



# Zombie ZERO

**A Reliable Choice for Defending APT  
Attacks and Data Exfiltration**



## TWO-LEVEL APT **Defense Solution**

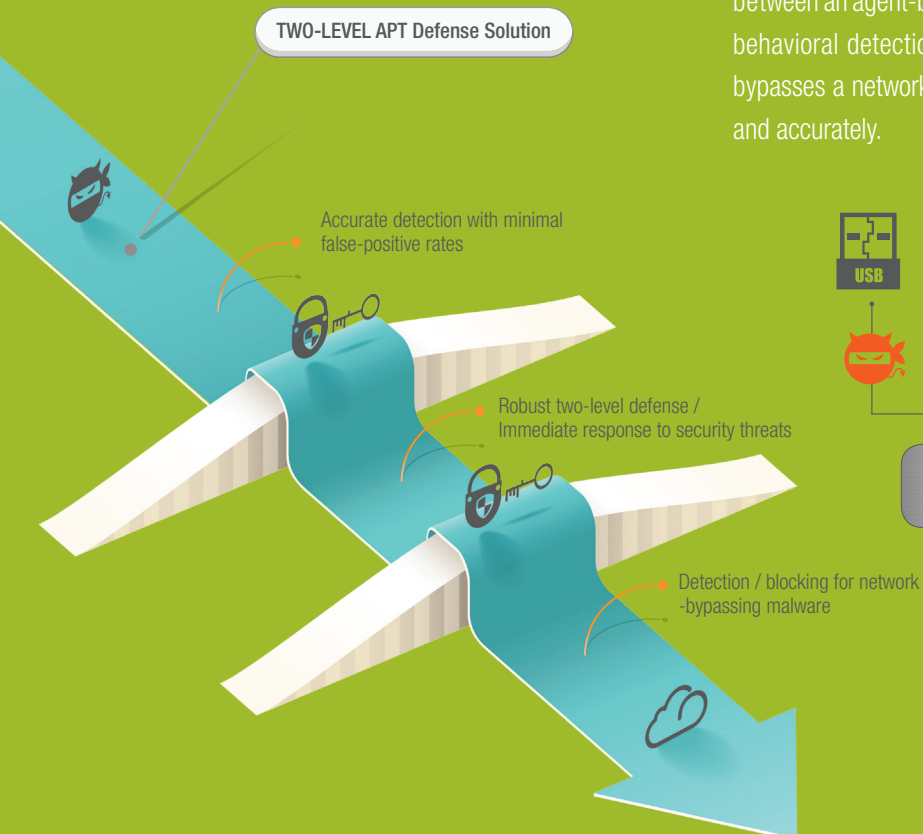
# Zombie ZERO

Advanced persistent threat (APT) is a new hacking technique used by cyber criminals to persistently attack target victims using various methods (e-mail, web, etc.) until their objectives are achieved. Zombie ZERO uses an agent-based behavioral detection system installed on PCs and a network-based behavioral detecting system analyzing files from network traffic through virtual machines. This is a new security solution designed to defend against APT attacks and detect malware. Zombie ZERO provides robust information security to prevent data exfiltration and network damages.

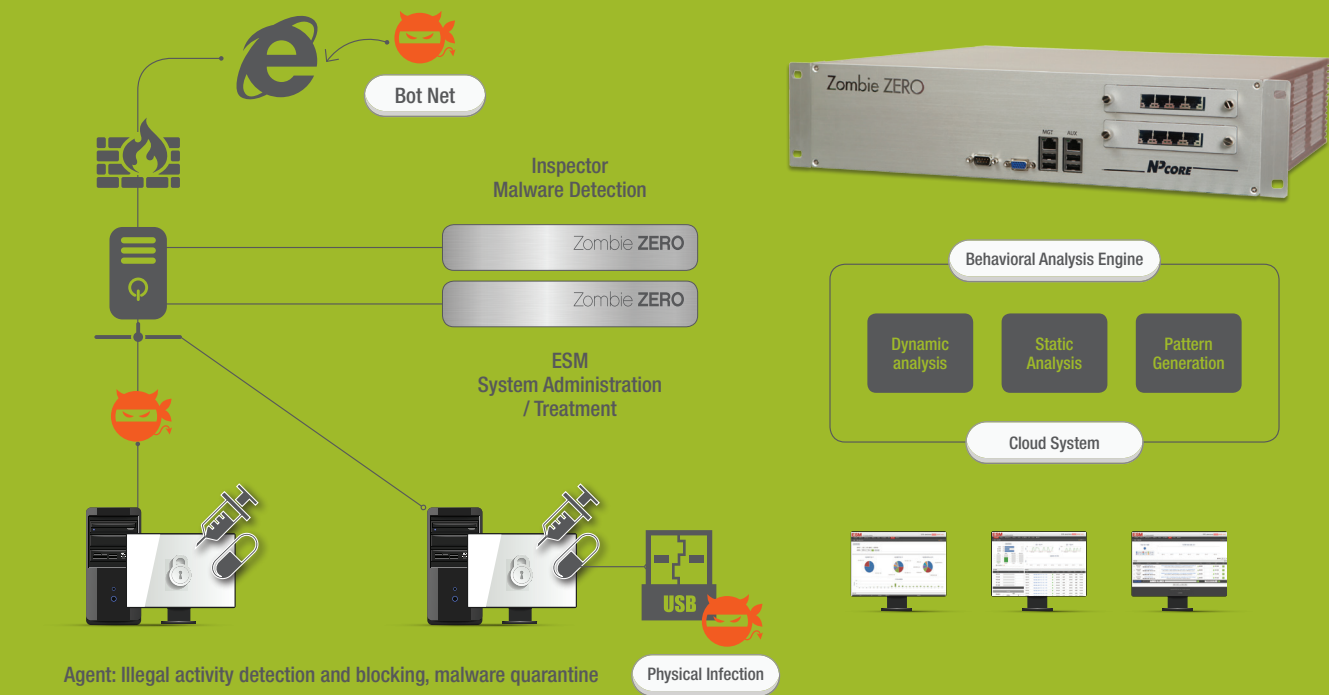


## TWO-LEVEL APT **Defense System**

The two-level defense system of Zombie ZERO, which interworks between an agent-based behavioral defense system and a network-based behavioral detection system, can defend the infiltrating malware that bypasses a network and responds with lower false-positive rates quickly and accurately.



# The Diagram of TWO-LEVEL APT Defense System



<p><b>Network-based Detection and Analysis</b> <b>ZombieZERO Inspector</b></p> <ul style="list-style-type: none"> <li>Malware detection through file analysis from network traffic</li> <li>Behavioral analysis through virtual systems</li> <li>Pattern generation for detected malware</li> </ul>	<p><b>Agent-based Analysis and Quarantine</b> <b>ZombieZERO Agent</b></p> <ul style="list-style-type: none"> <li>Detection and blocking based on behavioral analysis for malware</li> <li>Process management and detection / blocking of malicious changes</li> <li>Detection and quarantine for data exfiltration</li> </ul>	<p><b>System Management and Monitoring</b> <b>ZombieZERO ESM</b></p> <ul style="list-style-type: none"> <li>System operation and monitoring</li> <li>Generation of detailed logs and reports</li> <li>Centralized and policy-based management</li> </ul>
---	---	--

## Features of TWO-LEVEL Defense

<p><b>Interworking Analysis between Agent-based and Network-based systems</b></p>	<ul style="list-style-type: none"> <li>Accurate detection with minimal false-positive rates through interworking between agent-based and network-based analysis.</li> <li>Independent behavioral analysis on agent-based and network-based systems.</li> <li>Malware detection and blocking from bypassing the network security systems such as encrypted traffic, and other hidden threats.</li> <li>Blocking harmful outbound traffic.</li> </ul>
<p><b>TWO-LEVEL Defense</b></p>	<ul style="list-style-type: none"> <li>Firstly, network-based behavioral engines respond to the incoming files and secondly, agent-based behavioral engines respond to them at end-point.</li> </ul>
<p><b>Multiple Analysis</b></p>	<ul style="list-style-type: none"> <li>A signature-based anti-virus engine detects known malware and behavior-based engines detect unknown malware.</li> </ul>

## \*Certifications and Intellectual Property Rights

Zombie ZERO has received the CC (Common Criteria) and GS (Good Software) certifications, and U.S. and Korean patents that relate to intellectual property rights. So they guarantee the quality of products.

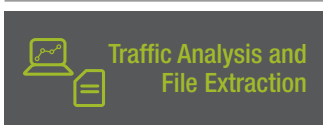
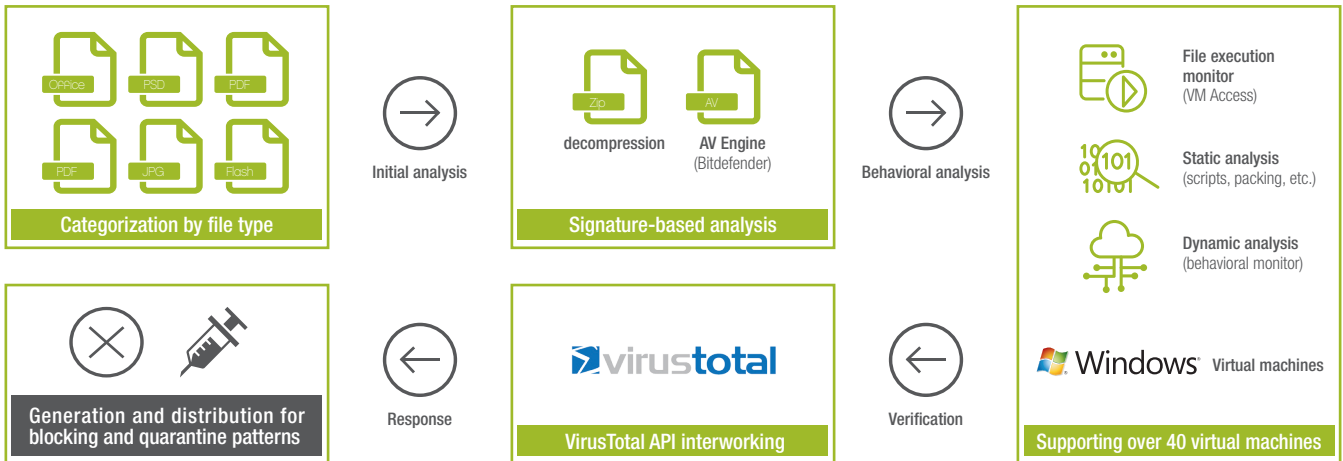


US Patent  
10-2011-0000572  
APPARATUS AND METHOD  
FOR BLOCKING ZOMBIE  
BEHAVIOR PROCESS

## Network-based Detection Solution

# ZombieZERO Inspector

ZombieZERO Inspector is made up of a network-based detection and analysis system that operates as a virtual system. Three step signature-based and behavioral analysis enables the system to prevent the internal potential threats in advance through detecting unknown, and variant malware.



### Traffic Analysis and File Extraction

#### Collection of incoming files through traffic analysis

- Collection of Incoming files being transferred via file transmission protocols such as Web, FTP, SMTP, IMAP, POP, etc.
- Analysis of Incoming files with various extensions (executable, compressed, document files, etc.).



### Three Steps of Malware Analysis



#### Step 1

Detection on signature-based anti-virus engines.



#### Step 2

Behavioral analysis on static and dynamic engines.



#### Step 3

Verification on VirusTotal engines from Google.

- Support signature-based and behavior-based analysis.
- Quarantine for the infected PC through signature patterns of the detected malware.
- Detection of malware attempting to bypass the virtual machines through the manipulation that eliminates virtual machine aware codes and forcing it into execution.



### Behavioral Analysis

#### Behavioral analysis on virtual systems

- Provide the sandbox made up of static analytical engines and dynamic analytical engines.
- Analyze the PE files (DLL, EXE, etc.), compressed files, and document files in various formats (MS Office, HWP, PDF, etc.).
- Determine the presence of malware through monitoring and analyzing the behavior of processes, files, networks, and memory by the dynamic analytical engines after suspicious files are executed.
- Provide details about the analysis of the static analytical engine (PE-static, document-static) to detect attacks, source codes, and scripts aiming at software weaknesses.

## Strengths



### Dual Detection and Blocking of C&C Server Connection

- Detection of C&C connection through analysis of outbound URL and URI connecting patterns.
- Dual monitoring and blocking (DNS Sinkhole, TCP Reset) C&C server connections from internal users.
- Live-update for C&C database in real-time by interworking with NPCore and KISA (Korea Internet and Security Agency) analytical centers.



### Detection of Malicious Behavior through the Intelligent Analysis of Incoming and Outgoing Traffic

- Detect malicious activities of the files using web and e-mail protocols.
- Detect harmful traffic such as C&C server connections and DDoS attacks caused by internal users.



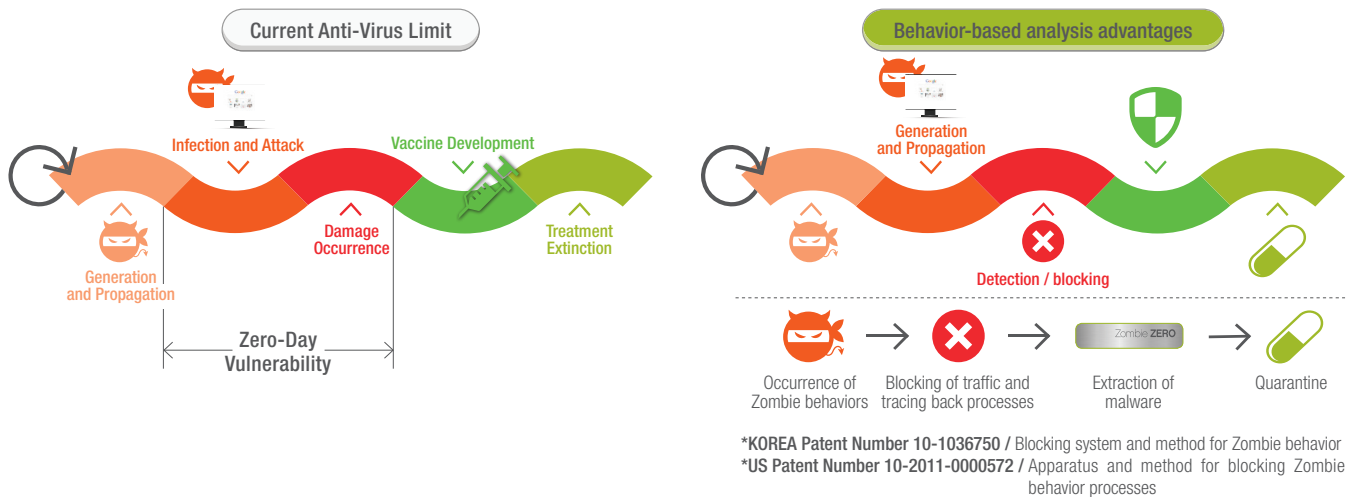
### Analysis in High-volume Traffic

- NPCore's Multi-core Processing "SmartNIC" with its own traffic-processing capacity enables Advanced Analysis in High-volume Traffic
- Collect all packets on 20Gbps bandwidth, even with a small packet size.

## End-point **Detection and Blocking Solution**

# ZombieZERO Agent

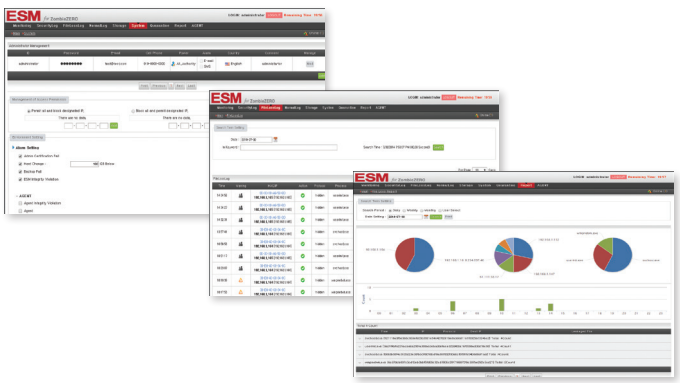
ZombieZERO Agent uses a behavior-based analytical engine that detects, blocks, and quarantines new and variant malware without patterns. Therefore, it detects malware in real-time that attempts to bypass.

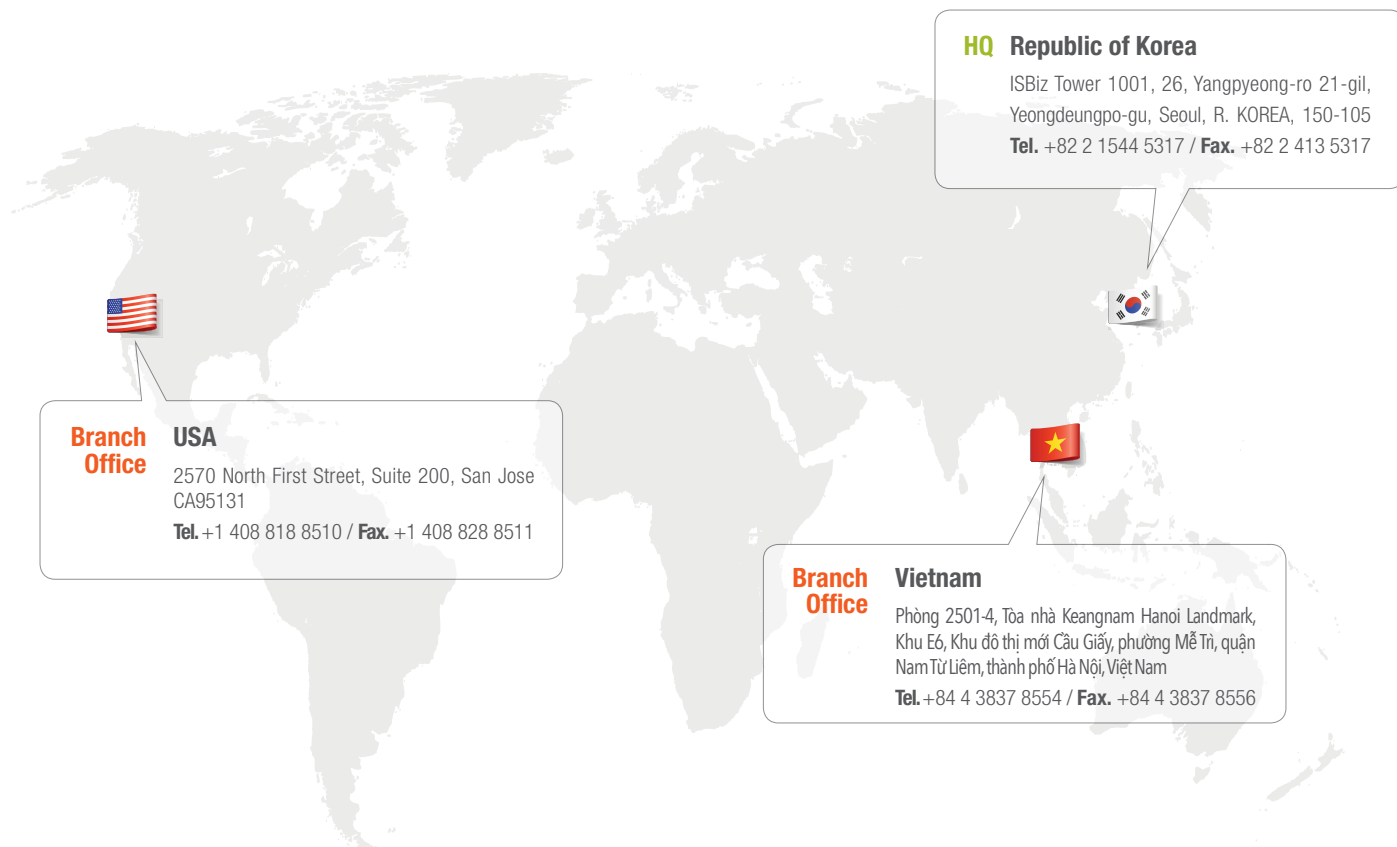


## Strengths

 <b>Behavior-based Malware Detection</b>	<ul style="list-style-type: none"><li>Minimal risk of false-positive detection through multiple step analysis of processes, files, and traffic.</li><li>Fundamental blocking of harmful activities (DDoS attacks, data exfiltration, screen capture, etc.) through an agent-based behavioral engine at end-point.</li><li>Capability of independent detection and quarantine without network-based system through a built-in behavior analytical engine with patented technology.</li></ul>
 <b>Data Exfiltration Detection and Blocking</b>	<ul style="list-style-type: none"><li>Fundamental detection and blocking of data exfiltration and harmful traffic from malware by distinguishing between user behavior and process behavior.</li><li>Fundamental blocking of commands on the zombie PC from hackers by detecting reverse connections.</li><li>Detection and blocking of the user screen monitoring on PC in real-time from hackers via network</li><li>Detection and blocking of DDoS attacks and system hackings.</li><li>Detection of file transmission through web mail and messengers.</li></ul>
 <b>Guaranteed System Stability and compatibility with Other Network Devices</b>	<ul style="list-style-type: none"><li>Provide system stability and minimize the use of resources through installation on kernel driver level that avoids conflicts with other programs.</li><li>Provide efficiency of enhanced security and management cost of two-level protection through interworking with other existing network devices.</li></ul>
 <b>Response to Malware targeting Vulnerabilities in Applications</b>	<ul style="list-style-type: none"><li>Respond to malware targeting vulnerabilities in document editors such as MS Office, Adobe Reader, etc., and web browsers such as IE, Firefox, Chrome, etc., or media players, messengers, etc.</li></ul>

## System Management and Monitoring

<ul style="list-style-type: none"><li>Monitoring in real-time for main conditions such as system data, zombie PCs, harmful traffic, etc.</li><li>Remote and centralized management via user-friendly web interface.</li><li>Provide summaries of malware infections and treatments.</li><li>Provide daily, weekly, and monthly statistical reports based on the administrator's demand</li><li>Keyword searching for the administrator's convenience.</li><li>Group generation based on IP addresses for management and policy setting for each group.</li></ul>	
--	--



**Branch  
Office**

**USA**

2570 North First Street, Suite 200, San Jose  
CA95131

**Tel.** +1 408 818 8510 / **Fax.** +1 408 828 8511

**HQ Republic of Korea**

ISBiz Tower 1001, 26, Yangpyeong-ro 21-gil,  
Yeongdeungpo-gu, Seoul, R. KOREA, 150-105

**Tel.** +82 2 1544 5317 / **Fax.** +82 2 413 5317

**Branch  
Office**

**Vietnam**

Phòng 2501-4, Tòa nhà Keangnam Hanoi Landmark,  
Khu E6, Khu đô thị mới Cầu Giấy, phường Mỹ Trì, quận  
Nam Từ Liêm, thành phố Hà Nội, Việt Nam

**Tel.** +84 4 3837 8554 / **Fax.** +84 4 3837 8556

Zombie **ZERO**

[www.npcore.com](http://www.npcore.com)