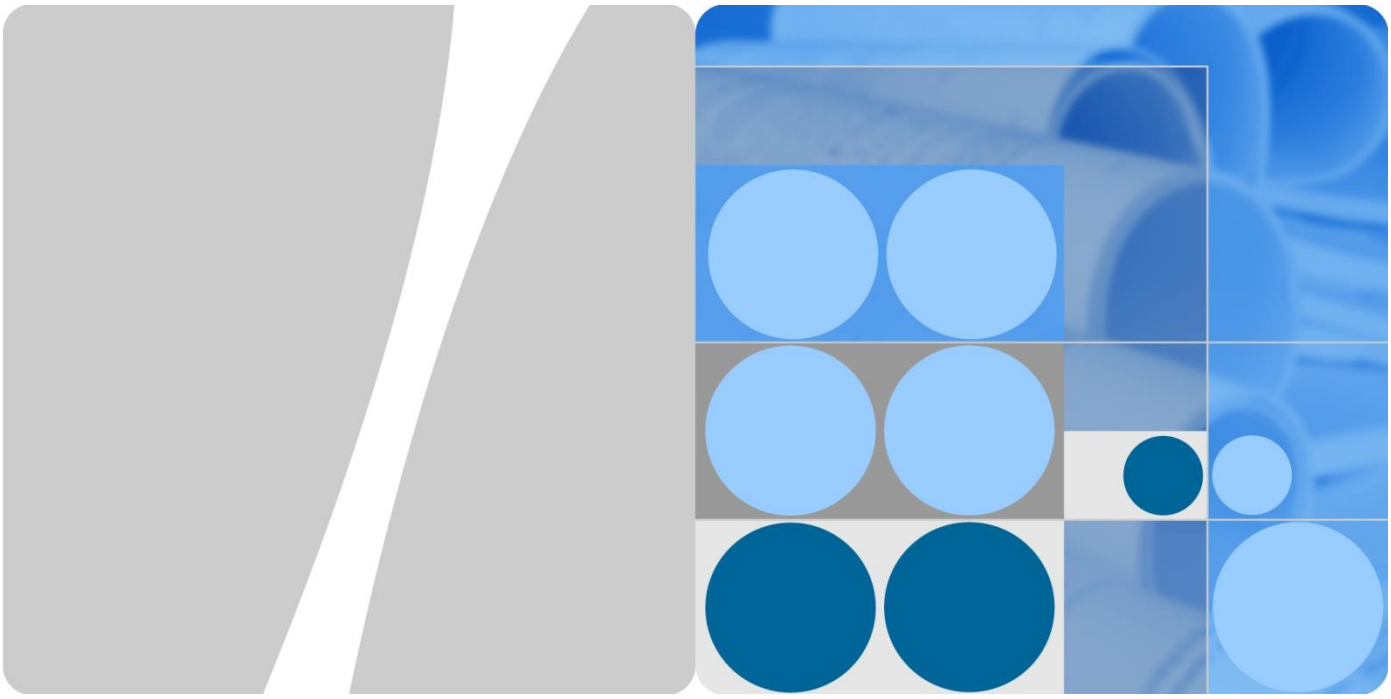


Huawei APT Defense Technical White Paper

Issue 1.0

Date 2017-03-03

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 Overview

The rapid increase of Advanced Persistent Threats (APTs) brings brand new challenges to network security defense systems. The conventional security defense mechanism that discovers and blocks attacks based on threat signature intelligence obtained in advance is no longer effective for APT attacks.

This document analyzes in detail the APT attack mechanism and offers effective defense policies. More importantly, Huawei proposes APT defense solutions that can be rapidly deployed on enterprise networks to help enterprises build APT defense capabilities and maximize the return on investment (ROI).

2 Conventional Network Threat Defense Challenged by APTs

2.1 Conventional Network Threat Defense

The mechanism of a conventional network security defense solution is that an enterprise acquires threat intelligence before attacks in a timely manner for defense. Its effectiveness depends on whether the threat intelligence is accurate and timely.

The threat intelligence refers to the information about network threats that an enterprise or organization may suffer from, including the threat context, mechanism, signature, and coping strategy. The information helps determine security defense actions.

The following figure shows a typical model of conventional threat defense.

As shown in the figure, a mature conventional security vendor possesses abundant security intelligence resources. Through honeypot systems, security labs, and various associations, partners, and organizations, the vendor can usually acquire first-hand samples of viruses or intrusion behaviors. Then with efficient security research and development, the vendor can extracts security intelligence information promptly and pushes the information to client systems or network security devices, such as the UTM, NGFW, and intrusion prevention system.

This mechanism is the most common and effective threat defense mode in the past decades and is still effective now. Typical security functions that employ this mechanism include antivirus, intrusion prevention, and malicious website filtering.

2.2 Features and Challenges of APTs

The constant evolvement of attack means gives birth to APT. At present, APT has no accurate definitions. Strictly, APT is not a new technology. It is more like a new type of behavior. The attacker may be a regulated team that abounds with budgets and resources. Its attack target and objective can be very clear, such as stealing trade secrets or destroying infrastructure. The attacker, being sophisticated in attack skills, employs various attack means, with some of them even tailored for specific targets.

In a large number of APT attack cases, zero-day attacks are frequently used.

Zero-day attacks are initiated by exploiting software or system defects and vulnerabilities and therefore are nothing different from common attacks in terms of the attack process. The key

feature that differentiates zero-day attacks from common attacks is that zero-day attacks exploit vulnerabilities that are not disclosed and are known to a very few people. Even large security vendors and labs cannot obtain information about such vulnerabilities in advance for sure, let alone attack targets. Therefore, it is impossible for attack targets to obtain threat intelligence in a timely manner to defend against APT attacks. Certain advanced threat defense mechanisms, such as heuristic or behavior-based defense, also provide limited effectiveness in that APT attackers always have a way to evade these mechanisms.

As for ransomware, you may think that your enterprise or organization has no specifically sensitive data that is worth a intrusion or theft. However, you may be wrong in this regard. Initially, attackers indeed intrude only into targets that they are interested in, such as banks, government departments, and military institutions. Recent years, however, their attack ranges have been significantly widened. What really matters to a kidnapper is the money they can get but not the kidnapped. This is also the case for an APT attacker. An attacker can "kidnap" key data of an enterprise and blackmail the enterprise.

Therefore, each and every enterprise or organization can be the target of an APT attack. With only conventional network security defense means, enterprises and organizations will be easily compromised by APT attacks.

2.3 Challenges of High Enterprise IT Costs

A full-fledged and comprehensive APT defense solution is usually costly in that it may consist of multiple sets of systems, including the device security software suite and big data analytics system. For enterprises, especially small and medium-sized enterprises or organizations, the costs are usually unbearable. In addition, such a solution also has high O&M requirements, whereas few common enterprises or organizations will have professional network security and information security personnel in place due to the high costs.

Therefore, an APT defense solution that is cost-effective and easy to deploy and maintain is in urgent need.

3 APT Attack Analysis

The APT attack process is complicated. After the final target is set, a series of activities are implemented as planned. The activities include research and preparation, single point of breach, horizontal development, and task implementation. Instead of being implemented in sequence, the activities can be repeated, overlapped, and flexibly combined.

3.1 Research and Preparation

To better implement APT attacks, attackers shall first research on attack targets. Research objects are not only organizations or their network systems but also specific individuals.

Attackers will make every effort to collect information about attack targets from key sources, such as enterprise websites, public bidding files, and news. Attackers are most concerned about network and system related information from which they can identify network vulnerabilities.

Attackers can purchase names, email addresses, and phone numbers of individuals related to attack targets from "black markets". They can also acquire information from the Internet in a more direct way. For example, they can obtain latest information from social networking tools, such as microblog, Facebook, LinkedIn, and WeChat.

With the information already obtained, they can further implement social engineering attacks to acquire more information or perform intrusions.

Social engineering attacks, different from conventional attacks targeting at hardware devices or software systems, involve psychological manipulation of people into performing actions. For example, attackers may trick people into telling their passwords over phone calls and into opening attachments containing malware in email messages with intriguing subjects. Most social engineering attacks employ email. However, hotpot keywords in search engines, forum comments, news comments, IM tools, online shopping websites, SMSs, and MMSs can also become the bearers of such attacks.

After attackers have prepared well enough and dug out several opportunity points that can be breached, they start to intrude.

3.2 Initial Intrusion

If attackers have obtained such key information as target network architectures and software deployed through detailed researches and preparations, they may then initiate attacks by

exploiting known vulnerabilities. Even the slightest neglect of security policies, such as a failure to install security patches for systems in a timely manner, may cause the systems to be compromised. Even if enterprises have been well prepared in terms of security construction, attackers can also exploit zero-day vulnerabilities purchased from "black markets" for attacks. Considering that it is impossible for enterprises to acquire intelligence for defending against zero-day attacks in advance, the attackers can easily breach the target network systems and succeed in their initial intrusions.

It the attackers cannot directly breach the target networks, they may employ social engineering technologies for phishing attacks. The most common method is to send forged email messages that contain malicious attachments or links. Different from common phishing email messages, those employed in APT attacks are relatively small in quantity and therefore difficult to be captured by anti-spam systems. In addition, the subjects, bodies, and greetings of such messages are specifically customized for attack individuals and are much like normal messages, enabling them to easily evade mail content filtering mechanisms.

Eventually, individuals with poor security awareness may click the malicious links or open the attachments, enabling the attackers to implement their initial intrusions.

3.3 Command and Control

Malware programs operating during initial intrusions are categorized as Trojan horse or bot programs. These programs are usually neither large in size nor powerful in function. After they intrude, they hide themselves and proactively listen to instructions from the attackers for further actions. In this process, a technology of Command & Control (C&C) is used.

These programs stay latent in the organizations and proactively connect to the servers controlled by the attackers at the appropriate time to establish C&C channels. Trojan horse programs can receive C&C instructions from the attackers. These Trojan horse programs use various technologies to hide and disguise themselves. Their executions and communications with the servers are difficult to be detected.

C&C is a key step in APT attacks. Only through this mechanism can the attackers intrude further into the target networks for more activities. If the C&C channels cannot be successfully established, the software programs that already intrude into the networks cannot receive commands from the attackers and therefore become useless.

3.4 Consolidation

If the attackers deploy only one Trojan horse program, the C&C channel may become invalid once the target system is re-installed or the antivirus software discovers and deletes this Trojan horse program. In this case, the attackers must start all over again. This is obviously the last thing they want to see. Therefore, the attackers will consolidate and expand their intrusion as soon as possible to continue network penetration so that they can implement subsequent tasks whenever they want.

Common consolidation methods are as follows:

Installation of remote access tools: By installing various types of remote access tools and enabling network backdoors, attackers may have multiple network intrusion paths to prevent deletion.

Privilege elevation: By exploiting known or unknown software vulnerabilities or cracking passwords, attackers can obtain management privileges over networks or hosts so as to implement tasks more flexibly.

Horizontal expansion: With access permissions that have been obtained or software exploitation, attackers can continue to intrude other workstations, servers, and devices on networks, install Trojan horse programs, and collect related information and data for subsequent use.

3.5 Implementation

APT attacks have clear business or political purposes, such as stealing high-value information assets or destroying specific key infrastructures. The preceding processes are technical preparations that the attackers have made. They will stay latent for a long period of time and wait for the best time to implement the tasks at one stroke.

Attackers may deploy certain software programs on the target networks. These programs proactively dig and collect valuable data, search for covert locations to store the data, and eventually transmit the data out to the servers deployed by the attackers in a way that is difficult to detect to steal data.

Attacks using ransomware are gaining momentum. For attacks of this type, the attackers do not transfer key data out of networks. Instead, they directly encrypt and store the data, delete the original data, and then ask for a ransom from the victims to decrypt the data. If the victims do not pay for the ransom, they will never get the data back.

APT attacks can be a one-time thing. That is, the attackers declare the end of the attacks once they succeed and erase various traces to prevent source tracing. More frequently, however, the attackers will maintain their control over the networks and continue to stay latent for a next task.

3.6 Summary

After the preceding analysis of the entire APT attack process, you may be quite clear about why it is called an APT.

It is advanced because the attacker has abundant budgets and a comprehensive management and control over various attack techniques. The attacker usually employs multiple methods, tools, and techniques in a combined manner and constantly changes the ones being used. In addition, the attacker can customize and develop tools as required. All these features make APTs stand out from attacks of other types.

It is persistent because the attacker has a clear goal, namely, a specific task. Generally, it is difficult to complete such a task in a short period of time. To achieve this goal, the attacker will maintain a long-term access privilege over the target network after the initial intrusion, instead of implementing the task immediately. This behavior of staying latent for a long period of time, monitoring the target continuously, and taking actions at the right time is a long-term threat to the target.

4 Solution

4.1 No Specific Solution

Enterprises and institutions hope to find a device or a simple method to resolve APT issues fundamentally. To their disappointment, such a specific solution is not available now and will not possibly be available in the future.

With the preceding detailed analysis, you have got the point that APT attacks employ different techniques at various phases and even at a same phase for better attack effectiveness. Remember that your opponents are individuals or teams with high intelligence hidden in the dark, instead of mechanical programs and amateur rookies.

A complete solution shall be one that has a proper defense mechanism that is well designed and combined according to technical features of APT attacks at various phases. In addition, such a solution shall have proper products deployed at different locations and deliver risk and emergence response management. Last but not least, the solution shall also be within a proper budget.

4.2 Huawei Solution

4.2.1 Overview

As shown in the figure, Huawei APT defense solution requires the joint deployment of the NGFW and sandbox. As for the sandbox, two options, namely, the FireHunter local sandbox and FireHunter cloud sandbox, are available.

Local sandbox: A local sandbox is a physical sandbox device purchased and deployed by the customer. Huawei NGFW can communicate with the local sandbox without having to connect to the Internet. Files to be detected do not need to be sent to the cloud, shortening the delay.

FireHunter cloud sandbox: As for the cloud sandbox, the customer does not need to purchase any physical sandbox device. Instead, the sandbox system is deployed in the cloud for the customer to purchase the sandbox service as required. Huawei NGFW deployed on the customer network must communicate with the cloud sandbox system through the Internet for file security checks. For small and medium-sized enterprises with limited budgets, the cloud sandbox is an optimal choice.

The APT defense mechanism described in this document applies to both the local and cloud sandboxes.

4.2.2 Blocking

The purpose of blocking is to block illegitimate access channels, including unnecessary external ports and known vulnerabilities. This is the layer-one defense. Huawei NGFWs are deployed and proper security policies are configured at the gateway and intranet border for layer-one defense.

Security policies are optimized for least privilege, preventing unnecessary external ports from being enabled and reducing the possibility of further expanding remote access capabilities after initial intrusions.

Security functions, such as intrusion detection and defense, antivirus, and malicious URL filtering, are enabled to block known threats. A large number of applications and service software programs exist on customer networks, and some of them may fail to have security patches installed in a timely manner. This gives attackers opportunities of low-cost intrusions. Huawei NGFWs, with the intrusion defense function enabled, can prevent attackers from exploiting known vulnerabilities for breaches, increasing attacking difficulties and possibly prolonging the time taken by attackers' initial intrusions.

The layer-one defense increases intrusion difficulties. However, it cannot completely block attacks.

4.2.3 Virus Probe

As analyzed earlier, attackers are sophisticated in techniques and abundant in funds. They have information about unknown vulnerabilities, through which they can initiate zero-day attacks. They can also develop software programs that can evade the intrusion defense and antivirus detection mechanism.

When these software programs eventually breach the intrusion defense and antivirus detection mechanism, a virus probe mechanism is in need to detect in details executable files or scripts transmitted to the networks for security. Huawei FireHunter, which is a sandbox product, performs this task. It executes target files in a controllable environment (called "sandbox") and tracks and checks their behaviors to guarantee that they are secure. This method of executing target files helps detect threats that cannot be discovered with conventional techniques.

Huawei NGFW can interwork with Huawei FireHunter. When files are transmitted into the network, the NGFW first employs conventional detection technologies to detect them. If no anomalies are detected, the files are transmitted to the FireHunter for in-depth checks. This interworking deployment ensures that all files entering the network go through a strict virus probe process. Only files confirmed as secure are permitted.

Enterprises and organizations with sufficient budgets can directly purchase a physical FireHunter product locally for it to interwork with the NGFW. Enterprises and organizations with a small traffic volume or limited budgets can purchase a FireHunter cloud sandbox. The local and cloud sandboxes have the same core functions, namely, performing virus probe on unknown files.

Both the local and cloud sandboxes detect threats through real file execution. Generally, it takes the sandbox far more time to detect a file than the conventional signature database-based detection mechanism. To improve performance, Huawei NGFW and FireHunter both use the local reputation mechanism, in which the previous file detection results are saved to formulate a local reputation database. This prevents same files from being repeatedly detected. Instead, their detection results can be directly extracted from the local reputation database.

For detailed virus probe mechanism of the FireHunter, see the following core technology chapter.

4.2.4 Interruption

After attackers succeed in their initial intrusions, does that mean there is nothing the enterprises can do but to wait for all defense means to break down?

The answer is definitely No. The attackers cannot achieve their ultimate goals as long as you can interrupt their further actions.

Attackers manipulate malware implanted during initial intrusions through C&C communications. The implanted malware will be out of control and can no longer properly function as long as you interrupt this communication process. Till then, attackers can do nothing but to give up on the malware and turn to other intrusion opportunities. Another situation is that the implanted malware has certain automation capabilities. The malware can proactively collect key data even if it is not remotely manipulated and wait for a right time to transmit the data to the servers pre-specified by the attackers through covert channels. In this case, these covert channels must be blocked.

Therefore, the key to prevent attackers from expanding their intrusions is to interrupt C&C communications and block covert channels to interrupt communications between the attackers and implanted malware. This also prevents the attackers from implementing multiple key tasks, such as tool installation, horizontal moving, and data transmission.

In the suggested solution, Huawei NGFW provides defense against botnets, Trojan Horses, and worms to interrupt communications between attackers and malware. Defense against botnets, Trojan Horses, and worms is a unique function of Huawei NGFW and an expansion of basic intrusion prevention functions. With a special detection mechanism, this function can identify and interrupt communication behaviors of botnets, Trojan Horses, and worms through C&C and covert channels. In addition, the NGFW is deployed at the Internet gateway and network boarder. The administrator shall deploy strict security policies to implement least privilege and to ensure that unnecessary network traffic is not permitted by default.

4.2.5 Management

The real challenge of network security lies in that there is no absolute security. After device installation and policy deployment are complete, enterprises must proactively manage APT attack risks, instead of resting easy.

The management involves prevention and response. Prevention involves deploying proper security policies and monitoring the network security status. Response involves responding to detected security anomalies in a timely manner. Huawei APT defense solution provides a powerful visualization capability that assists network security management personnel in routine security risk inspection and management.

- The SmartPolicy function of the NGFW can analyze its security policies in combination with actual network traffic to assist network security management personnel in identifying polices with security risks, such as redundant policies, unnecessary policies, and policies that excessively grant access permissions.
- In the joint deployment of the NGFW and FireHunter for interworking, not only the trends of conventional attacks can be analyzed, but also dedicated APT attack reports can be outputted. Periodical check of these reports helps network administrators discover APT intrusion attempts as early as possible.
- This solution also suggests experienced security administrators periodically reading through analysis reports of malicious files detected by the FireHunter. These reports

detail behavior features of malicious files, based on which the administrators can make proactive responses.

- The administrators shall pay special attention to threats of botnets, Trojan Horses, and worms, and malicious URL access events detected by the NGFW. These two types of events are usually associated with APT attacks and C&C channels. Based on the reports of these events, the administrators can locate hosts that initiate connections for isolation and removal.

4.3 Summary

In terms of APT attack defense, the entire industry has no specific solution. In this case, a relatively complete defense system is in need.

The deployment for the interworking between the NGFW and sandbox suggested in this document takes behavior patterns of APT attacks at various phases into full consideration and delivers a defense mechanism accordingly. This helps enterprises and organizations with limited maintenance resources and budgets rapidly build relatively complete APT defense capabilities.

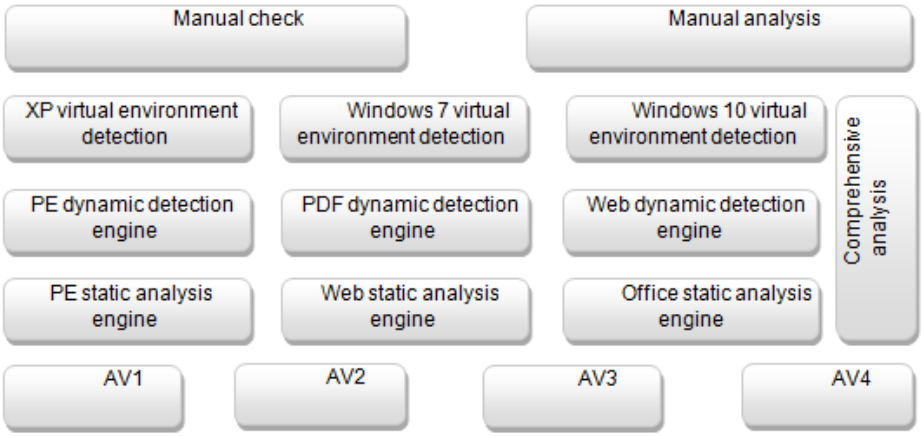
5 Core Technologies

5.1 Virus Probe Mechanism of Huawei FireHunter

Vertically, Huawei FireHunter cloud sandbox provides multiple detection means of multi-engine-based antivirus, static analysis engine, dynamic detection engine, and virtual machine (VM) environment check. These detection means complement each other. Even if certain advanced malware evades some of the detection means, the malware may eventually be detected by other means. These detection means analyze files in their own ways and give threat evaluation scores. The comprehensive analysis engine then analyzes the output results and scores of all detection means comprehensively to deliver the final conclusion.

As for suspicious malicious files or suspicious zero-day-vulnerability-exploited files, security experts will perform manual check and analysis. The following figure shows the detection model of Huawei cloud sandbox.

Figure 5-1 Detection model of Huawei cloud sandbox



- Multi-engine-based antivirus

  Huawei cloud sandbox has detection engines of multiple mainstream antivirus vendors deployed. After the cloud sandbox receives files, all these engines will detect the files. The antivirus engines deliver high detection performance, with a detection ratio of over 99% in terms of known threats. Multi-engine-based antivirus helps rapidly detect known

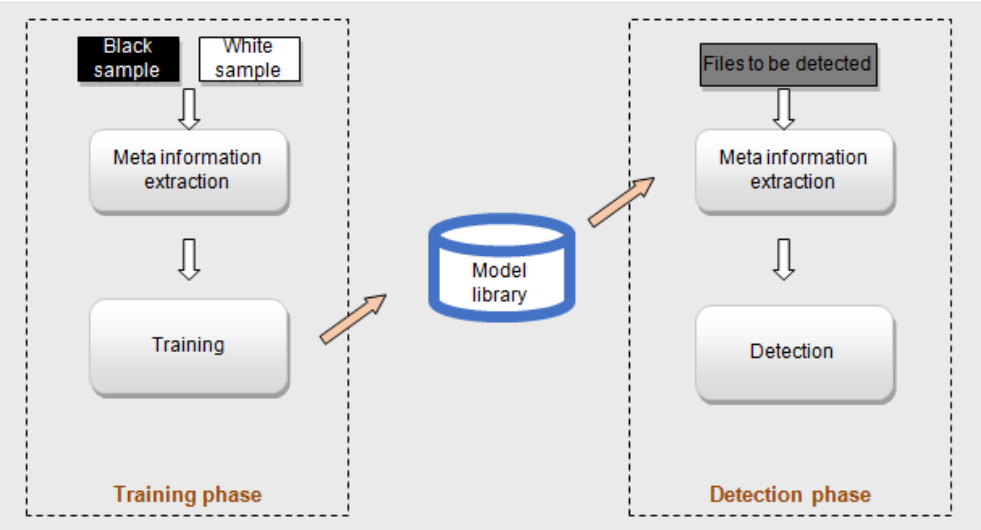
threats and provide powerful support for the cloud sandbox to give the final detection conclusion.

No matter what the antivirus detection results will be, the files will continue to be detected with the detection means that are described in the following part. For files detected as malicious ones, subsequent detection means can discover their malicious behaviors, such as accessing malicious websites to download malicious files, and can confirm the malicious categories to which the files belong, such as ransomware or worm. For files detected as normal ones, subsequent detection means may identify them as unknown threats.

- Static analysis

The static analysis technology performs binary analysis on files to check whether they are malicious without opening (documents or image files) or executing (executable files) them. Static analysis involves file structure analysis, string semantic analysis, function calling sequence analysis, and code logic analysis. The following figure shows the training and detection process of static analysis.

Figure 5-2 Static analysis of Huawei cloud sandbox



Static detection falls into the training and detection phases. At the training phase, a large number of black and white samples are selected and parsed based on file types. In addition, meta information, including strings at specific locations, function sequences, and coding language keywords, is extracted from the samples. Then the machine learning algorithm is used for training based on the meta information. During the training, the training model and various parameters are constantly adjusted until the optimal detection ratio and false positive rate are delivered. Then a model library is obtained.

The model outputted at the training phase is the input for the detection phase. At the detection phase, similarly, the files to be detected are first parsed, and meta information is extracted from the files. Then the same machine learning algorithm is used to determine their threat scores according to the model library.

Static analysis engines delivered by Huawei cloud sandbox include the PE static analysis engine, web static analysis engine, and Office static analysis engine. Each engine corresponds to a specific file type. Various types of files are different in their formats and vulnerability exploitation modes, so are the meta data extraction methods and machine learning algorithms. Therefore, there is a specific static analysis engine for each type of files.

- Dynamic detection

  In dynamic detection, files are opened (documents and image files) or executed (executable files) in a simulated environment. In addition, their behaviors during the opening or execution process are collected, and their threat levels are determined based on their threat levels.

  The PE dynamic detection engine simulates a PE execution environment in which various branches of PE files are executed as many as possible, all behaviors are collected, and threat scores of files are determined based on the dynamic behavior library. The dynamic behavior library is a behavior set formulated by Huawei security personnel by analyzing a large number of malicious samples and collecting their behaviors during execution.

  The PDF dynamic detection engine simulates a PDF Reader to open PDF files, detects scripts contained in the files, makes an attempt to execute various file branches, and collects behaviors during execution. Certain malware can detect the PDF Reader version and determine whether to trigger malicious behaviors accordingly. The PDF dynamic detection engine can proactively try on various execution branches to prevent evasion in this way.

  With a similar method, the web dynamic detection engine simulates a browser to open web files, attempts to execute various branches of embedded scripts, collects file behaviors, and eventually determines their threat scores based on the dynamic behavior library.

- Virtual environment detection

  In virtual environment detection, real operating systems and application software programs are installed on a virtual machine to simulate a user's work or home environment. In this environment, corresponding software is used to open or execute files. For example, the IE browser is used to open web files, and the Adobe Reader is used to open PDF files. In addition, PE files are directly executed, and various behaviors during the opening or execution process are collected, including network behaviors, registry operation behaviors, and file operation behaviors. Then a behavior pattern library is used to analyze file behaviors, during which auxiliary threat determination is performed in combination with Huawei reputation database. For example, if a file accesses a C&C site during its execution, its threat level is increased.

  Huawei cloud sandbox provides three types of virtual environments, namely, Windows XP, Windows 7, and Windows 10. Various environments trigger different malicious behaviors. These three virtual execution environments provided by Huawei cover currently mainstream work and home environments for discovering malware to a maximum extent.

  Compared with the preceding dynamic detection technology, virtual environment detection is an OS-level detection technology. If the virtual environment is destroyed by malware, resetting at the OS level is required. Dynamic detection, however, is a process-level detection engine and requires only process-level resetting after being destroyed. The strength of the dynamic detection engine lies in that it is fast in detection and can attempt to execute various branches. The strength of virtual environment detection lies in that it can simulate real environments to detect files of various types.

- Comprehensive analysis

  Certain files can be identified as malicious through a single detection mean, whereas certain files cannot. For those cannot, the comprehensive analysis engine gathers the results and threat scores of all detection means to deliver final conclusions and summarizes various threat behaviors to output detection reports.

- Manual analysis by security experts

As for suspicious files, security analysis personnel from Huawei security analysis team manually check suspicious zero-day-vulnerability-exploited samples and dig up zero-day vulnerabilities.

5.2 Various File Types Supported

Huawei cloud sandbox supports the detection of various types of files, including Windows executable files, Microsoft Office 97-2003 files, Microsoft Office files, PDF files, web pages, flash files, WPS files, CHM files, compressed files, image files, Linux executable files, and script files. Files of all the preceding types can be manually submitted. When the NGFW interworks with the cloud sandbox, the manual submission of files of certain types may be restricted for the consideration of performance. At present, the NGFW supports the submission of only Windows executable files, Microsoft Office 97-2003 files, Microsoft Office files, and PDF files.

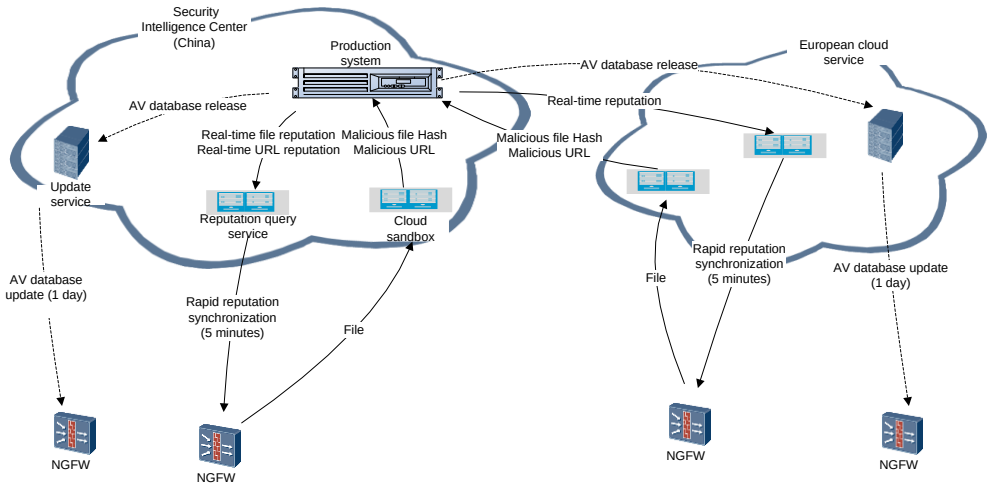
In addition, the cloud sandbox also supports URL detection. After users submit URLs, the cloud sandbox detects corresponding web pages and outputs detection results.

5.3 Rapid Global Threat Information Sharing

- Threat information sharing

  Compared with antivirus, the most significant feature of the sandbox lies in that it can detect unknown threats. After the cloud sandbox detects unknown threats, it rapidly synchronizes threat information to all NGFWs around the global through the reputation mechanism to block the threat spread.

Figure 5-3 Global threat information sharing



The NGFW capable of interworking with the cloud sandbox sends files to the cloud sandbox for detection. After detecting malicious files, the cloud sandbox reports malicious file hashes and URLs to the production system. The production system generates real-time reputation information and rapidly synchronizes the reputation information to the reputation query server in the cloud. Then the reputation query server synchronizes the real-time reputation information to the NGFW, based on which the

NGFW can block malicious files and URLs. The entire process from the NGFW detects threats to the NGFW receives real-time reputation information takes only five minutes.

In addition to generating real-time reputation information, the production system can also generate the antivirus signature database based on the information reported by the cloud sandbox and release the database to the update server in the cloud. The NGFW of an earlier version that does not provide the reputation function can obtain latest threat information by updating the antivirus signature database. However, the release and update cycle of the database is one day. Therefore, this mode is outshone by reputation synchronization in terms of timeliness.

6 Conclusion

APT attacks are gaining momentum. Each and every organization and individual may become an APT attack target. Attackers employ constantly evolving attack means, and there has been no specific solution that can completely defend against APT attacks till now. Enterprises and organizations are in urgent need of a comprehensive solution that helps build basic APT attack defense capabilities and reduce attack risks to the maximum extent.

Based on years of experience in defending against APT attacks, Huawei summarizes major processes and key technical points of attacks and designs a comprehensive APT defense solution accordingly. This solution can be easily deployed, without the need of sophisticated routing knowledge and complicated networking adjustment. Its core is the NGFW and FireHunter and their interworking deployment, which offer a comprehensive APT defense solution based on blocking, virus probe, interruption, and audit.