ThreatBook
微步在线

Threat Detection Platform - TDP Product White Paper

2021 ThreatBook

微步在线科技有限公司
LEADER IN THREAT DETECTION AND RESPONSE

1.0 Full traffic Analysis and Storage

1.1 Traffic Analysis and Storage

1.1.1 Technology Architecture

In the process of analyzing the source of network threats, especially external attack events, in addition to the attack alert behavior itself, all other network behaviors of the attacker before and after the alert is triggered also have extremely high analytical value.

Based on this, security operations personnel can study and judge the attacker's intentions, techniques and ideas, find weak joints in security tactics, and effectively take prevention and improvement themselves.

However, in a high-traffic scenario, a full-traffic record of the smallest detail will leave a lot of useless information, causing the really useful logs to be overwritten due to insufficient storage space during post-event review and analysis.

TDP innovatively adopts a dynamic hierarchical storage strategy. Through comprehensive consideration of IP historical threat activities and intelligence reputation data, the dynamic classification can determine the full-traffic storage mode of each IP address, and record the original logs and original traffic packets (PCAP) for certain attack behaviors, also record the original logs of the full-traffic for suspicious and malicious IPs, and only record the summary of the network activities of normal IPs. It will improve the utilization efficiency of storage space and save valuable information for a longer period of time, on the premise of ensuring the demand for full traffic analysis and traceability.

Analysis and standardization modules： The data to be detected and asset information accessed by the detection module will enter the analysis and standardization module. In this module, traffic data and log data will be further analyzed into standard format and enriched with asset data. Part of the asset data comes from the data connected with the users of the input module, and the other part comes from the assets automatically identified from the traffic in the analysis and standardization module.

Detection module: The data processed by the analysis and standardization module is called metadata. The metadata will enter the detection module and be detected by various detection engines. The local real-time detection engine includes a threat intelligence detection engine, a machine learning model detection engine, a local file detection engine, and a signature feature detection engine. Users can enable the cloud detection engine to detect malicious URLs and cloud sandbox files to find various unknown threats. In addition, TDP also includes a local analysis module, which can cache full traffic information for a certain period of time, dynamically adjust the detection granularity according to the current corporate network threat situation, and trace back and record the pre-sequence sensitive behaviors of the detected threats, without missing any traces of attackers.

Storage module: In terms of storage technology selection, we chose elasticsearch, an open source distributed data analysis engine. Elasticsearch is developed on the basis of Apache Lucene. It is applicable to all types of data, including text, digital, geospatial, structured and unstructured data, and is applicable to the security analysis scenario of TDP.

Local storage module: Elastic Search (ES) is used for local storage technology selection. ES is an open source and highly extended distributed full-text retrieval engine. It can store data almost in real time, retrieve and perform logical operations for massive data, and meet the alert information recording of the detection subsystem

and the multi-dimensional analysis requirements of the analysis subsystem.

1.1.2 Traffic Analysis

High concurrency, full traffic analysis and restoration technology： In terms of hardware, TDP uses the high-performance server of dual Xeon processor as a strong hardware support. When one device does not meet the requirements, it can also cascade multiple devices to achieve more powerful processing capacity. At the same time, IP fragmented messages can be reorganized. When IP datagrams are transmitted on the Internet, they may have to pass through multiple physical networks to be transmitted from the source to the destination. Due to the different physical characteristics of link layer and medium in different networks, there is a limit on the maximum length of data frame during data transmission, which leads to the fragmentation of IP message. When analyzing security threats, we need to reassemble these fragments in order to accurately obtain the application layer data for analysis.

In terms of accurate data extraction for TCP-borne traffic, protocol decoding can be performed to make detection more accurate. Only after the data packets are reassembled can a complete TCP session be restored. Due to network problems, data packets may be transmitted to the destination through different routes, and the order of the data packets arriving at the destination may be changed. In the transmission process, the protocol controls the data transmission. For data packets lost during transmission, the protocol will control the system and retransmit the lost data packets. Out-of-order, retransmission, and data overlap are all problems that will be encountered when TCP sessions are reorganized.

1.2 HTTPS Decryption

With the development of network security in the market, more and more customers are gradually migrating their original http services to https, which largely guarantees the security of customers' access to the network, and data will not be easily peeped by third parties. In this way, to a large extent, it is difficult for network administrators to obtain the relevant data of intranet users' access to the extranet. For enterprises, the intranet of the group is very risky. Based on this, the customer puts forward requirements for the product manufacturer, requiring the device to be able to decrypt the customer's https traffic, so as to complete the audit function of the original https traffic. TDP can not only match most aspects of SSL/TLS exchange information in the rule set language, record and analyze all key exchanges, but also realize conditional decryption of https traffic. On the condition that the user provides the private key, the traffic whose key exchange method is RSA can be decrypted. The decrypted traffic re-enters the HTTP decryptor for decomposition and threat detection.

2.0 Advanced Threat Detection

2.1 Bidirectional full traffic detection

Unlike traditional IDS and IPS that only detect one-way traffic, TDP detects bidirectional traffic, not only covering request traffic, but also detecting return traffic, as well as outgoing requests. Using the traffic analysis and data restoration module, it can support multiple mainstream protocols for high-performance analysis in the IPv4/IPv6 network environment. It has covered all scenarios, such as supporting office scene downloads and outbound requests, supporting reverse connection and packet-back detection of the production network and the office network, and supporting direct attack detection on the production network/business network.

On the basis of full traffic detection, TDP can also use suspicious traffic analysis technology, combined with the model of normal network behavior, to screen and judge

the traffic that differs from 90% within the enterprise, and mark it as suspicious, thereby discovering unpublished attack techniques and exploit vulnerabilities.

2.2 Detection for Intranet host compromise

After the intranet host is compromised, various malicious programs will be implanted to achieve the ultimate goal of hackers. After running, these malicious programs will actively connect to the hacker's remote server, report the attack status, return sensitive information or obtain further attack instructions.

TDP detects the above reverse connection behavior through three methods to accurately locate the intranet compromised host:

- Compare the reverse connection address and high-quality indicator of compromise (IOC) intelligence by ThreatBook to find the known threats.
- Detect based on deep learning DGA domain name model and DNS tunnel communication model, covering common typical techniques.
- Perform baseline modeling of the external access address characteristics of the entire enterprise network, detect abnormal behaviors such as heartbeat connections and uncommon domain name connections, and discover unknown threats.

TDP supports multiple alert methods for suspicious traffic such as DNS tunnels and DGA domain names. While generating alerts, TDP will provide rich threat context information and detection basis at the same time, which is convenient for security operations personnel to conduct attack research and judgment and hazard assessment.

2.3 Unknown Threat Detection

2.3.1 Based on the deep learning model, identifying suspicious and sensitive behaviors

TDP can use machine learning to identify suspicious and sensitive behavior in traffic, and automatically mark the traffic that generated the behavior. Many important behavior of the attacker are not all displayed in the form of attack. For example, further collection of information after obtaining a user name, further enumeration of data after obtaining a certain permission, and combing and re-use of information in the system after obtaining a shell. From a behavioral point of view, these are just normal operations, but they are not normal in the real environment of the intrusion. Through regular rule matching, these behaviors cannot be fully identified and judged. TDP uses self-developed behavior model algorithms to accurately identify suspicious and sensitive behaviors.

2.3.2 Combined with in-depth analysis of the cloud, discovering unknown threats and APT attacks

In the process of targeted and advanced attacks, attackers often deliver carefully crafted brand-new malicious programs, even including 0day exploits. Due to the limitation of local equipment analysis performance and the lag in the update of detection modules, malicious program samples are difficult to be discovered in time, which will cause greater harm to the enterprise.

In order to enhance the TDP device's ability to detect the unknown，0day, and APT threats, ThreatBook provides a cloud in-depth analysis service that can be subscribed separately. Users can choose different ways to link TDP devices with the cloud for in-depth threat analysis and discovery:

- **URL detection:** TDP will send the URL of the external access / download file of the intranet host to the cloud for inspection. The cloud analysis engine will try to connect the URL, and conduct in-depth analysis on the returned content by using multi-engine detection, cloud sandbox and network-wide threat intelligence to find the hidden threat.

- File detection: TDP provides file cloud detection capability. After it is enabled, TDP will upload the file samples restored in the traffic to the cloud for in-depth analysis and detection by using multi-engine detection, cloud sandbox and network-wide threat intelligence.

3.0 Automated Threat Handling and Response

The disposal module of TDP includes two threat blocking modes: bypass blocking and linkage blocking. The malicious address found by TDP device can be blocked through different principles.

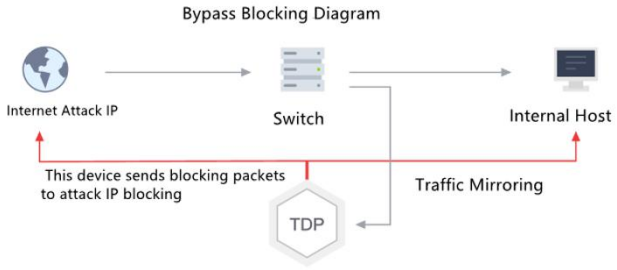
Bypass blocking: When TDP finds an illegal connection, it will send a TCP RESET packet to both ends of the communication, so as to realize the purpose of actively cutting off the connection. Then the stacks of the two communication parties will interpret the RESET packet as a response from the other end, and then stop the entire communication process, release the buffer and cancel all TCP status information. At this time, the attack data packet may still be in the TCP/IP stack buffer of the target host operating system, and has not been submitted to the application. As the buffer is emptied, the attack will not occur.

For the RESET packet, the prerequisite for TDP to send the RESET packet is to know the current serial number and confirmation number of the entire session, otherwise the RESET packet will be ignored. We assume that the confirmation number of a session must be 152. If the confirmation number of the RESET packet you send is

142, the stack will consider this to be an invalid or corrupted data packet and ignore it.

ThreatBook 微步在线

- After the bypass blocking is turned on, the device sends a blocking packet to block the attack IP.
- After enabling, users can manually add blocking IP or configure automatic blocking policy.
- Please configure the blocking white list as needed to avoid affecting normal business.

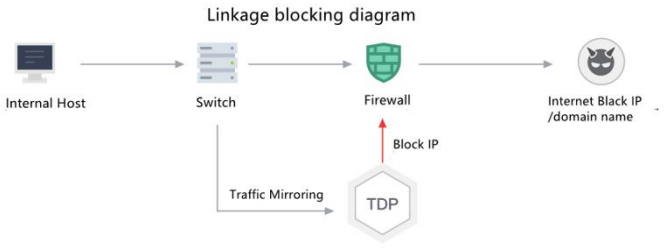


Linkage blocking: TDP regularly generates malicious address sets that need to be blocked and publishes them as static file resources. Firewall devices can configure to reference this address set to block connections.

Both bypass blocking and linkage blocking support refined blocking policy configuration, allowing the security operations team to block external malicious addresses associated with different severity levels, different attack properties, and different attack results according to actual security policy requirements, so as to achieve targeting automated response to different threats.

ThreatBook 微步在线

- After the third-party linkage blocking is enabled, a download link is provided for the third-party device to call the inbound IP to be blocked.
- Firewall devices supporting this mode: PA, Fortinet (Fortios 6.2 and above), Checkpoint (R77 and above)
- Please configure the blocking white list as needed to avoid affecting normal business.



TDP adds a processing record to the disposal, which is used to record the content of the user's disposal of the alert host in the threat, so as to facilitate the query of the disposal result.