

Cyber Threat Protection for Communications Service Providers (CSPs)



Internet service providers (ISPs), telcos, and Internet backbone providers are under increasing pressure to provide 'clean pipes', regardless if those pipes are wireless, cable, fiber or satellite. For these Communications Service Providers (CSPs), **advanced malware, botnets and targeted threats** infect subscribers' devices and can have a devastating impact on the CSP's network and business.

The malicious traffic generated by these attacks and the intent of the criminal operators behind them impose many risks for the CSP and its subscribers:

- Negatively impacting network performance
- Generating excessive bandwidth and equipment costs
- Damaging customer relationships and goodwill due to infections and fraudulent charges
- Increasing cost of customer service operations due to fraudulent charges
- Putting the business at risk with regulators
- Subjecting the CSP to subpoenas for subscriber information

CSPs that lease bandwidth are also negatively impacted by bandwidth constraints from unauthorized malicious network traffic, especially for communication traversing the different providers' networks to reach destinations across the world.

Threats to service provider networks are rampant and diverse, ranging from stolen intellectual property, identity theft, fraudulent transactions, click fraud and spam, to Distributed Denial of Service (DDoS) attacks. Despite having limited control over endpoints, CSPs are being held accountable when their networks are being used for criminal activity, often resulting in costly subpoenas for information.

CSPs must approach security differently than normal enterprise network administrators. Deep packet inspection (DPI) of CSP network traffic is typically not feasible or permitted. CSPs must focus their efforts on passive monitoring of data streams and protocols that provide high threat visibility, while considering both scalability and privacy concerns.

Damballa® CSP

Damballa CSP is specifically designed to identify malicious activity originating from subscriber's devices on the CSP's network. Damballa CSP sits out-of-band inside the service provider's network and monitors DNS requests (non-PII traffic) from the subscriber's IP address.

By monitoring DNS query behavior, Damballa CSP can identify which subscriber's are infected with advanced malware. The relatively light traffic that results from DNS protocol enables Damballa CSP to passively monitor extremely large networks with minimal hardware requirements, making deployment simple. Further, by working out-of-line inside the service provider's network, Damballa CSP won't impede network performance and remains undetectable by the criminal entities trying to evade detection.

Cyber Threat Detection

Indifferent to whether the infected device is a smartphone, tablet, PC, or Mac, **DNS-based detection** offers the best opportunity for threat detection in a service provider's network. Before an advanced malware / botnet infected victim can communicate with its **Command-and-Control (CnC) server**, steal data, and receive commands, it must first locate the server's IP address.

By utilizing the **Damballa FirstAlert cyber threat intelligence system** and monitoring DNS, detection of an infected machine's 'beaconing' can be made while the victim's device is waiting for an authoritative DNS server to respond with the IP address – i.e. infected victims can be detected before they even connect to the criminal operator's CnC server.

The Damballa Difference

The richest data source available for detecting botnet and cyber threat activity within a CSP's network is DNS traffic. DNS traffic offers a number of critical advantages for detecting and enumerating botnets and infected subscriber's:

- The vast majority of criminal operators rely on DNS to manage and control their network of victim devices.
- DNS is a well understood network protocol and is easily accessible within CSP networks.
- Deep packet inspection (DPI) is not required to extract actionable intelligence from streaming DNS data.
- DNS data is typically deemed to be public and does not contain any personally identifiable information.
- DNS traffic is generally "low volume" when compared to data-carrying Internet protocols.

Damballa Integration Partners:



Damballa

817 W. Peachtree Street NW
Suite 800
Atlanta, GA 30308

sales@damballa.com
www.damballa.com
(404) 961-7400

Damballa CSP sits within the service provider's network monitoring DNS traffic. Damballa CSP sensors are located at strategic network locations to view SPAN'd traffic between the subscriber and the service provider's DNS servers or egress. Damballa CSP sensors monitor DNS traffic for queries indicative of the presence of advanced malware. All malicious queries are captured and delivered to the Damballa CSP Collector. The Damballa CSP Collector aggregates and correlates the findings from the Damballa CSP sensors and generates the alerts of infections (reports) for integration with other service provider systems.

Threat Termination

Upon seeing the infected subscriber's DNS query, Damballa CSP can swiftly terminate the infected device's specific communication with the criminal operator. By interceding on the DNS query, Damballa CSP can forge the service provider's DNS response to the infected subscriber, directing the malware to communicate to a controlled IP address within the service provider's control instead of the CnC server. Termination of the malware's ability to receive new instruction sets and talk to the criminal operator effectively deadens the threat to the subscriber while the CSP notifies the subscriber of the infection, and the subscriber remediates the infection on the device.

Sensor Location

Depending on the service provider and their network configuration, there are two logical places in which to monitor DNS traffic for the presence of cyber attacks and botnet communications:

Below the Recursive for networks where the CSP hosts their own recursive DNS servers. This deployment yields the highest botnet detection fidelity, with the ability to clearly indicate which subscriber IP address made the DNS lookup request.

Network Spanning for networks where the CSP either does not host their own recursive DNS services or allows customers to use third-party DNS services. This deployment broadens the CSP's ability to encompass victim computing devices that have opted out of utilizing the CSP's specified DNS resolvers – whether they chose to intentionally or because the botnet malware agent was programmed to do so.

Damballa CSP Collector

The Damballa CSP Collector resides within the service provider's network and is the central communication element for the Damballa CSP Sensors. The Collector correlates data from the sensors and provides reports, data exports, and SIEM integration, and communicates directly with Damballa FirstAlert to receive threat updates. The Damballa CSP Collector also serves as the control mechanism for Damballa CSP. Service providers can control how frequently to receive activity reports, establish and configure event delivery to their SIEM, manage network configuration options, and configure SNMP monitoring settings.

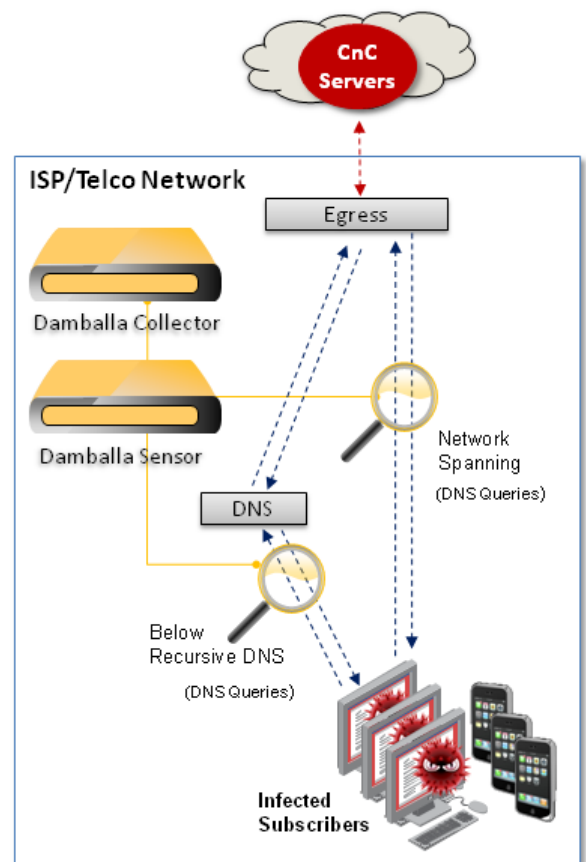
Cyber Threat Protection for Service Providers

Managing extremely large networks and providing Internet services to customers whose devices (smartphones, tablets, PCs, Macs, and others) are beyond the CSP's control, requires a unique approach to network security. DNS-based detection offers the best method for CSPs to secure their networks. Damballa CSP provides service providers with the ability to:

- Provide "Clean Pipes"
- Address customer/regulator concerns
- Provide a more differentiated service
- Reduce operating costs/improve margins
- Notify subscribers of infections and the risk it may cause
- Discover infected subscribers by monitoring the malware's malicious communication
- Monitor millions of subscribers with a single 1U Sensor
- Provide "Opt-In" security services
- Offer termination of malicious traffic
- Provide walled garden services
- Improve network performance by eliminating fraudulent activity
- Eliminate fraudulent activity that results in excessive charges for subscribers
- Reduce the cost of operations associated with dealing with fraudulent charges and activity

Reporting and Integration

Damballa CSP is specifically designed to work with large service providers and their special data management needs. All forensic evidence related to the malicious DNS queries from infected subscribers are aggregated and correlated for processing by service provider systems. These reports are either provided in JSON format so they can be input into custom network systems or they can be delivered via a syslog output into SIEM solutions – including Damballa partners ArcSight and Q1 Labs. Forensic evidence includes the subscriber's IP address, timestamp of each malicious query, queried domain, threat name / industry name, and information on the malware related to the threat.



Contact Damballa

Web: www.damballa.com | Email: sales@damballa.com | Phone: 404-961-7400



Damballa CSP Reporting Addendum



Damballa CSP Reports

Damballa CSP reports are generated utilizing the JSON file format, providing simple integration into service provider systems. These reports include extensible data that describe the malicious activity within the service provider's network. Reports may be pulled from the Collector at intervals defined by the customer.

Activity Report - For each subscriber IP involved in malicious communications, the report provides:

- botnet_id: unique identifier for the botnet
- sensor_hostname: sensor reporting the activity
- client_ip: IP address of querying subscriber
- first_seen: timestamp of first query in time period
- last_seen: timestamp of last query in time period
- lookup_count: number of queries from first/last seen
- domain: CnC domain name

Resolved IP Report - Identification of CnC hosting activity:

- Resolved_IP: For each CnC domain detected in network, the current resolved IP address. Used by service providers to identify if they are the host of any Command and Control servers.

Threat Report - For each botnet_id, the report provides:

- botnet_id: unique identifier for the operator
- operator_name: unique Damballa name for the operator
- industry_name: common industry name for the operator
- first_operational: date Damballa started tracking operator
- total_associated_malware: quantity or related malware to operator
- global_severity_score: Damballa severity score for operator
- last_malware_captured: date Damballa captured last related malware to operator
- For each AV Vendor(McAfee, Avira, Trend, Symantec), the report provides "coverage" information for the known related malware:
 - malware_detected - quantity of related malware that AV vendor can detect
 - common_avnames - most common AV signature names matching related malware for operator
 - recent_avnames - most recent AV signature names matching related malware for operator

SIEM Integration

Damballa CSP also provides the ability to directly integrate with SIEM products that can receive syslog events. Damballa CSP SIEM integration includes the following content in each syslog event:

Field (Data Type)	Contents	Description
Syslog Version	1	Output Format Version
Device Vendor (String)	Damballa	
Device Product (String)	Damballa CSP	
Device Version (String)	1.6	CSP Solution version number
Signature ID (String)	(botnet ID)	A unique identifier for the botnet. Provides tie to content provided in Damballa CSP Activity and Threat reports via the field "botnet_id".
Name (String)	Evidence	Type of event
cnt (Integer)	(count)	The number of queries from first/last seen for a threat/botnet identified on a Subscriber IP. Provides a tie to content provided in Damballa CSP Activity report via the field "lookup_count".
Severity (Integer)	(severity)	The Damballa severity score for the threat / botnet. Provides a tie to the content provided in the Damballa CSP Threat report via the field "global_severity_score".
Cat (String)	DNS Query	The event category
start (TimeStamp)	(start_time)	The timestamp of first query in the time period - MMM dd yyyy HH:mm:ss or milliseconds since epoch. Provides a tie to the Damballa CSP Activity report via the field "first_seen".
end (TimeStamp)	(time)	The timestamp of last query in the time period - MMM dd yyyy HH:mm:ss or milliseconds since epoch. Provides a tie to the Damballa CSP Activity report via the field "last_seen".
src (IPv4 Address)	(source IPv4)	The IP address of querying subscriber. Provides a tie to the Damballa CSP Activity report via the field "client_IP".
destinationDnsDomain (String)	(destination domain)	The CnC domain name being queried by a Subscriber IP. Provides a tie to the Damballa CSP Activity report via the field "domain".
cs1Label (String)	Threat Name	Custom Field Label
cs1 (String)	(Threatname)	The unique Damballa name for the operator / threat. Provides a tie to the Damballa CSP Threat report via the field "operator_name".
cs2Label (String)	Industry Name	Custom Field Label
cs2 (String)	(Industry Name)	The common industry name for the operator/threat (if available). Provides a tie to the Damballa CSP Threat report via the field "industry_name".
dvchost (String)	(sensor name)	Name of the sensor which collected the evidence