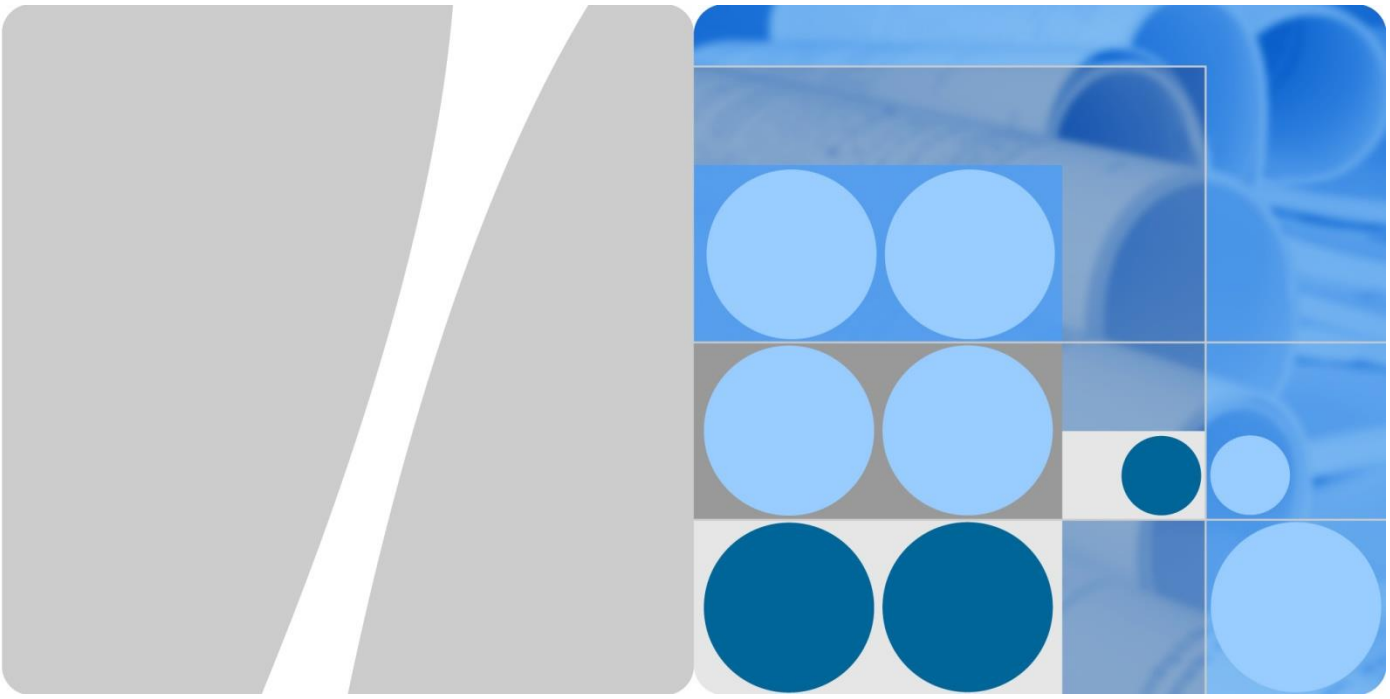


FireHunter6300
V100R001C60
Technology White Paper

Issue 01

Date 2017-02-24

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 3
1.1 APT Background 4
1.2 APT Development Trend 5
1.3 Status Quo of Live Networks 6
2 Security Protection Solution 7
2.1 File Detection Technology Principles 8
2.2 C&C Detection Technology Principles 9
2.3 Typical Application Scenarios 11
2.3.1 Off-line Deployment for Traffic Restoration 11
2.3.2 Off-line Deployment for Firewall Interworking 11
2.3.3 Deployment for Interworking with the CIS 12
2.3.4 Deployment for Interworking with the Firewall and the CIS of Basic Edition 13
3 Product Features 14
3.1 Comprehensive Traffic Detection 14
3.2 Detection of Mainstream Applications and Files 14
3.3 Simulation of Mainstream Operating Systems and Applications 14
3.4 Layered Defense System 14
3.5 Near-real-time Processing 14
3.6 Anti-evasion 15
3.7 C&C Detection 15
4 Product Specifications 16
5 Hardware Configuration 18

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 was attacked by 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

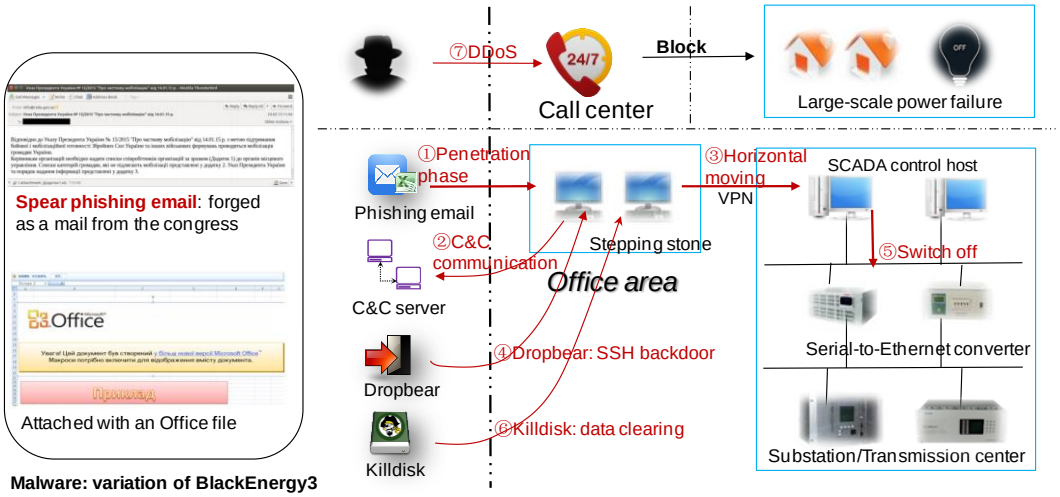
Since Google admitted being attacked in 2010, APT has become a hot topic in the information security circle.

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, fossil 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.

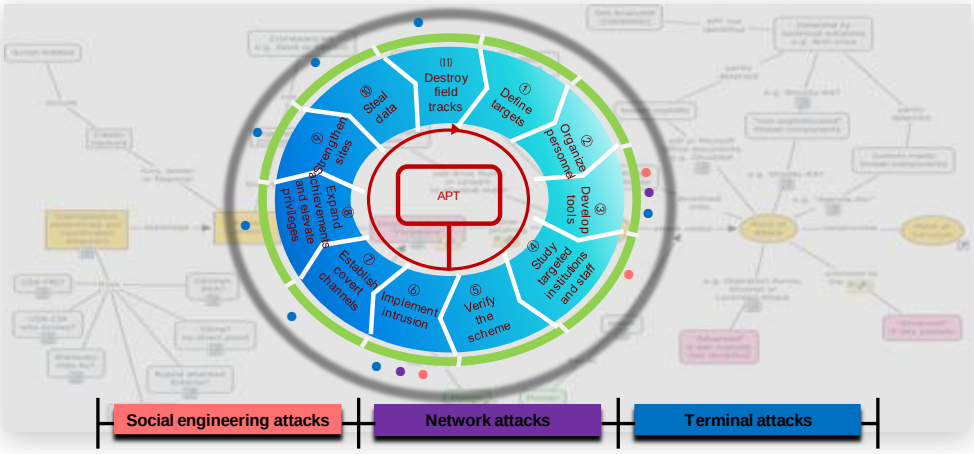
1.2 APT Development Trend

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 DOC, 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 preventing next-generation threats represented by APTs. Therefore, how to deal with the next-generation threats has become a headache of all enterprises.

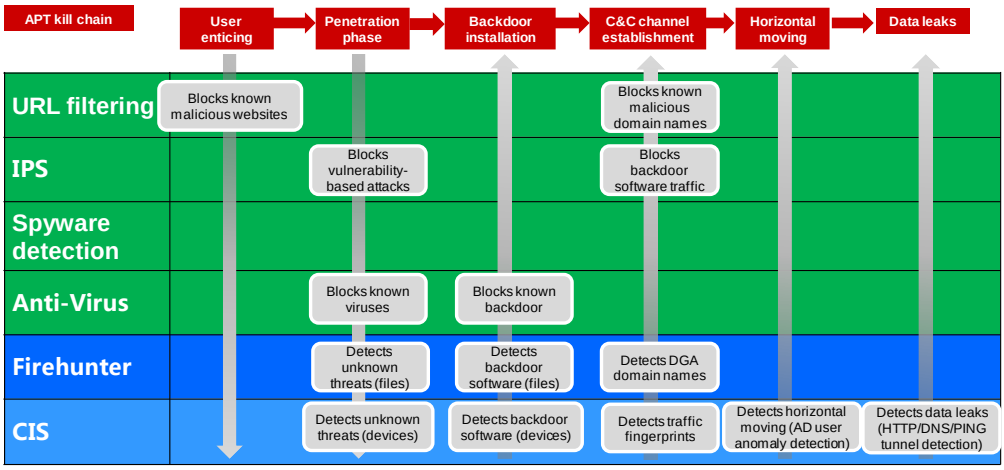
2 Security Protection Solution

Figure 2-1shows an APT kill chain and protection measures for all phases of the kill chain. An APT kill chain includes enticement, penetration, backdoor installation, C&C channel establishment, horizontal moving, and secret theft. Especially in the phases of penetration, backdoor installation, and C&C channel establishment, attackers try hard to break through security defenses by technical means, enter the targeted networks, and establish control and theft channels for preparation of ultimate attacks.

With advanced technical capabilities, Huawei proprietary FireHunter can help customers identify APT attacks in the phases of penetration, backdoor installation, and C&C channel establishment respectively 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 malicious software, and identifies APT attacks in the phases of penetration and backdoor installation. After successful penetration, 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 Domain Generation Algorithm (DGA) for identifying C&C attacks caused by requesting or accessing DGA malicious domain names.

Figure 2-1 APT kill chain and protection chain

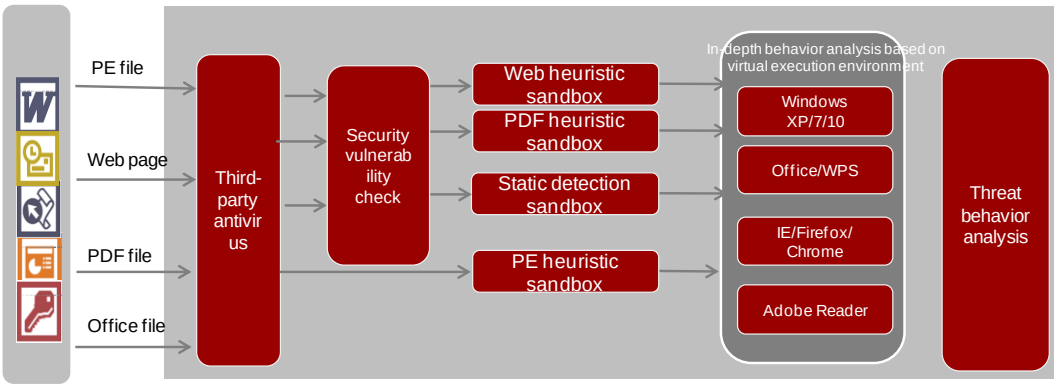


- The FireHunter performs detection mainly in the penetration phase, backdoor installation phase, and C&C communication phase.
- The CIS performs detection and analysis mainly in the horizontal moving phase and data leaks phase.
- An integrated solution of CIS + FireHunter covers the APT kill chain detection and provides the capabilities of investigating incidents and collecting evidences for the whole kill chain.

2.1 File Detection Technology Principles

As shown in Figure 2-1, an APT kill chain includes enticement, penetration, backdoor installation, C&C channel establishment, and secret theft. Penetration is the most important phase in the APT kill chain. Successful penetration is the basis for the subsequent attack phases. The file detection technology can effectively detect malware and identify unknown threats in the penetration phase and backdoor installation phase. Traditional security products cannot do this.

Figure 2-2 File detection technology principles



File detection includes third-party antivirus detection, security vulnerability check, static & heuristic sandbox detection, and behavior detection based on the virtual execution environment. It implements correlation analysis for all detection results and finally gives the threat detection result.

Different sandboxes are introduced as follows:

1. PE heuristic sandbox
   - Simulates the operating system environment, CPU instructions, and API calls.
   - Monitors the software instruction stream and API call stream.
   - Matches the specific features of virus families about static instructions and API calls for static analysis through disassembly instruction, API calls, and parameters.
   - Simulates executable files, monitors threat behavior, and matches the specific behavior and behavior sequence of virus families.
   - Analyzes abnormal file formats and attributes.
2. Web sandbox
   - 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.
3. PDF sandbox
   - 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. Static sandbox
   - 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 shellcode.
   - Matches virus family features.
5. Virtual execution sandbox
   - Uses the virtualization technology to simulate the operating system and other software environment.
   - 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.

2.2 C&C Detection Technology Principles

If user enticement and system 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 command control channels are not often changed. Therefore, you can use the traditional intrusion detection method to detect APT command control channels. The key to success is to

obtain detection features of command control channels for all APT attack means in time. In addition, it is a common attack means in recent years that attackers generate and register a domain name using DGA, entice users to access the malicious website, and plant Trojan horses to establish C&C channels.

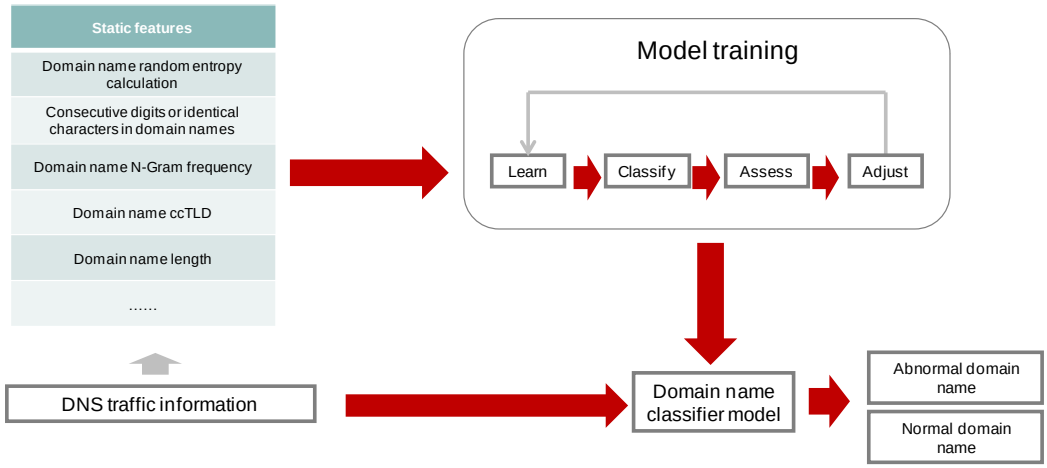
The FireHunter provides two C&C detection technologies: C&C detection based on remote control tool features and DGA malicious domain name detection.

1. C&C detection based on remote control tool features
   - Is a traditional detection method based on features.
   - Extracts features from flow information and compares them with remote control tool features.
2. DGA malicious domain name detection

   DGA malicious domain name detection uses machine learning and specific algorithms. Figure 2-3 shows the detection process.

   The detection process is as follows:
   - The FireHunter extracts domain name features based on traffic information and generates a classifier through model training.
   - After detecting new traffic, the FireHunter extracts domain name-related features and sends them to the classifier. The classifier determines whether the domain name is normal.
   - The FireHunter adjusts model training parameters and feature formats based on the classifier's detection results to make the classifier more accurate.

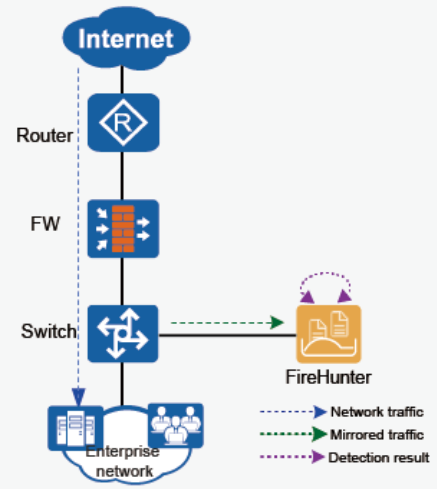
Figure 2-3 DGA detection principles



2.3 Typical Application Scenarios

2.3.1 Off-line Deployment for Traffic Restoration

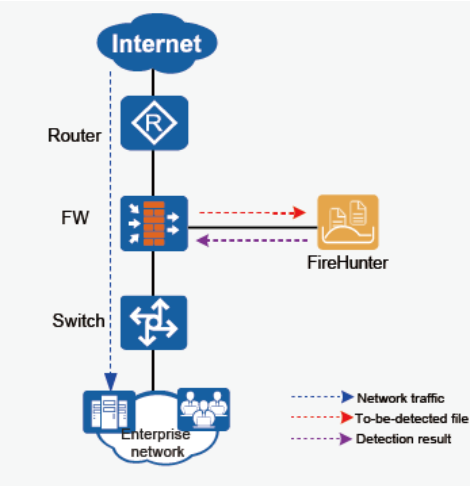
Figure 2-4 Off-line deployment for traffic restoration



In the independent deployment scenario, the mirroring port of the FireHunter is directly connected to that of the switch or other gateway. The switch or other 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.

2.3.2 Off-line Deployment for Firewall Interworking

Figure 2-5 Off-line deployment for firewall interworking



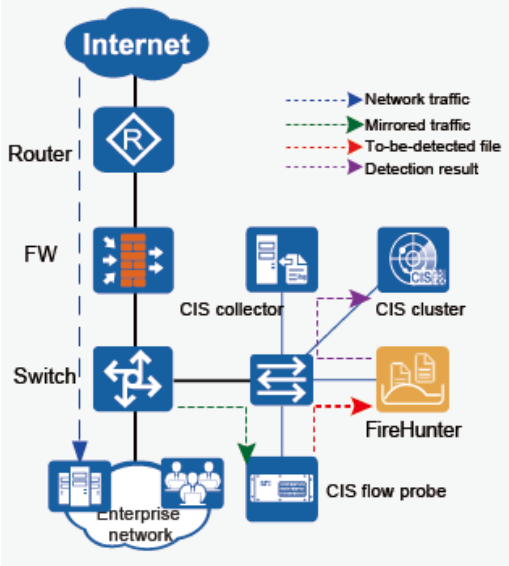
In the scenario where the FireHunter interworks with the firewall, it is necessary to ensure that the FireHunter's interworking interface is reachable. When network traffic passes through

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 can further provide 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.

2.3.3 Deployment for Interworking with the CIS

Figure 2-6 Deployment for interworking with the CIS

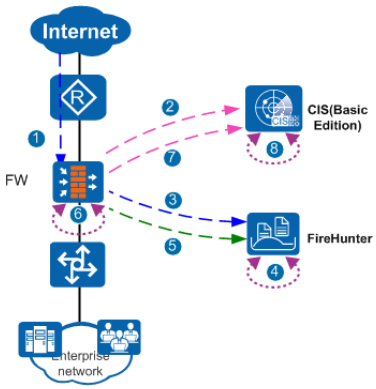


When the FireHunter interworks with the CIS, it is also necessary to ensure that the sandbox interworking interface is reachable. In this scenario, the CIS flow probe receives mirrored traffic, restores the traffic to files, and sends files to the FireHunter through the FireHunter's interworking protocol.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

2.3.4 Deployment for Interworking with the Firewall and the CIS of Basic Edition

Figure 2-7 Deployment for interworking with the firewall and the CIS of 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 of 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 of basic edition.
8. The CIS of 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 of 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.

3 Product Features

3.1 Comprehensive Traffic Detection

The FireHunter provides an independent traffic restoration capability. It can 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.

3.2 Detection of Mainstream Applications and Files

The FireHunter can detect and analyze mainstream applications and files, such as DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, HTML, JS, EXE, JPG, GIF, PNG, CHM, SWF, executable scripts, and compressed files.

3.3 Simulation of Mainstream Operating Systems and Applications

The FireHunter is capable of simulating 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.

3.4 Layered Defense System

The FireHunter provides the reputation system, signature-based attack detection method, heuristic detection engine, and virtual execution environment, improving the capabilities of coping with next-generation threats represented by APTs. The FireHunter also provides a list of all risky operations of next-generation threats to help customers gain visibility into the attack process and targets.

3.5 Near-real-time Processing

The FireHunter reduces the detection response time of next-generation threats from weeks to seconds and interworks with the NGFW for online attack defense.

3.6 Anti-evasion

The FireHunter detects evasion techniques by running code in virtual machines or based on user interaction.

3.7 C&C Detection

The FireHunter supports not only the traditional signature-based C&C attack detection, but also the DGA malicious domain name detection based on machine learning and a specific algorithm.

4 Product Specifications

Function	Indicator 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 features.
	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.
Traffic restoration	L2 protocols: VLAN and PPPoE

Function	Indicator Requirement
supported protocol (traffic is directly transmitted to the FireHunter for independent deployment)	L3 and L4 protocols: IPv4, TCP, UDP, ICMP, and GRE
	Application layer protocols: HTTP, SMTP, POP3, IMAP, FTP, NFS, and SMB
Sandbox environment support	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.

5 Hardware Configuration

Model	FireHunter6300
Network port	8 x Gigabit electrical port 2 x 10GE optical fiber port (optional)
Hard disk	SATA 2TB*4(RAID10) SATA 2TB*2(RAID1)
SSD	2 x 200 GB (RAID1)
Processing performance	70,000 files per day
Power module	Redundant AC power supplies
Dimensions (H x W x D)	86.1 mm (2 U) x 447 mm x 748 mm