FORTINET

White Paper

Fighting Advanced Threats

With FortiOS 5

Introduction

In recent years, cybercriminals have repeatedly demonstrated the ability to circumvent network security and cause significant damages to enterprises.

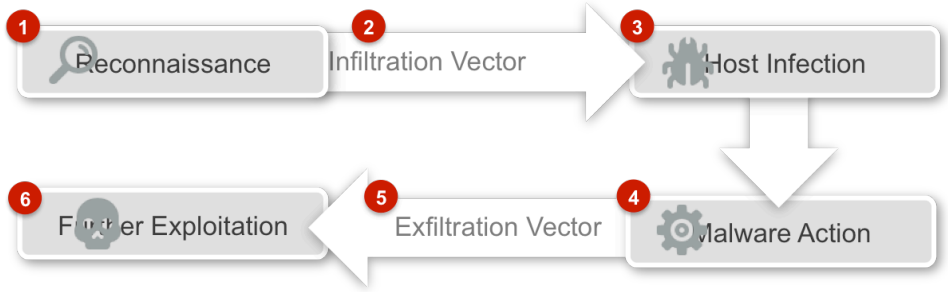
This whitepaper will discuss the changing threat landscape and the best practices in securing networks against them.

Next Generation Threats

Cybercriminals today are organized, sophisticated and have powerful resources at their fingertips. In most cases, attacks are initiated with specific targets and objectives in mind. The aim is to infiltrate hosts in networks and steal valuable data. The data may be personal information, accounts or intellectual property. This information can be used for future attacks (second stage) to further penetrate networks.

These attacks are often crafted to evade common traditional security tools, such as firewalls, intrusion prevention systems and antivirus gateways. This is referred to as advanced evasion techniques, or AETs. They're low-profile, targeted and stealthy, avoiding notice and suspicion. These threats are a combination of malware – executable code running on the attack target – and exploits for vulnerabilities, weaknesses on a system. These exploits can attack what is known as a zero-day vulnerability, a software flaw to which there is no patch, update or fix. These attacks usually cannot be detected by signature-based filters that compare them to known attacks. Other advanced threats include spearphishing, impersonation and polymorphic malware.

Threats that we see today typically adopt a six-stage lifecycle:



1) Reconnaissance

Unlike typical malware infiltration, advanced threats either perform initial probes towards targets or collect information about them by various means, such as phishing, social engineering or obtaining intel from other infected hosts.

2) Infiltration Vector

Armed with relevant information, these threats infiltrate their targets in various ways – these are also known as attack vectors. Think of these vectors as things like phishing emails, malicious flash (SWF) or PDF documents, malicious websites that attack flaws in browsers like Internet Explorer or Firefox. Phishing emails can be targeted and very convincing, with the goal to get the victim to click on a malicious link or open an attachment. These are known as spear phishes.

3) Host Infection

To evade traditional security systems, malware transmissions are typically encrypted and arrive via unexpected routes like corporate email with a file share invitation or a prompt for software updates from an impersonated site. There are many tricks that modern malware employ, including security software evasion – code specifically designed to destroy antivirus processes running on the system. Another trick is polymorphism, code that shifts shape constantly to escape signature-based antivirus detection.

4) Malware Action

Once the malware is installed, it often attempts to initiate a call back, using common transmission methods that are allowed by typical security policies. Otherwise, it keeps a low profile, generating no activities that are likely to be noticed. It remains in sleep mode, awaiting further instructions. Increasingly, malware is aware of its environment and won't allow itself to be detected in a virtual machine sandbox.

5) Exfiltration Vector

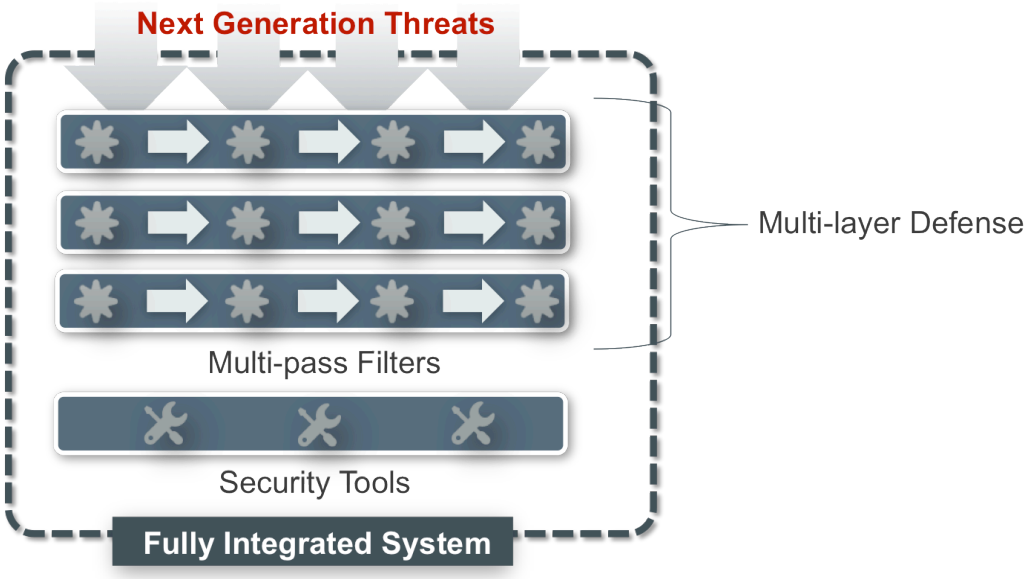
The exfiltration usually involves the surreptitious delivery of stolen data via often encrypted but common channels, such as HTTPS, back to the command center or to another compromised system controlled by cybercriminals.

6) Further Exploitation

With successful communication links between the command center and the compromised hosts, further exploitation is easy to accomplish. These malicious acts include attempts to access materials the host has connection to, such as documents on servers, cloud-based applications and database credentials.

Best Practices against new advanced Threats: Advanced Persistent Defence

In order to defend against advanced threats, organizations must update and adjust existing network security and adopt new security implementations.



The challenge is to add protection to the network without straining budgets, resources or performance. The components of a comprehensive approach are:

- Multi-layer Defense System
- Multi-pass Anti-Malware Protection
- Integrated Systems & Security Tools

Multi-layer Defense System

Next generation threats use multiple vectors of attack to exploit weak defenses, avoid detection and increase the odds of penetration.

To detect these threats, organizations can no longer simply rely on a single solution; multiple layers of defense are needed to fill possible network security gaps. Multi layer defense seeks to detect polymorphic malware, prevent receipt of phishing emails, block connection to compromised websites, and deny malware access to its command channel.

Multi-pass Anti-Malware Protection

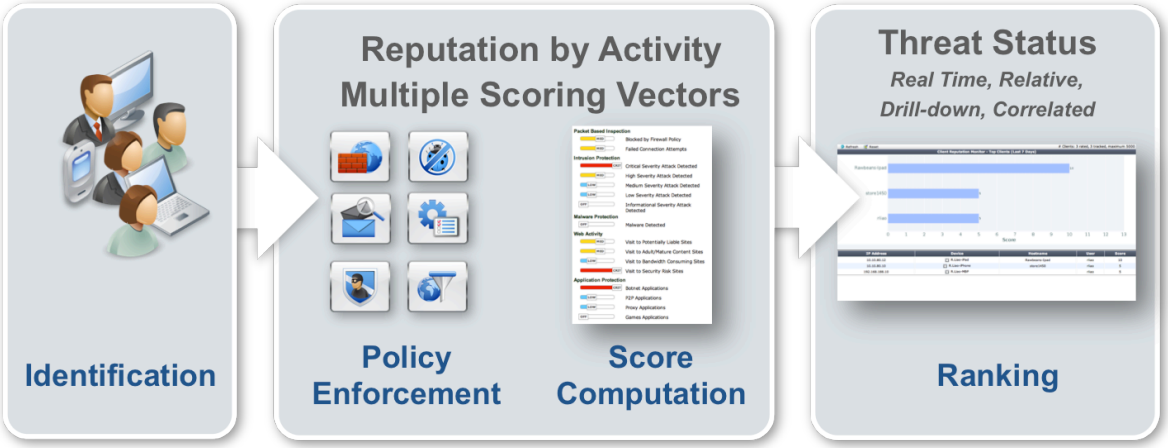
Detecting and blocking stealthy malware is becoming more challenging. Many malicious codes are now designed to evade traditional signature-based filters. Although antivirus signatures remain a critical part of the solution, new proactive real-time technologies that don't rely on signatures are necessary for air-tight protection. An intelligent virus inspection engine is key to proactively detect these threats.

Cloud-based services with real-time databases and robust processing resources are also an important component.

Integrated Systems & Security Tools

Cybercriminals no longer work alone. They use coordinated expertise and share resources, producing disparate components that challenge many typical network security implementations. It's difficult to collate information to identify and deter these advanced threats.

It's important to integrate security components in the network, including threat and network activity correlations. Deploying an integrated security platform can yield even more benefits, like efficient traffic processing, with better network performance and low-latency communications.

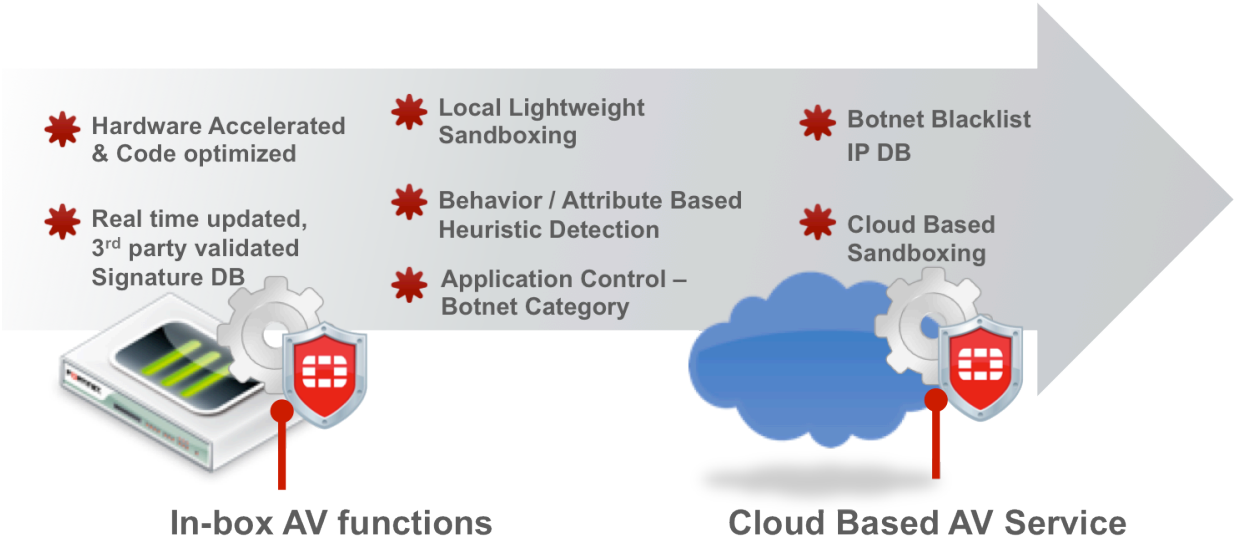


There should be abilities to correlate threat landscape information, enabling administrators to use a cumulative security ranking of network terminals to spot suspicious activities that might evade detection in a typical isolated setup. This client reputation capability allows administrators to detect signs of advanced threats within their networks and set up appropriate responses.

Most malicious infections are the result of exploits on vulnerable hosts, particularly those with out-of-date operating systems and application patches, weak passwords or poorly configured security settings. Vulnerability scans are one of the most useful tools against these threats, identifying weaknesses before the bad guys do.

How FortiOS 5 fights next generation threats

FortiOS 5 has enhanced anti-malware capabilities, including file analysis with intelligent sandboxing and a botnet IP blacklist. We introduced the patent-pending client reputation system to assist administrators in protecting their networks with advanced analytics and controls.



FortiOS 5 includes:

A) AV Signatures

Detect and block known malware and most of its variants. Highly accurate with few false positives. The signature approach is backed by a sophisticated antivirus engine that can detect polymorphic malware. In fact, the signatures are quite intelligent. For example, one single signature can detect over 50,000 polymorphic viruses in some scenarios.

B) Behavioral and attribute-based heuristic detection

Detects and blocks malware based on a scoring system of known malicious behaviors or characteristics. This detects malware that doesn't match a signature, but behaves similarly to known malware. Used to flag suspicious files for further analysis, either local or cloud based.

C) File Analysis

Detects new threats by running suspicious files in a contained emulator to determine whether they're malicious. This technique is resource-intensive and may impact performance and latency while increasing visibility for zero-day or previously unknown threats. Modern malware is written to detect such analysis machines, however Fortinet's file analysis engine has lots of technology built in to defeat these counter-measures cyber criminals employ.

D) Application Control

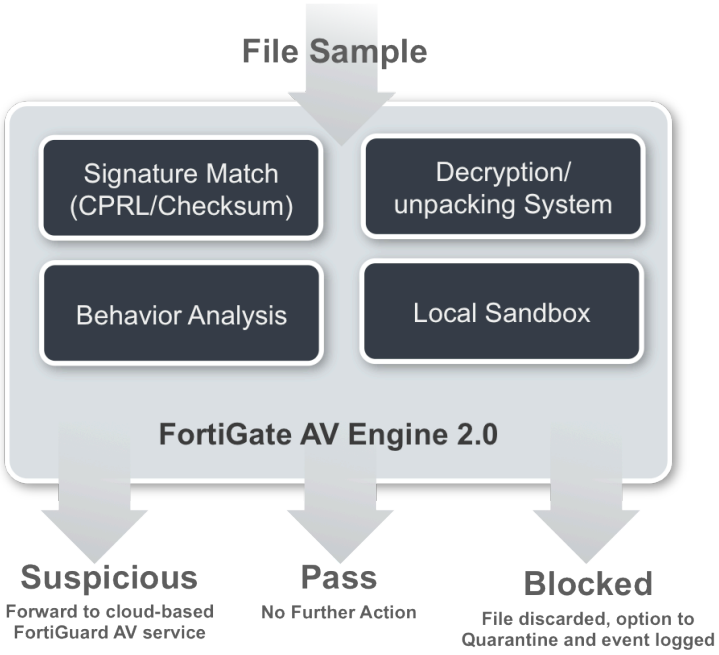
Detects and blocks known botnet activities by examining traffic that passes through the gateway. Also effective in preventing zombies from leaking data or communicating instructions. This is known as chatter. By identifying and blocking chatter, these threats are mitigated since it doesn't matter what URL, domain, or IP the infected host is trying to connect to.

E) Botnet Servers Backlist Filter

Detects and blocks known botnet command and control communication by matching against blacklisted IP addresses. Stops dial-back by infected zombies.

FortiGate AV Engine 2.0

The new engine is designed to detect and block today's advanced threats. It provides inline file processing capability that utilizes the FortiGate's hardware acceleration component.



A) Signature Match Processor

The signature match processor uses the unique and patent-pending Compact Pattern Recognition Language (CPRL), which is optimized for performance without compromising accuracy. With CPRL, a single signature is able to cover well over 50,000 different viruses, including zero-day virus variants as previously mentioned. The processor also performs blacklisted file checksum matching for common large-volume static malwares. To achieve this, FortiGuard analysts go through intensive training to write optimized CPRL signatures.

B) Decryption/Unpacking System

Most modern malware is compressed or encrypted to evade traditional file matching systems. This system unveils the actual content for further analysis to detect stealthy polymorphic malware. Think of it as matching the inner components, or true DNA of a virus.

C) Local Sandbox

This system consists of various OS-independent emulators and uses intelligent filetyping to execute suspicious codes, such as malware that uses JavaScript obfuscation.

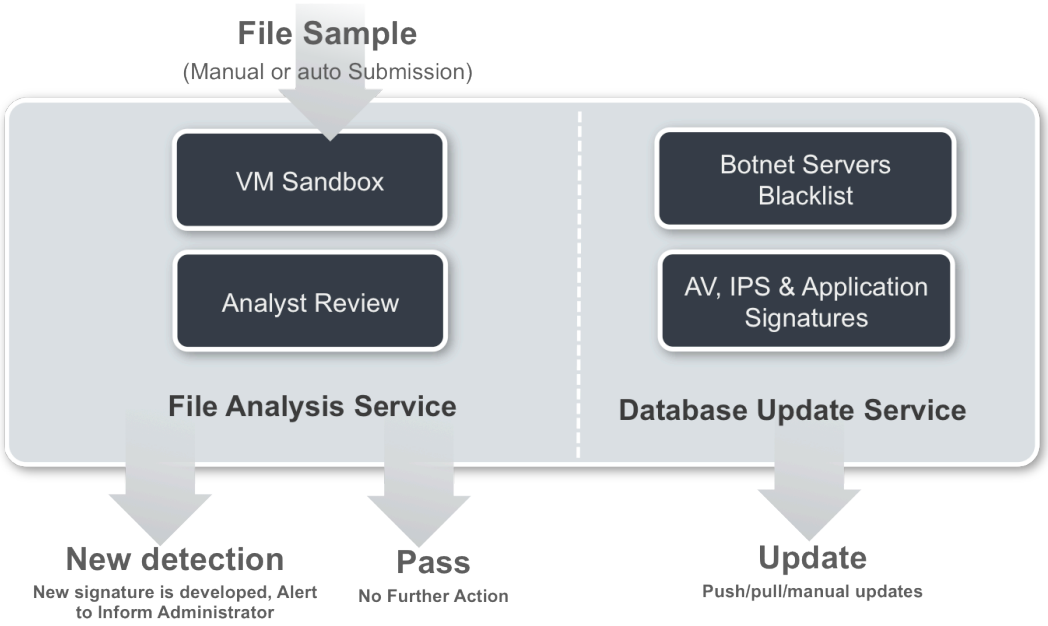
D) Behavior Analysis Engine

This heuristic engine performs behavioral and attribute-based analysis to detect zero-day malicious code for further analysis. It looks at the intent of a virus – what is it trying to do based on the executable code that is analyzed by the engine.

New FortiGuard Services

The new FortiGuard services are cloud-based capabilities that enhance the detection and provide real-time protection against next-generation threats.

Unlike some competitors' solutions, file submissions to FortiGuard services are minimal since the in-box local engine captures most malware.



A) Cloud Based Sandbox Environment & File Analysis

The sandbox environment consists of various operating system simulators that execute suspicious programs and compute a Bayesian score based on lists of activities and attributes.

FortiGuard antivirus researchers are based around the world, providing 24x7 round-the-clock malware analysis. New viruses and variants are examined to provide accurate detection, reduce false positives and discover new evasion techniques. When these techniques are discovered, researchers work side by side with Fortinet development to built in the appropriate technology to defeat evasion techniques.

B) Database Updates

Up-to-date signatures are essential in stopping malicious activities in the network. Apart from regular antivirus, intrusion prevention systems and application control signatures, FortiOS 5 introduces a new botnet blacklist database. With this new database, users will be able to prevent zombies in the network from communicating to botnet servers.

Conclusion

With FortiOS 5, Fortinet has taken the fight against advanced threats to a new level, breaking the lifecycle of today's malware to ensure comprehensive security without compromising performance.

GLOBAL HEADQUARTERS
Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia
Antipolis, France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480