Huawei FireHunter6000 series sandbox

Huawei FireHunter6000 series sandbox

Product Overview

Advanced Persistent Threats (APTs) often use social engineering to obtain contact information and send phishing emails to unsuspecting people. They exploit security vulnerabilities in Internet of Things (IoT) devices, and hide, without being detected, in high-value business assets to steal or compromise target information. Attacks are commonly seen in compromised infrastructure, such as the finance sector, resource suppliers, and government agencies, affecting people's livelihoods. Before launching attacks, perpetrators are usually well-prepared and wait patiently for their opportunity. Once attacks are launched, perpetrators usually use technologies, such as advanced evasion techniques in combination, to exploit known vulnerabilities. This makes the security devices that detect attack traffic ineffective.

The Huawei FireHunter6000 series of sandbox products is a new-generation, high-performance APT detection system that can accurately identify malicious files and malicious external Command & Control (C&C) connections. FireHunter6000 series products are designed to work in conjunction with next generation firewalls (NGFWs), analyzing the extracted suspicious files in a virtualized environment to identify viruses and unknown malicious attacks. Huawei FireHunter6000 series products can analyze and collect static and dynamic behavior of advanced malware through reputation-based scanning, real-time behavior analysis, and threat intelligence update from the cloud. With the unique Huawei ADE threat detection engine, the FireHunter6000 series and NGFW can detect, block, and report suspicious traffic, effectively preventing the spread of unknown threats and loss of core enterprise information assets.

Product Features

Inspection of over 50 File Types for Comprehensive Detection of Unknown Malware

- **Comprehensive traffic restoration and detection**
  The FireHunter6000 is capable of identifying all major file transfer protocols, such as HTTP, SMTP, POP3, IMAP, FTP and SMB, and detecting malicious files transmitted using these protocols.
- **Detection of major file types**
  The FireHunter6000 can detect malicious code in major application software and over 50 file types, including PE, PDF, Web, Office, images, scripts, SWF, and COM.

Multi-layer In-Depth Detection with 99.5% Accuracy or above

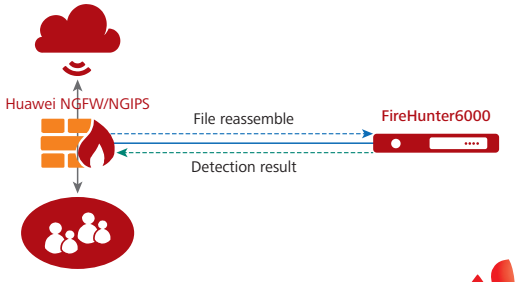
- **Simulating multiple software operating environments and operating systems**
  The FireHunter6000 provides heuristic detection for PE, PDF, and Web files, and virtual execution environment. The virtualized execution environment supports various versions of Windows operating systems, browsers, and office software.
- **Combined static and dynamic detection**
  Static detection analyzes code snippets, abnormal file formats and malicious behavior in scripts to pinpoint suspicious traffic. This is combined with dynamic detection which monitors the instruction stream, identifies files and server operations and provides correlation analysis to determine traffic legitimacy.
- **Advanced anti-evasion**
  Numerous anti-evasion technologies prevent malware from staying stealth and evading detection.

Detection and Rapid Blocking of Malware in seconds

- **Industry-leading performance**
  Scalable sandbox throughput by deploying multiple FireHunter sandboxes in clusters.
- **Real-time processing**
  Provide threat detection and response time in seconds.
- **Detailed threat reports aid in O&M and decision-making**
  Detailed reports include results of file inspection, relevant session information, abnormal file formats and behavior, abnormal network communication, and behavior of the virtual execution environment, network and host.

Product Deployment

- **Deploy in conjunction with NGFW/NGIPS devices**
  NGFW/NGIPS devices reassemble files, decrypted (SSL) if necessary and send them to the sandbox for inspection.
- **Single-node deployment**
  Traffic is mirrored onto the sandbox to be reassembled and inspected.



Huawei FireHunter6000 series sandbox

Product Specifications

Hardware		
Model	FireHunter6200	FireHunter6300
Performance	1Gbps	2Gbps
File Detection	50,000 files/day	100,000 files/day
Hard Disk	Data disk: 2TB*2, RAID1; System disk: 2TB*2, RAID1	Data disk: 2TB*4, RAID10; System disk: 2TB*2, RAID1
Height	2 U	
Power source	Dual power redundancy	
Fixed port	8 x GE electrical ports (1 Gigabit management port, 3 Gigabit spare ports, and 4 Gigabit listening ports) 2 x 10GE optical ports (optional)	
Major Functions		
Category	**Description**	**Detailed Description**
Supported operating systems	Windows XP, Windows 7/10	Simulation of multiple types of operating systems, dynamic detection in a virtual execution environment
Protocols supported in traffic restoration	Restoration of traffic of multiple protocols	Restoration of HTTP, SMTP, POP3, IMAP, and FTP traffic
File types supported in detection	Compressed files	GZ, RAR, CAB, 7ZIP, TAR, BZ2, and ZIP files
	PE	EXE, DLL, and SYS files (detection of 32-bit PE files not supported)
	Office 97 to Office 2003	DOC, XLS, and PPT files
	Office 2007 and later	DOCM, DOTX, and DOTM files XMSM, XMTX, XLTM, and XLAM files PPTM, POTX, POTM, PPSX, PPSM, and PPAM files
	RTF	RTF files
	Image	JPG, JPEG, PNG, TIF, GIF, and BMP files
	WPS	WPS, DT, and DPS files
	Web page	HTM, HTML, and JS files
	Video	SWF files
	Java	JAR and CLASS files
	PDF	PDF files
	Python	PY, PYC, and PYO files
	Executable scripts	CMD, BAT, VBS, VBE, RUBY, PS1, and PY files
Built-in antivirus detection	Built-in antivirus function supports the detection of CHM, ASP, PHP, COM, and ELF files, in addition to the preceding file types.	
C&C anomaly detection	C&C malicious server external connection detection	DGA domain name detection algorithm-based detection of random malicious domain names for C&C external connections
Report output	Output of detailed malicious file detection reports that contain the file detection details, threat behavior category, and dynamic behavior analysis	
Machine-readable IOC threat intelligence	Output of abundant machine-readable indicators of compromise (IOC) for intelligence sharing between northbound and southbound interfaces	