CHECK POINT
ANTI-BOT SOFTWARE BLADE

FEATURES

Integrated Anti-Bot Network Solution

- Post-infection protection by discovering bots and stopping their damage
- Management, reporting and policy unified with Antivirus Software Blade
- Available on every gateway
- Optional SandBlast Agent provides Anti-Bot protections on the endpoint

Powered by ThreatCloud™

ThreatCloud is the first collaborative network to fight cybercrime that feeds security gateway software blades with real-time security intelligence

- 20 million unique websites used for bot communications with a command and control server
- 12 million malicious file signatures
- 3.5 million malicious websites

Multi-tiered ThreatSpect™ Bot Detection Engine

Discover infections by correlating multiple bot detection methods

- Reputation of IPs, URLs, DNS addresses
- Patterns detection of bot communication
- Scan for bot actions
- Unified protection and management integrated with the Anti-Bot Software Blade
- Centrally managed from a single, user friendly console

BENEFITS

- Discover bots that have infiltrated your computers
- Stop APT Attacks
- Prevent damage such as stolen data
- Keep up with the ever-changing dynamic threat landscape with real-time intelligence from ThreatCloud
- Easily investigate infections, assess damage and decide on next steps with extensive forensics tools
- View and manage the "big malware picture" with integrated threat reports and dashboards

WHAT IS A BOT?

A bot is a malicious, stealthy software that invades your network and allows criminals to remotely control your computer. Cybercriminals can remotely execute illegal activities such as stealing data, spreading spam, distributing malware and participating in Denial of Service (DOS) attacks without your knowledge. Bots play a key role in targeted attacks also known as Advanced Persistent Threats (APTs). A multi-layered integrated threat prevention solution is needed to protect your company from such attacks.

CHECK POINT ANTI-BOT SOFTWARE BLADE OVERVIEW

The Check Point Anti-Bot Software Blade detects bot-infected machines and prevents bot damages by blocking communications from the cybercriminals' Command and Control (C&C) servers. Using a continually updated list of C&C addresses from ThreatCloud™, the largest real-time security threat knowledgebase from the cloud, the Anti-Bot Software Blade detects stealthy bots before they can do damage and affect users.

THE SOLUTION TO BOTS

Check Point Threat Prevention Solutions, including the Anti-Bot Software Blade, are powered by ThreatCloud™ which feeds the security gateway with up-to-the-second security intelligence with over 75 million addresses analyzed daily for bot discovery, over 12 million malware signatures and over 3.5 million malware infested websites.

THREATCLOUD

ThreatCloud is the first collaborative network to fight cybercrime. It delivers real-time dynamic security intelligence to security gateways. That intelligence is used to identify emerging outbreaks and threat trends. ThreatCloud powers the Anti-Bot Software Blade allowing gateways to investigate always-changing IP, URL and DNS addresses where Command and Control Centers are known. Since processing is done in the cloud, millions of signatures and malware protection can be scanned in real time.

ThreatCloud's knowledgebase is dynamically updated using attack information from worldwide gateways, feeds from a network of global threat sensors, Check Point research labs and the industry's best malware feeds. Correlated security threat information is then shared among all gateways collectively.

August 22, 2016

THREATSPECT™ BOT DISCOVERY ENGINE

Bots are stealthy, often hiding in your computer undetectable by common antivirus programs. The Check Point Anti-Bot Software Blade detects bot-infected machines with its ThreatSpect™ engine, a unique multi-layer discovery technology with up-to-the-minute updates feeds from ThreatCloud. ThreatSpect correlates information for accurate bot detection.

- Remote operator addresses including IP, DNS and URLs
- Detect unique botnet communication patterns
- Detect attack behavior such as spam or clickfraud

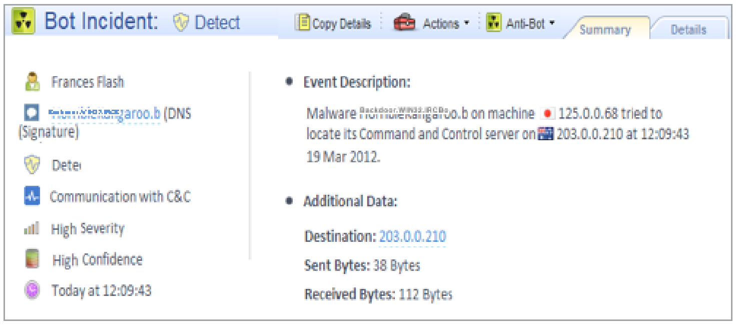
BLOCK BOT COMMUNICATION

Once a bot is detected, the Check Point Anti-Bot Software Blade blocks remote command communication between the infected machine and the C&C server, rendering the bot useless to the Cybercriminal and protecting the organization from potential bot damage.

INVESTIGATE BOT INFECTIONS

Seamlessly investigate bot infections with advanced logs and management system providing key inputs such as infected machine/user, bot name, bot actions (such as communication with command & control and spam sending), amount of data sent/received, infection severity and more.

In addition, the solution includes a comprehensive ThreatWiKi enabling security teams to easily understand the bot they are facing—what does it do, how it operates and any other available technical information.



Frances Flash

[illegible]garoo.b (DNS (Signature)

Dete

Communication with C&C

High Severity

High Confidence

Today at 12:09:43

- Event Description:

  Malware [illegible]o.b on machine 125.0.0.68 tried to locate its Command and Control server on 203.0.0.210 at 12:09:43 19 Mar 2012.

- Additional Data:

  Destination: 203.0.0.210

  Sent Bytes: 38 Bytes

  Received Bytes: 112 Bytes

Figure 1. Extensive forensics for deeper understanding of security events.

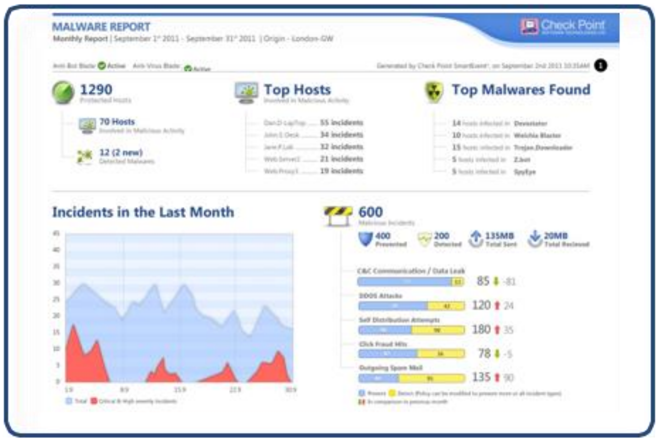


Figure 2. View the "big malware picture" with integrated threat reports.

INTEGRATED INTO CHECK POINT SOFTWARE BLADE ARCHITECTURE

The Anti-Bot Software Blade Software Blade is fully integrated into the Software Blade architecture, saving time and reducing costs by allowing customers to quickly expand security protections to meet changing requirements. It can be easily and rapidly activated on existing Check Point Security Gateways saving time and reducing costs by leveraging existing security infrastructure. The Anti-Bot Software Blade is centrally managed enabling central policy administration, enforcement and logging from a single, user-friendly console.

EXTENDED PROTECTION TO ENDPOINTS

Anti-Bot capabilities are also available in the optional SandBlast Agent, extending post-infection protectionto end-user systems, to keep users safe no matter where they go. Malware contracted while roaming outside the network perimeter will be detected, and Command & Control activity blocked, With the addition of SandBlast Agent, additional information is available for Anti-Bot detections, including the specific system and process demonstrating suspicious behavior, even when behind a NAT router.

ANTI-BOT SOFTWARE BLADE SPECIFICATIONS

Supported Appliance Families

- Available on all Check Point Appliances (Small and Medium, Enterprise, Large and Data Center Appliances)
- Check Point Power-1
- Check Point IP Appliances
- Check Point UTM-1
- Check Point IAS

Supported Operating Systems

- GAiA
- SecurePlatform
- IPSO 6.2 Disk-based
- Windows

August 22, 2016