outgoing traffic.
* Apply filters in e-mail accounts to restrict the unwanted traffic.
* Contact the network administrators if there is a problem in accessing a legitimate website or opening a file. This indicates that either the user’s end system or the network on which it is might be under attack. [21]

1. **Blacklisted URLs**

Blacklisted URLs are those which are already detected as websites which are malicious. Following are few examples:

|  |
| --- |
| Fortinet's Web Filter / fortiguard.com |
| MDL / malwaredomainlist.com |
| DNS-BH / malwaredomains.com |
| mnemonic secure DNS / mnemonic.no |
| OpenPhish / openphish.com |
| PhishTank / phishtank.com |
| Spamhaus DBL / spamhaus.org |

There are many websites (e.g.: <http://urlquery.net/>, https://developers.google.com/safe-browsing/v4/lookup-api) which detect and analyse the blacklisted websites. We can use them to find out if a website we are trying request is safe or not.

Following is report for a movie website (<http://www.thiruttuvcd.biz/movie/>) where we detected malicious website using urlquery.net:

* Settings used by the urlquery developers to find out transactions and detect malicious websites:

TABLE II

|  |  |
| --- | --- |
| UserAgent | Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13 |
| Access Level | Public |

* Intrusion detection systems used by the urlquery website are Snort and Suricata.
* Following details are given during verification with the blacklisted websites:

Blacklists: Fortinet’s Web Filter

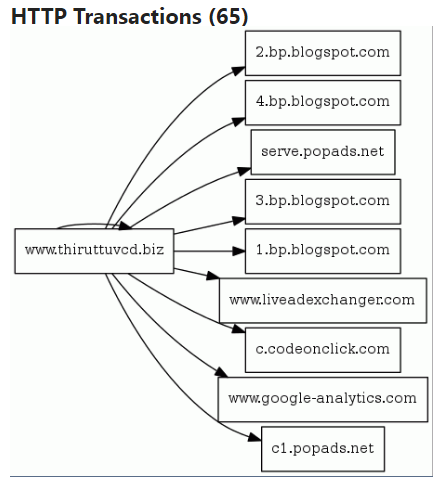
Added / Verified: 2016-11-24

Severity: 2

Host: [www.liveadexchanger.com/a/display.php?r=264348](http://www.liveadexchanger.com/a/display.php?r=264348)

Comment: Malware

* The websites which our request will be directed to, after sending the request.



1. CONCLUSION

In this paper, we have discussed about how the concept of flow is present in several seemingly different works in malware detection. Various tools can be used to capture an analyze network flows. There are few limitations for the tools that are currently deployed. Flows can be used for detection, containment and eradication of the malware. Attackers can distribute the malware in three popular ways: DoS attack, malvertisements and DNS spoofing. These attacks can be prevented by following some measures which are mentioned in the paper.

REFERENCES

1. Flow Analysis vs Packet Analysis

<https://www.netfort.com/wp-content/uploads/PDF/WhitePapers/NetFlow-Vs-Packet-Analysis-What-Should-You-Choose.pdf>

1. Monitoring Network Traffic for Android Devices

<https://www.sans.org/reading-room/whitepapers/detection/monitoring-network-traffic-android-devices-34097>

1. Detecting Malware P2P Traffic Using Network Flow and DNS Analysis

<http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51184>

1. WATERING HOLES AND MALVERTISING: UNCOVERING THE ROOT CAUSE OF COMPROMISE

<https://www.fireeye.com/blog/threat-research/2015/09/part-1-watering-holes-and-malvertising-uncovering-the-root.html>

1. Why NetFlow is not a web usage tracker

<http://unroutable.blogspot.com/2012/04/why-netflow-isnt-web-usage-tracker.html>

1. A Summary of Network Traffic Monitoring and Analysis Techniques

<http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors3.pdf>

1. Network Flow Analysis

<https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-potter.pdf>

1. Flow Based Algorithm for Malware Traffic Detection by Mirosław Skrzewski

<http://link.springer.com/chapter/10.1007%2F978-3-642-21771-5_29>

1. Network Flow Analysis

<http://choonsiong.com/public/books/Network%20Flow%20Analysis.pdf>

1. Detecting Malware P2P Traffic Using Network Flow and DNS Analysis

<http://www.cert.org/flocon/2013/presentations/jerrim-john-detecting-malware.pdf>

1. Malware Tutorial: Learn About Malware, Vulnerabilities and How to Avoid Malware

<https://www.veracode.com/security/malware>

1. malvertisement (malicious advertisement or malvertising)

<http://searchsecurity.techtarget.com/definition/malvertisement-malicious-advertisement-or-malvertising>

1. Improve the security of your application

<https://www.veracode.com/security/mobile-code-security>

1. A Survey of Network Traffic Monitoring and Analysis Tools

<http://www.cs.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors3/>

1. Shedding Light on Security Incidents Using Network Flows

<https://www.sans.org/reading-room/whitepapers/networkdevs/shedding-light-security-incidents-network-flows-33935>

1. Deciphering Malware’s use of TLS (without Decryption)

<https://arxiv.org/pdf/1607.01639v1.pdf>

1. Malware - definition, history and classification

<http://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/malware-definition,-history-and-classification.aspx>

1. DNS Spoofing

<https://www.menandmice.com/resources/dns-spoofing/>

1. Spoofing Attack: IP, DNS & ARP | Veracode

<https://www.veracode.com/security/spoofing-attack>

1. What is DNS Spoofing?

<http://www.securitysupervisor.com/security-q-a/network-security/195-what-is-dns-spoofing>

1. What is Malvertising and How Do You Protect Yourself?

<http://www.howtogeek.com/227205/what-is-malvertising-and-how-do-you-protect-yourself/>

1. Towards a framework for network based malware detection system

<http://www.ieee-security.org/TC/SP2014/posters/CARRA.pdf>

1. Malware Tutorial: Learn About Malware, Vulnerabilities and How to Avoid Malware

<https://www.veracode.com/security/malware>

1. WindowsNetworking.com What is passive DNS?

<http://www.windowsnetworking.com/blogs/chetcuti/security/what-passive-dns.html>

1. An enhanced model for network flow based botnet detection

<http://crpit.com/confpapers/CRPITV159Wijesinghe.pdf>

1. Understanding Denial-of-Service Attacks

<https://www.us-cert.gov/ncas/tips/ST04-015>

1. denial of service (DoS)

<http://searchsoftwarequality.techtarget.com/definition/denial-of-service>

1. Deciphering Malware’s use of TLS (without Decryption)

<https://arxiv.org/pdf/1607.01639v1.pdf>0