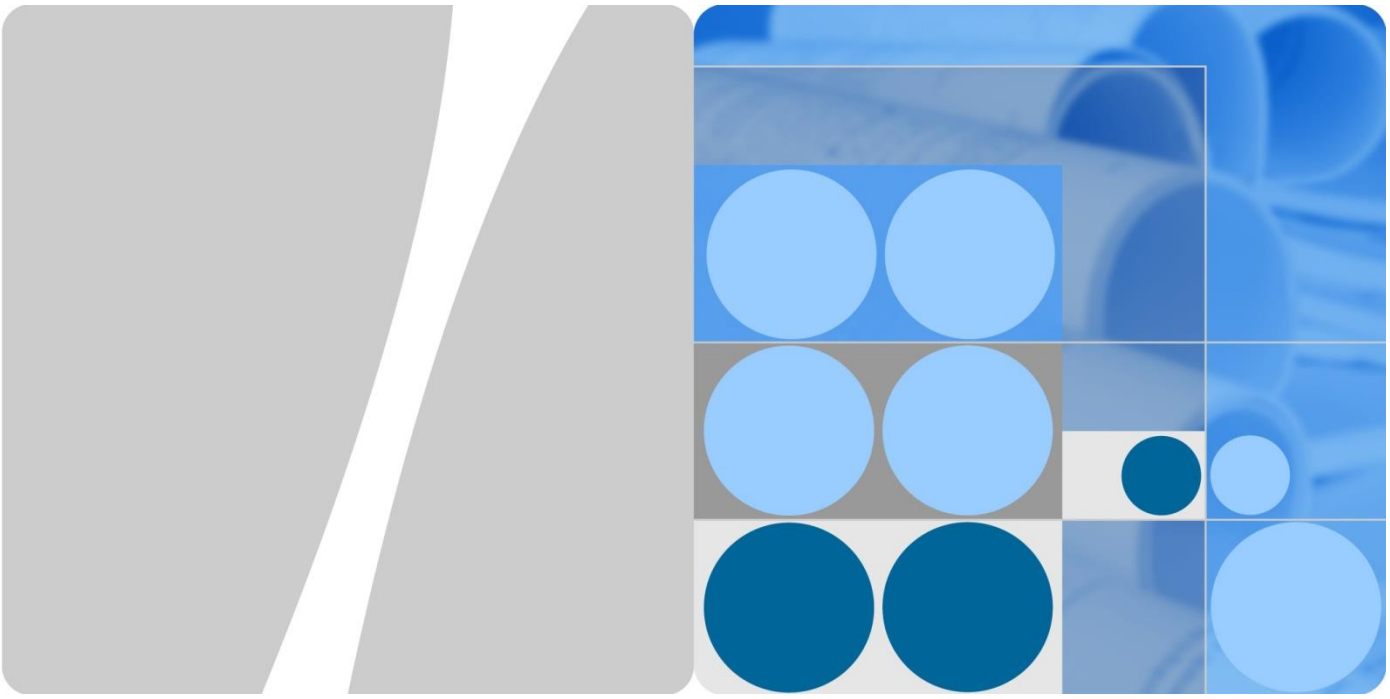


FireHunter6300
V100R001C60
Technical Proposal

Issue 01

Date 2017-02-27

HUAWEI

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

In 2010, Google suffered the Aurora next-generation attack, which caused a great number of Gmail email leaks and great damages to Google brand.

In the same year, the Stuxnet attack was launched on Iran's nuclear facilities, causing severe damages to the centrifuge. The damage caused by this attack is no less than that of a spot bombing.

In 2011, RSA underwent a next-generation attack targeted at a SecurID server, causing large-scale SecurID data leaks and threatening the security of SecurID users. The public doubts on the company's security protection capabilities adversely affected the company's image.

In March 2013, the banking industry in Korea suffered a targeted advanced persistent threat (APT) attack, crashing a great number of banking computer systems and greatly affecting banks' reputation.

In December 2015, the Ukraine power grid was attacked by malicious code in at least three power supply regions. As a result, the power was cut off for several hours in half of the regions in Ivano-Frankivsk, Ukraine.

In February 2016, Bangladesh Bank's account in the Federal Reserve Bank of New York was attacked by hackers and lost more than US$100 million.

With the debut of next-generation threats represented by APTs, conventional security protection approaches are greatly challenged. An APT attack may disclose a company's core business secrets, leading to inestimable losses to the company, or even compromise the industries related to people's livelihood, such as the financial, energy, and transportation industries. The effect of such an attack is nothing less than a war. In the future, how to cope with next-generation threats represented by APTs is relevant to national security, which is not merely the responsibility of security companies. We should defend against the next-generation threats from the national security perspective to cope with possible cyberwars in future.

1.1 APT Background

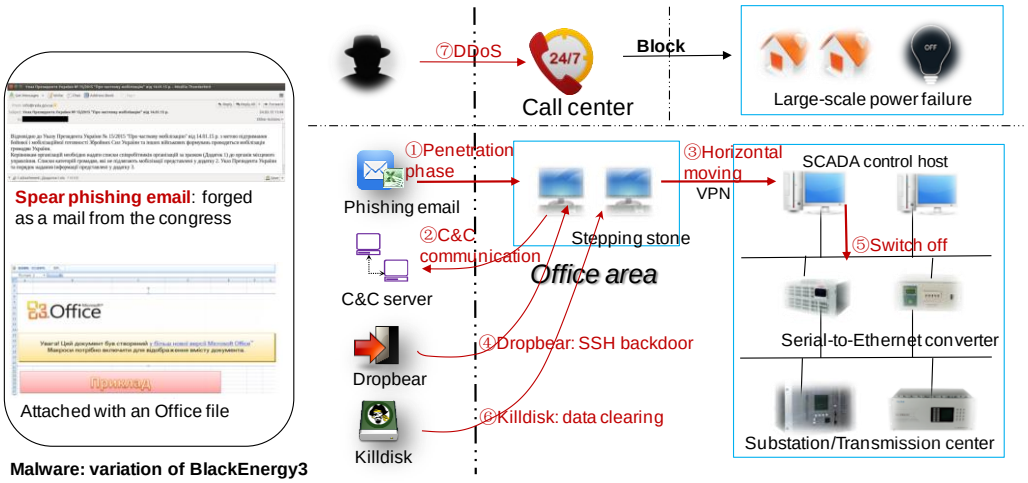
Since Google admitted being attacked in 2010, APT has become a hot topic in the information security circle.

For the companies that have experienced APT attacks, such as Google, RSA, and Comodo, APT is no doubt a nightmare. Then, they start to contemplate on the existing security defense systems.

APT is very good at concealing itself. It usually exploits the vulnerabilities of trusted applications in enterprise or institution networks to form a C&C network required by attackers. APT is also highly targeted. Before launching an APT attack, attackers usually need to collect a great deal of information about the target's service processes and systems. The information collection process is a perfect reflection of the arts of social engineering. Besides, attackers need to collect information about 0-day vulnerabilities on the targeted network.

The following part describes the process of the APT attack on the Ukraine power grid in December 2015, which is a typical APT attack.

Figure 1-1 APT attack process of the Ukraine power grid



During the APT attack on the Ukraine power grid, attackers first forged a mail from the congress for penetration. When staff in the office area opened the malicious Office file attached to the mail, the malicious macro ran to embed malware into office hosts. The malware established a C&C communication with an external C&C server and accessed SCADA control hosts in the equipment room through employees' VPN permissions. By exploiting SSH vulnerabilities, attackers added a fixed password to SSH servers of the SCADA control hosts in the equipment room, leaving a backdoor for attacks. Attackers logged in to office staff's hosts through the C&C channel, connected to control hosts in the equipment room through the staff's VPN, and operated on control hosts in the equipment room through SSH to issue a switch-off command. As a result, the power was cut off in multiple regions of Ukraine. Then, attackers erased evidence and destroyed the system. In addition, attackers initiated a DDoS attack to the Ukraine power grid's call center, resulting in power failure for several hours and social chaos in Ukraine. This attack was achieved by penetrating and embedding malicious code into staff hosts, causing extremely vicious social and political impact.

Great importance must be attached to APT attacks because any negligence may cause catastrophic damages to the information system. Just like the seemingly solid Maginot Line, the German army simply changed the strategy and the Line became a decoration. The following table lists differences between traditional cybercrimes and APT attacks.

Figure 1-2 Differences between traditional threats and APT attacks

Comparison Item	Traditional Threat	APT Attack
Identity of attacker	Opportunist, hacker, and cybercrime criminal	**Organized illegal company with worldwide networks, hacker, and hostile**
Attack target	No specific targeted user. Common targets are personal e-banking accounts, credit card data, and valuable online accounts.	**Specific attack targets, for example, national lifeblood industries such as military technology, power grid, energy, telecommunications, transportation, finance, and culture, covering national security data, trade secrets, and business & production plans**
Attack motivation	Money profit, identity theft, spoofing, spam, and reputation	**Control the strategic advantages in the market/military, economic advantages in the industry, and competitiveness in commercial negotiations; damage key infrastructures; be driven by political factors.**
Attack frequency	One-time attack	**Long concealment and persistent attacks**
Attack means	Widely disperse existing malware to increase opportunities for obtaining benefits.	**Use the malware developed by exploiting 0-day vulnerabilities or targeted users' environmental defects to hijack systems, implement transfer, steal data, and destroy field tracks during the process of attacking targeted organizations.**
Detection difficulty	Easy to capture because of the short lifetime; high detection rate	**Blank samples for a long time; low detection rate**

APT attacks are like well-armed troops. The high-tech weapons can invalidate the traditional security defense systems, such as the IPS/IDS, firewall, and antivirus software. The traditional signature-based passive defense systems are unable to defend against the targeted attacks that exploit 0-day vulnerabilities or well-designed malicious programs.

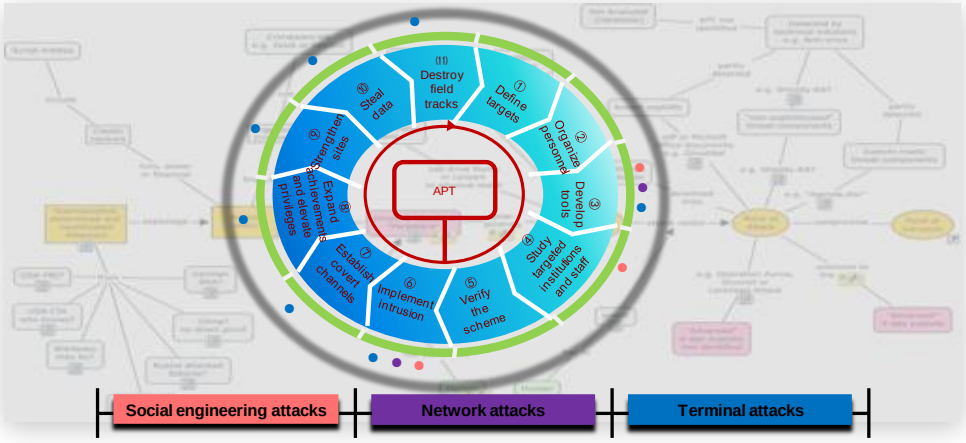
1.2 APT Development Trend

A typical APT attack may exploit the following means to intrude an enterprise network:

- Uses attack methods, such as SQL injection, to intrude enterprise servers (such as web server and mail server) oriented to the Internet and further scans other servers or desktop terminals on the enterprise network for further attacks.
- Sends mails with malicious attachments to senior managers.
- Sends malicious links to enterprise employees using the account of an acquaintance.
- Uses USB disks to spread malware to an isolated network.

Once a computer is planted with malware, such as Trojan horse, backdoor, or Downloader, the malware establishes a C&C communication with the Internet in the enterprise network, persistently collects sensitive files (such as Word, PPT, PDF, and CAD files), and transfers the files back to the attackers through covert channels.

Figure 1-3 Typical APT attack process



APT attacks exploit Advanced Evasion Techniques (AETs), 0-day vulnerabilities, and social engineering techniques to primarily attack high-value industries and the infrastructures that affect people's livelihood, such as finance, energy, telecommunications, and transportation networks. APT attacks exploit complicated attack methods, have long latency time, and are difficult to detect. One APT attack can cause the disclosure of core business secrets and even paralyze the entire enterprise or industry. Next-generation threats represented by APTs have shown their prototypes, and a solution is in urgent demand.

1.3 Status Quo of Live Networks

Customers have deployed dedicated firewalls, IPS devices, antivirus software, and terminal security software to defend against mainstream threats. However, the signature-based traditional defense methods identify only known threats and are slow to catch up with the ever-changing threats. They are ineffective in defending against next-generation threats represented by APTs. Therefore, how to deal with the next-generation threats has become a headache of all enterprises.

2 Analysis on XX Network

[Based on the communication with XX Enterprise, we have a thorough understanding and analysis of its network…]

2.1 Status Quo of XX Network

[This section covers the following parts:]

1. *Internal networking diagram of XX enterprise: You must provide the networking diagram without FireHunter devices if the enterprise network is newly built. This networking diagram will be used to analyze the security solution.*
2. *Services carried by the intranet of XX enterprise: mainly include internal services and egress network services.]*

2.2 Service Analysis on XX Network

[Provide the service flow analysis diagram for the customer to better understand network security issues.]

2.3 Analysis on APTs of XX Enterprise

[This section mainly includes the following parts (based on analysis and communication with customers):]

1. *After XX enterprise's servers oriented to the Internet, such as the web server and mail server, are compromised, XX enterprise cannot be aware of attack activities, such as scanning other network servers or desktop devices.*
2. *XX enterprise's existing mail filtering systems are mostly based on the spam address library, while attackers use malicious mails that are counterfeited with legal senders. In addition, the malicious code hidden in mail attachments is generally 0-day vulnerabilities, which are difficult to be detected in mail content analysis.*
3. *XX enterprise's existing security defense/detection devices cannot identify such 0-day vulnerability attacks.*

4. *XX enterprise's existing security devices cannot analyze the content transmitted when the targeted devices are under the control of attackers, and are incapable of analyzing suspicious connections.*
5. *XX enterprise's existing security devices use the detection method based on signature databases, and cannot analyze the enterprise's compressed, encrypted files without fingerprint signatures thieved by attackers.*

2.4 FireHunter6300 Design Principles of XX Enterprise

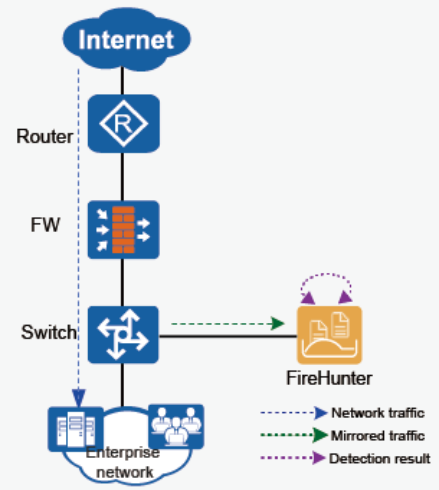
According to XX enterprise's requirements for defending against next-generation threats represented by APTs and Huawei's experience accumulated with new attack technologies such as APTs, we propose that XX enterprise must comply with the following principles in FireHunter application design.

- Security: Design and implementation of information security products and technical schemes should fully ensure system security with specific measures.
- Reliability: Project implementation should ensure product quality and system reliability with strict technical management and redundant device configuration.
- Advancement: Specific technologies and technical schemes should ensure that the system supports advanced technologies and sustainable development.
- Easy promotion: Schemes and technologies should support system expansion and more sites.
- Scalability: With the rapid development and update of IT technology, the technology used must have good scalability to fully protect the current investment and profits.
- Compatibility: The system's standardization degree must be high enough to implement full compatibility between application systems. In addition, a non-compatible design is supported according to special requirements.
- Manageability: All security systems should support the online security management mode.

3 Huawei XX Network Security Solution

3.1 Off-line Deployment for Traffic Restoration

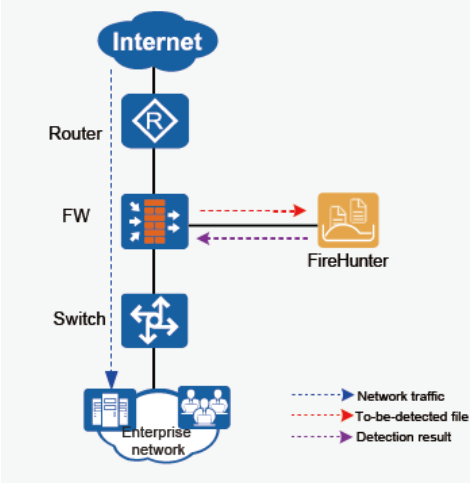
Figure 3-1 Off-line deployment for traffic restoration



In the independent deployment scenario, the mirroring port of the FireHunter is directly connected to that of the switch or another gateway. The switch or another gateway transmits the network traffic to be detected to the FireHunter over the mirroring port. The FireHunter receives the mirrored network traffic, restores the traffic, and performs C&C detection and file detection for the traffic. Both the C&C detection and file detection results are displayed on the FireHunter's web UI. You can also query detection result reports of malicious files as well as malicious files and threat analysis-related files and evidence.

3.2 Off-line Deployment for Firewall Interworking

Figure 3-2 Off-line deployment for firewall interworking

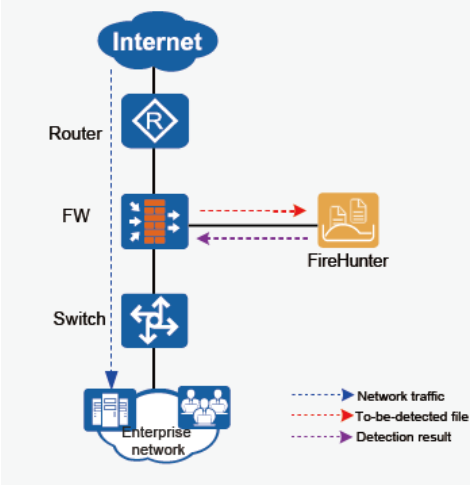


In the scenario where the FireHunter interworks with the firewall, it is necessary to ensure that the FireHunter's interworking interface is reachable. When network traffic passes through the firewall, the firewall extracts files from network traffic and sends the files to be detected to the FireHunter through the interworking protocol. The FireHunter receives and detects the files, and the firewall queries the detection result of the files through the interworking interface. In this scenario, the firewall can provide file detection logs, and the FireHunter can display not only detection logs but also detection result reports of malicious files on its web UI. In addition, the FireHunter allows you to query malicious files and threat analysis-related files and evidence.

The FireHunter's interworking interface is a RESTful interface. The FireHunter opens the interface so that interworking clients can be developed for other devices to submit files to the FireHunter for detection.

3.3 Deployment for Interworking with the CIS

Figure 3-3 Deployment for interworking with the CIS

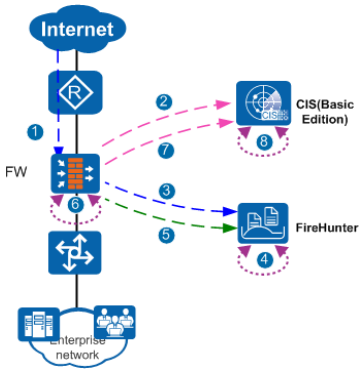


When the FireHunter interworks with the CIS, it is also necessary to ensure that the sandbox interworking interface is reachable. In this scenario, the CIS flow probe receives mirrored traffic, restores the traffic to files, and sends files to the FireHunter through the FireHunter's interworking protocol. The FireHunter receives and detects the files and sends detection logs to the CIS collector.

In this scenario, besides detection logs, the FireHunter also displays detection reports of malicious files as well as malicious files and threat analysis-related files and evidence on its web UI.

3.4 Deployment for Interworking with the Firewall and the CIS Basic Edition

Figure 3-4 Deployment for interworking with the firewall and the CIS Basic Edition



1. The FW detects traffic and restores the traffic to files.
2. The FW performs local AV and IPS detection and sends logs to the CIS Basic Edition after detecting known threats.
3. The FW sends unknown files that cannot be locally detected to the FireHunter for detection.
4. The FireHunter performs file detection.
5. The FW proactively queries the detection result from the FireHunter.
6. The FW blocks or generates an alarm on files or traffic based on the FireHunter detection result.
7. The FW generates logs based on synchronized information and sends them to the CIS Basic Edition.
8. The CIS Basic Edition displays the security posture, trend, and details of known and unknown threats.

In this scenario, ensure that the FireHunter's service interface is reachable. When network traffic passes through the firewall, the firewall restores traffic to files and sends the files to the FireHunter for detection. The firewall queries detection results from the FireHunter, generates security policies based on the detection results, and allows or blocks the network traffic with detected files. In addition, the firewall generates detection logs and sends them to the CIS Basic Edition for displaying the security posture of the whole network.

In this scenario, the FireHunter displays detection reports of malicious files as well as malicious files and threat analysis-related files and evidence on its web UI.

4 FireHunter6300 Security Sandbox

4.1 Introduction to the FireHunter6300

The FireHunter sandbox is an APT detection system developed by Huawei. It uses the multi-engine virtual detection technology and traditional security detection technology to identify malicious files and C&C attacks, making up for the deficiency of traditional signature-based detection methods. It effectively prevents diffusion of unknown threat attacks and loss of enterprises' core information assets, especially applicable to finance and government agencies, energy providers, and high-tech enterprises.

The FireHunter sandbox provides the following features to detect the next-generation threats represented by APTs:

- Comprehensive traffic detection: provides an independent traffic restoration capability to identify mainstream network protocols, such as HTTP, SMTP, POP3, IMAP, FTP, NFS, and SMB. That is, it can identify all files transferred over the network. That is, it can identify all files transferred over the network.
- Detection of mainstream applications and files: supports Word, Excel, PPT, PDF, HTML, JS, EXE, JPG, GIF, PNG, CHM, SWF, executable scripts, and compressed files.
- Simulation of mainstream operating systems and applications: supports the Windows XP/7/10 operating systems, Internet Explorer 6/7/8/9/10/11 and Chrome browsers, Office 2003/2007/2010/2013, and Adobe Reader 8/9/X/XI.
- Layered defense system: provides the reputation-based and signature-based attack detection methods, heuristic detection engine, and virtual execution environment, improving the capabilities of coping with next-generation threats represented by APTs; provides a list of all risky operations related to next-generation threats to help customers gain visibility into the attack process and targets.
- Near-real-time processing: reduces the detection response time of next-generation threats from weeks to seconds and interworks with the NGFW for online attack defense.
- Anti-evasion: detects evasion techniques by running code in virtual machines or based on user interaction.
- C&C detection: supports not only the traditional signature-based C&C attack detection, but also the Domain Generation Algorithm (DGA) malicious domain name detection based on machine learning and a specific algorithm.

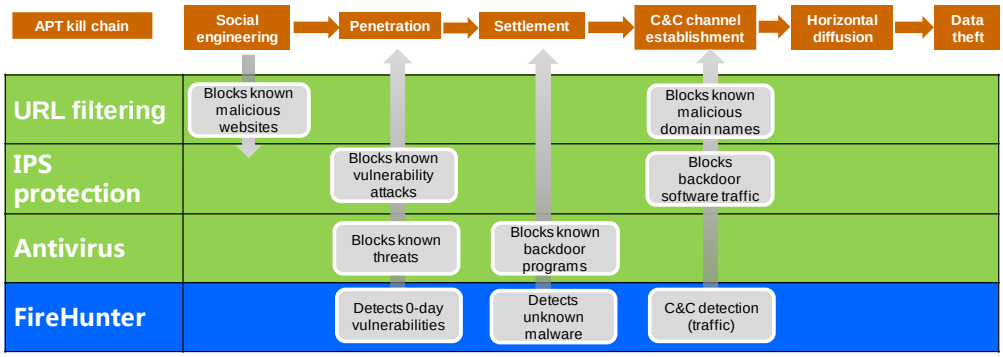
4.2 FireHunter6300 Protection Solution

Figure 4-1 shows an APT kill chain and protection measures for all phases of the kill chain. An APT kill chain includes social engineering, penetration, settlement, C&C channel establishment, horizontal diffusion, and data theft. Attackers put their concentration mostly to the penetration, settlement, and C&C channel establishment phases.

With advanced technical capabilities, Huawei proprietary FireHunter can help customers identify APT attacks in the phases of penetration, settlement, and C&C channel establishment to further eliminate or block APT attacks.

In the penetration phase, attackers usually send mails with malicious links or attachments to targeted objects or release malicious files to websites. If employees click malicious links or download malicious mail attachments, malicious files are penetrated into enterprise networks. The FireHunter's file detection function, with 3-layer detection technologies (innovative static analysis, heuristic detection, and virtual execution) and malicious behavior analysis technologies, effectively makes up for the deficiency of traditional signature-based detection methods, accurately detects malware, and identifies APT attacks in the phases of penetration and settlement. Upon successful settlement, attackers further establish C&C channels to issue commands and control enterprise network devices to provide desired services. The FireHunter's C&C detection technologies include not only the traditional signature-based technology for identifying known C&C attacks, but also a technology based on machine learning and Huawei proprietary DGA for detecting C&C attacks caused by requesting or accessing DGA malicious domain names. In addition to unknown threats, the FireHunter can detect known threats, and it has the built-in antivirus and IPS engines.

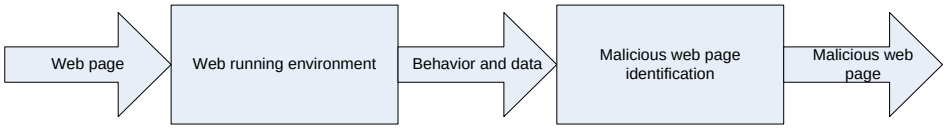
Figure 4-1 APT kill chain and protection chain



4.3 FireHunter6300 File Detection Technology

4.3.1 Web Sandbox Detection Functions

Figure 4-2 Web sandbox detection principle



The web technology's fast development brings about more and more applications and services. Accordingly, more security threat categories targeted at the web technology come into being with more types of attack means and more severe damages. Using the traditional antivirus software to extract signatures from known samples cannot identify and block malicious pages promptly, that is, cannot properly defend against web threats.

To detect the new unknown threats, the FireHunter uses the sandbox technology to build a web page running environment, extracts running data by analyzing real-time script behavior, and identifies malicious pages as soon as possible. The detection principle is shown in Figure 4-2. The FireHunter performs the following functions:

- Simulates the Internet Explorer browser environment, completely de-obfuscating web pages.
- Classifies web files through machine learning.
- Performs shellcode detection for the binary content generated during the browsing process.
- Detects various risky behavior during page execution in real time.
- Analyzes in real time whether POC overflow code exists during page execution.

4.3.2 PDF Sandbox Detection Functions

The currently known malicious PDF files perform the buffer overflow attack (that is, shellcode attack) using the implementation defects of Adobe Reader. The attack process is as follows:

1. The JS engine restores the shellcode from the encoded data (including encrypted data).
2. The Adobe Reader transfers the memory area containing the shellcode to the Adobe Reader function that has the buffer overflow vulnerability as a parameter.
3. Adobe Reader runs the shellcode to implement the buffer overflow attack.

The shellcode attack in PDF files can be identified in any of the above steps. According to in-depth analysis of Adobe Reader, the shellcode always calls the character string operations (such as allocation and access) in the JS engine. Therefore, the FireHunter monitors character string operations and checks whether the character string is shellcode to determine whether malicious code exists in PDF files. The FireHunter performs the following functions:

- Simulates the PDF file parser environment.
- Fully executes the internal script code in files.
- Analyzes in real time whether POC overflow code exists during script execution.

4.3.3 PE Heuristic Sandbox Detection Functions

After PE files are packed, obfuscated, or infected by viruses, some fields in the PE format are modified to implement normal execution of the PE files. However, the PE format fields modified are different from those generated by the normal compiler.

The PE sandbox can detect anomalies in the PE format and output the import table and segment table information for threat demonstration or combined virus reporting based on threat analysis. The FireHunter performs the following functions:

- Simulates the operating system environment, CPU instructions, and API calls.
- Monitors the software instruction stream and API call stream.
- Matches the specific virus family signatures such as static instructions and API calls for static analysis through disassembly instructions, API calls, and parameters.

- Simulates executable files, monitors threat behavior, and matches the specific virus family behavior and behavior sequences.
- Analyzes abnormal file formats and attributes.

4.3.4 Static Detection Functions

Malicious file detection falls into static detection and dynamic detection.

Static detection is implemented by matching characters. The FireHunter determines whether a file is malicious by searching the file's suspicious data block (querying the static library). Dynamic detection means to record all operations during file execution and check whether these operation records may damage the system. The FireHunter performs the following static detection functions:

- Supports in-depth decoding for Office, image, and SWF files.
- Analyzes abnormal file data formats.
- Parses macro and VB scripts and analyzes malicious behavior.
- Analyzes obfuscated data that evades detection.
- Detects the shellcode.
- Matches virus family signatures.

4.3.5 Heavyweight Sandbox Detection Function

The FireHunter identifies whether the program files corresponding to the process are malicious by monitoring API calling behavior during process running. The following file types can be detected:

1. Executable program file: The FireHunter determines whether an executable file is malware by monitoring behavior during process running.
2. Malicious web page: The FireHunter determines whether malicious code exists in a web page by monitoring suspicious behavior of the Internet Explorer process during web page browsing.
3. Office, PDF, or image file: The FireHunter determines whether malicious code exists in the Office, PDF, or image file by monitoring behavior of the corresponding software process. When the software process is compromised by malicious code, it may execute behavior of malicious code, for example, downloading and executing program files.

The FireHunter performs the following heavyweight sandbox detection functions:

- Uses the virtualization technology to simulate the operating system and other software environments.
- Provides a virtualized environment for the files to be detected and executable programs.
- Analyzes the behavior and parameter information of executable programs and files in real time.
- Supports multiple anti-evasion detection techniques, such as virtual machine environment check and delay control.

4.4 FireHunter6300 C&C Detection Technology

If social engineering and penetration in the APT kill chain can be compared to net casting, C&C channel establishment is the phase preparing net drawing. Although malware used in

APT attacks has many variations and is frequently upgraded, communication modes of C&C channels are not often changed. Therefore, you can use the traditional intrusion detection method to detect APT C&C channels. The key to success is to obtain detection signatures of C&C channels for all APT attack means in a timely manner.

In addition, DGA is a mainstream advanced C&C method and generally used in popular malware outside China. Seemingly random C&C domain names in VirusTotal belong to this attack. DGA is designed to write the domain name character string into a specific random algorithm, but not put it into malware code. Most of DGA domain names can be identified by comparing with legal domain names. However, it is not realistic to identify so many random domain names generated by the computer using human eyes one by one. While the computer can complete the competitive work using human experience. For example, the classification task is executed to determine whether a domain name is a C&C attack.

The FireHunter provides two C&C detection technologies: C&C detection based on remote control tool signatures and DGA malicious domain name detection.

- C&C detection based on remote control tool signatures: As a signature-based traditional detection method, it extracts signatures from flow information and compares them with remote control tool signatures.
- DGA malicious domain name detection: It uses machine learning and specific algorithms. The detection process is as follows:
  1. The FireHunter extracts domain name signatures based on traffic information and generates a classifier through model training.
  2. After detecting new traffic, the FireHunter extracts domain name-related signatures and sends them to the classifier. The classifier determines whether the domain name is normal.
  3. The FireHunter adjusts model training parameters and signature formats based on the classifier's detection results to make the classifier more accurate.

5 Product Specifications

Table 5-1 Product specifications

Function	Requirement
File type detection	Supports APT detection for Window executable files.
	Supports APT detection for Office files.
	Supports APT detection for PDF files.
	Supports APT detection for web pages.
	Supports APT detection for image files.
	Supports APT detection for Flash and SWF files.
	Supports APT detection for Java Applet files.
	Supports APT detection for WPS files.
	Supports detection for compressed files.
	Supports detection for executable script files.
	Supports detection for CHM files.
URL detection	Supports URL detection.
Interworking detection	Supports analog interworking detection.
	Supports actual interworking detection.
C&C detection (traffic is directly transmitted to the FireHunter for independent deployment)	Supports C&C detection based on remote control tool signatures.
	Supports DGA malicious domain name detection.
Anti-evasion	Supports anti-evasion based on time judgment.
	Supports anti-evasion based on interactive execution.
	Supports anti-evasion based on virtual machine probing.

Function	Requirement
Traffic restoration supported protocol (traffic is directly transmitted to the FireHunter for independent deployment)	L2 protocols: VLAN and PPPoE
	L3 and L4 protocols: IPv4, TCP, UDP, ICMP, and GRE
	Application layer protocols: HTTP, SMTP, POP3, IMAP, FTP, NFS, and SMB
Supported sandbox environment	Supports Windows XP, Windows 7, and Windows 10 operating systems.
	Supports Internet Explorer 6, 7, 8, 9, 10, and 11.
	Supports Adobe Reader 8, 9, X, and XI.
	Supports Microsoft Office 2003, 2007, 2010, and 2013.
Performance	Processes 70,000 files per day.
Management	Provides a web UI.
Deployment mode	Supports interworking with the firewall and CIS.
	Supports off-line deployment for traffic restoration.

6 Hardware Configuration

Table 6-1 Hardware configuration

Model	FireHunter6300
Network port	4 x Gigabit electrical port 2 x 10GE optical fiber port (optional)
Hard disk	4 x SATA 2 TB (RAID10)
SSD	2x 200 GB (RAID1)
Processing performance	70,000 files per day
Power module	Redundant AC power modules
Dimensions (H x W x D)	86.1 mm (2 U) x 447 mm x 748 mm

7 Huawei Service

7.1 Service Concepts

- Customer-oriented services

  Focus on the requirements and experience of the customer, improve the awareness and skills of service, and protect the network running of the customer with superior services to meet the security requirements of the customer.
- Sophisticated services

  Constantly optimize service content and provide professional, standard, and diversified services. Attach importance to service initiative and service personalization, build an excellent service brand, and maintain leadership in the industry.

7.2 Service Content

Table 7-1 Service list

Service	Support from Others	Deliverable
Preparations	Learn about the network conditions from the customer.	
Onsite service	Assistant personnel	Service implementation application Service implementation summary report
Test	Assistant personnel	Test report
Onsite training	Training venue and participants	Training summary report

7.3 Service System

Huawei has a three-tier service system for project implementation: local office, technical support department, and R&D department.