Introducing Cisco Umbrella for Cloud Based Threat Protection

Szilard Csordas,
Consulting Security Engineer
Agenda

Introduction

• What is Cisco Umbrella
• Architecture & Data Flow
• Statistical Models
By 2020, Cisco Global Cloud Index estimates:

92% of global data center traffic will come from the cloud
By 2021, Gartner estimates:

25% of corporate data traffic will bypass perimeter security
How IT was Built

Internet

Critical infrastructure

Business apps

Workplace desktops
IT Today

Critical infrastructure
Amazon, Rackspace, Windows Azure, etc.

Business apps
Salesforce, Office 365, DocuSign, etc.

Branch office

Roaming laptops

Workplace desktops

Internet
Agenda

- Introduction
- What is Cisco Umbrella
  - Architecture & Data Flow
  - Statistical Models
Secure Internet Gateway

Your secure onramp to the internet, anywhere users go

- On and off the corporate network
- All ports and protocols
- Open platform
- Live threat intelligence
- Proxy and file inspection
- Discovery and control of SaaS
DNS Overview

Domain registrar
Maps and records names to #s in “phone books”

Authoritative DNS
Owns and publishes the “phone books”

Recursive DNS
Looks up and remembers the #s for each name

GoDaddy
amazon web services
Route53
Cisco Umbrella
DNS is the Critical Lifeline of the Network

Every possible Device

All Network Architectures

All Operating Systems
What happens when you visit a single site?

68% of organizations don’t monitor DNS.
Simplest Security Deployment on the Planet

Point external DNS traffic to Umbrella

NETWORK DEPLOYMENT

208.67.222.222 (P)
208.67.220.220 (S)

Any device

Provision DNS or DHCP servers

DNS

Provision corporate and guest wireless APs

Any owner
Cisco AnyConnect Module
Roaming protection without another agent

1. Enable roaming security module
2. Set roaming policy in Umbrella
3. Gain visibility into internet activity and detailed logs for incident response
Cisco Security Connector
One app, two layers of security to protect enterprise iOS users

MOBILE DEPLOYMENT

VISIBILITY & CONTROL
• DNS-layer enforcement and encryption via net new iOS 11 functionality
• Customizable URL-based protection with intelligent proxy
• Available to Umbrella\(^1\) customers at no extra charge if subscription already covers iOS users

VISIBILITY
• App-layer auditing and correlation via net new iOS 11 functionality
• Logs encrypted URL requests without SSL decryption
• Available to AMP for Endpoints customers at no extra charge if subscription already covers iOS devices
Enforcing Inline, Analyzing Offline
Breadth to cover all ports and depth to inspect risky domains

**Inline Enforcement**
- DNS and IP layer
  - Domain request
  - IP response (DNS-layer) or connection (IP-layer)
- HTTP/S layer
  - URL request
  - File hash
- Umbrella / Talos and partner feeds
- Custom domain lists
- Custom IP lists (future)
- WBRS / Talos + partner feeds
- Custom URL lists
- AV
- AMP
- ALLOW, BLOCK, OR PROXY
- ALLOW, BLOCK, OR ANALYZE

**Offline Analysis**
- Internet-wide telemetry
- Umbrella statistical models
- Predictive updates
- Retrospective updates
- AMP threat grid
- Unknown files (roadmap)
Gather Intelligence, Enforce Security at the DNS Layer

User request patterns
Used to detect:
• Compromised systems
• Command and control callbacks
• Malware and phishing attempts
• Algorithm-generated domains
• Domain co-occurrences
• Newly registered domains

Authoritative DNS logs
Used to find:
• Newly staged infrastructures
• Malicious domains, IPs, ASNs
• DNS hijacking
• Fast flux domains
• Related domains

Recursive DNS
Where Does Umbrella Fit?

It all starts with DNS

- Precedes file execution and IP connection
- Used by all devices
- Port agnostic

Network and endpoint

- NGFW
- Netflow
- Proxy
- Sandbox

First line

Network and endpoint

Endpoint

AV

AV

AV

AV

AV

AV
Umbrella Resolver Flow

Destinations
Original destination or block page

Security controls
• DNS and IP enforcement
• Risky domain inspection through proxy
• SSL decryption available

Internet traffic
On- and off-network
Protection for Command and Control Callbacks

- 91% of C2 can be blocked at the DNS layer
- 15% of C2 bypasses web ports 80 & 443
Agenda

- Introduction
- What is Cisco Umbrella
- Architecture & Data Flow
- Statistical Models
Umbrella Data Centers Co-located at Major IXPs

Umbrella Datacenters
- Amsterdam
- Berlin
- Bucharest
- Chicago
- Copenhagen
- Dallas
- Frankfurt
- Hong Kong
- Johannesburg
- London
- Los Angeles
- Miami
- New York
- Palo Alto
- Paris
- Prague
- Seattle
- Singapore
- Sydney
- Tokyo
- Toronto
- Vancouver
- Warsaw
- Washington DC
https://system.opendns.com/

Current Status

System is currently online.

Total Activity
Number of DNS requests per day in billions

Sep 27 2018 00:00
169,134,710,212
How Fast does Umbrella Resolve DNS Requests?

<table>
<thead>
<tr>
<th>Region</th>
<th>Umbrella</th>
<th>Google</th>
<th>Neustar</th>
<th>Dyn</th>
<th>Level3</th>
<th>Comodo</th>
<th>SafeDNS</th>
<th>OpenNIC</th>
<th>FreeDNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>18</td>
<td>27</td>
<td>20</td>
<td>26</td>
<td>30</td>
<td>43</td>
<td>55</td>
<td>48</td>
<td>136</td>
</tr>
<tr>
<td>Europe / EMEA</td>
<td>44</td>
<td>36</td>
<td>35</td>
<td>39</td>
<td>41</td>
<td>52</td>
<td>94</td>
<td>147</td>
<td>53</td>
</tr>
<tr>
<td>Asia / APAC</td>
<td>65</td>
<td>56</td>
<td>83</td>
<td>85</td>
<td>201</td>
<td>215</td>
<td>241</td>
<td>247</td>
<td>316</td>
</tr>
<tr>
<td>Latin America</td>
<td>154</td>
<td>70</td>
<td>134</td>
<td>118</td>
<td>141</td>
<td>126</td>
<td>180</td>
<td>154</td>
<td>247</td>
</tr>
<tr>
<td>Africa</td>
<td>102</td>
<td>21</td>
<td>94</td>
<td>165</td>
<td>166</td>
<td>138</td>
<td>217</td>
<td>267</td>
<td>212</td>
</tr>
</tbody>
</table>

Measured in milliseconds

On-network Protection

DHCP Server – For locations without internal domains

- Uses built-in DHCP server on router, switch, Wi-Fi AP, firewall, SWG, or Windows Server
- DNS IP address is changed to Umbrella
- All devices connected to the network will point DNS requests to Umbrella
- Works best if there are no internal domains i.e. printers or intranet that require local resolution
On-network Protection

DNS Server – For locations that manage internal domains

• DNS server (or any device performing resolution) present on the network for internal resolution

• DNS server is configured to forward all external DNS requests for Internet domains to Umbrella

• In this and previous deployment scenario, policy control and visibility is still limited to the network’s public facing IP address
On-network Protection

Umbrella Virtual Appliance – For locations that require local IP granularity

- Supported on VMware and Hyper-V
- Internal/external requests sent to VA
- Internal requests resolved locally
- VA embeds local IPs into RFC-compliant extension mechanisms for DNS
On-network Protection

Virtual Appliance + AD Connector – For granular control and visibility with AD sync

- DCs registered with Umbrella
- Connector service is installed on one DC/member:
  1. Syncs group memberships of users and computers with Umbrella
  2. Sends IP to user mapping to VAs
- VA embeds unique identifiers that Umbrella uses for control & visibility
AnyConnect

Off-network protection, with and without VPN

• Captures all DNS traffic locally transparently, and redirects from Kernel level to Umbrella (Uses the AC Kernel driver)

• Supported when on and off VPN

• Supports optional binary updates (for all AC modules) without the need of an ASA head-end
Data Flow - Recap

- DNS request sent to Umbrella
- For safe requests that are not blocked by policy, the resolved IP address is returned
- Requests to malicious or prohibited destinations get redirected to block page (hosted by Umbrella or company)
- Requests to unknown destinations, or those that were defined for further inspection will be redirected to the intelligent proxy for further analysis
Enforcing Inline, Analyzing Offline
Breadth to cover all ports and depth to inspect risky domains

DNS and IP layer
- Domain request
- IP response (DNS-layer) or connection (IP-layer)

HTTP/S layer
- URL request
- File hash

Inline Enforcement
- Umbrella / Talos and partner feeds
- Custom domain lists
- Custom IP lists (future)

Offline Analysis
- Predictive updates
- Umbrella Statistical Models

INTERNET-WIDE TELEMETRY
- ALLOW, BLOCK, OR PROXY

WBRS / Talos + partner feeds
- Custom URL lists
- AV
- AMP

UNKNOWN FILES (ROADMAP)
- ALLOW, BLOCK, OR ANALYZE

RETSPECTIVE UPDATES
- AMP Threat Grid
Cloud-to-Cloud Log Storage Solution
with Amazon S3

S3 Benefits
- Triple redundant and encrypted storage
- Pre-built SIEM/log analytic integrations
- Elastic: pay only for the storage used

Every 10 min
HTTPS

Pre-built integrations
Amazon APIs
Agenda

- Introduction
- What is Cisco Umbrella
- Architecture & Data Flow
- Statistical Models
Gathering Intelligence at the DNS Layer

Any device

Recursive DNS

Authoritative DNS

User request patterns
Used to detect:
- Compromised systems
- Command and control callbacks
- Malware and phishing attempts
- Algorithm-generated domains
- Domain co-occurrences
- Newly registered domains

Authoritative DNS logs
Used to find:
- Newly staged infrastructures
- Malicious domains, IPs, ASNs
- DNS hijacking
- Fast flux domains
- Related domains
Statistical Models

Guilt by inference
- Co-occurrence model
- IP Geo-Location model
- Secure rank model
- Sender rank model

Guilt by association
- Predictive IP Space Modeling

Patterns of guilt
- Spike rank model
- Natural Language Processing rank model
- Live DGA Prediction

2M+ live events per second
11B+ historical events
Statistical Models: Inference Graph

Domain-IP Relationships in C2 Infrastructure

Domains Related to Malware Hashes

Domains Related to Malicious Registrant Email

...
Co-occurrence Model

Domains guilty by inference

Co-occurrence of domains means that a statistically significant number of identities have requested both domains consecutively in a short timeframe.
Spike Rank Model
Patterns of guilt

Massive amount of DNS request volume data is gathered and analyzed

DNS request volume matches known exploit kit pattern and predicts future attack

y.com is blocked before it can launch full attack
Details for j8le7s5q745e.org

This domain is currently in the Umbrella block list

Umbrella Investigate Risk Score: 71

This domain may have been created using a domain generation algorithm (DGA)

DNS queries

Friday, Sep 21, 07:00
Queries: 80
Details for 1dnscontrol.com

One or more of the IP addresses that this domain resolves to are currently blocked by Umbrella: 5.61.37.209

This domain is currently in the Umbrella block list

This domain has a suspicious SecureRank 2

DNS queries

Co-occurrences

autoecoleboisdesroches.com (100.00)
Predictive IP Space Monitoring

Guilt by association

Pinpoint suspicious domains, and observe their IP’s fingerprint

Identify other IPs (hosted on the same server) that share the same fingerprint

Block those IPs and their malicious domains
Details for 50.63.202.44

Hosting 613 malicious domains for 1 week

AS

<table>
<thead>
<tr>
<th>Prefix</th>
<th>ASN</th>
<th>Network Owner Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>50.62.0.0/15</td>
<td>AS 26496</td>
<td>AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US 86400</td>
</tr>
<tr>
<td>50.63.200.0/22</td>
<td>AS 26496</td>
<td>AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US 86400</td>
</tr>
</tbody>
</table>

Malicious domains hosted by 50.63.202.44

## WHOIS Record Data

**Registrar Name:** ENOM, INC.  **IANAID:** 48

<table>
<thead>
<tr>
<th>Created</th>
<th>Updated</th>
<th>Expires</th>
<th>Last retrieved</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Email Address</th>
<th>Associated Domains</th>
<th>Email Type</th>
<th>Last Observed</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:BOTSMustDie@GMAIL.COM">BOTSMustDie@GMAIL.COM</a></td>
<td>Greater than 500 Total - At least 403 malicious</td>
<td>Administrative, Registrant, Technical</td>
<td>July, 29, 2016</td>
</tr>
</tbody>
</table>

### Showing 1 of 1 Results

<table>
<thead>
<tr>
<th>Nameserver</th>
<th>Associated Domains</th>
<th>Last Observed</th>
</tr>
</thead>
<tbody>
<tr>
<td>ns1.sugarbucket.us</td>
<td>Greater than 500 Total - At least 270 malicious</td>
<td>July, 29, 2016</td>
</tr>
<tr>
<td>ns2.sugarbucket.us</td>
<td>Greater than 500 Total - At least 270 malicious</td>
<td>July, 29, 2016</td>
</tr>
</tbody>
</table>

### Showing 2 of 2 Results
NLP-Rank Model (natural language processing)
Identifies malicious domain-squatting and targeted phishing domains

1. Read APT reports

2. Patterns in domains used in attacks
   - Domain spoofing used to obfuscate
   - Often saw brand names and terms like “update”
   - Examples: update-java[.]net, adobe-update[.]net

3. Checked data & confirmed intuition
   - Dictionary words & company names merged
   - Changed small # of characters to obfuscate
   - Domains hosted on ASNs unassociated w/company
   - Different webpage fingerprints

4. Built model and continue to tune
   - Detects fraudulent brand domains:
     - ![Red X] linkedin.net
     - ![Green Check] linkedin.com

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public
IP Geo-location Analysis

**Host Infrastructure**
Location of the server
IP addresses mapped to domain

- Hosted across 28+ countries

**DNS Requesters**
Location of the network and off-network device
IP addresses requesting the domain

- Only US-based customers requesting a .RU TLD
Details for telvill.hu

This domain is currently in the Umbrella block list

Umbrella Investigate Risk Score: 46

This domain is associated with a Trojan attack called Emotet

DNS queries

Host

IP Count 1
Geo Distance (sum, mean) 0, 0 km
Registrant Country RU

Requester Distribution

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>PERCENTAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyprus</td>
<td>100.00%</td>
</tr>
</tbody>
</table>

Distribution 0 0 100%
‘Newly Seen Domains’ Category
Reduces risk of the unknown

1. Any user (free or paid) requests the domain
2. Every minute, we sample from our streaming DNS logs.
3. Check if domain was seen before & if whitelisted.
4. If not, add to category, and within minutes, DNS resolvers are updated globally.

Before expiration, if any user requests this domain, it’s logged or blocked as newly seen.

Later, Umbrella statistical models or reputation systems identify as malicious.

Umbrella’s Auto-WHOIS model may predict as malicious.

Attacker’s register domains.

Domains used in an attack.

Cisco Umbrella

Reputation systems

EVENTS

DAYS TO WEEKS

MINUTES

24 HOURS
Details for iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com

This domain is currently in the Umbrella block list

Umbrella Investigate Risk Score: 28

This domain is associated with a Ransomware attack called WannaCry

This domain has a suspicious SecureRank 2

This domain may have been created using a domain generation algorithm (DGA)

DNS queries

Queries: 152,192
14 Day Free Trial of Cisco Umbrella

Get started in 30 seconds
No credit card or phone call required

WHAT IS INCLUDED?

✓ Threat protection like no other — block malware, C2 callbacks, and phishing.

✓ Predictive intelligence — automates threat protection by uncovering attacks before they launch.

✓ Worldwide coverage in minutes — no hardware to install or software to maintain

✓ Weekly security report — get a personalized summary of malicious requests & more, directly to your inbox.

✓ 1,000+ users? — You’re eligible for the Umbrella Security Report, a detailed post-trial analysis.

Account Type
First Name
Last Name
Company Email
Select your country
Company phone
Company Name
Employee Count

CREATE MY TRIAL
How Umbrella integrates with Cisco Cloudlock

Complete discovery and control for SaaS apps

Umbrella identifies all the SaaS apps across an organization

Cloudlock revokes authentication for risky or inappropriate apps

Using Umbrella’s enforcement API, Cloudlock can programmatically add domains to Umbrella
## All Apps (37 Found)

<table>
<thead>
<tr>
<th>Application</th>
<th>Vendor</th>
<th>Weighted Risk</th>
<th>Identities</th>
<th>DNS Requests</th>
<th>Blocked</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flickr</td>
<td>Flickr</td>
<td>High</td>
<td>50</td>
<td>260</td>
<td>-</td>
<td>Unreviewed</td>
</tr>
<tr>
<td>Snapfish</td>
<td>Snapfish</td>
<td>High</td>
<td>48</td>
<td>248</td>
<td>&lt;1%</td>
<td>Unreviewed</td>
</tr>
<tr>
<td>Fileserve</td>
<td>Bigfile to</td>
<td>High</td>
<td>48</td>
<td>245</td>
<td>-</td>
<td>Unreviewed</td>
</tr>
<tr>
<td>LinkedIn SlideShare</td>
<td>Linkedin</td>
<td>High</td>
<td>41</td>
<td>174</td>
<td>-</td>
<td>Unreviewed</td>
</tr>
</tbody>
</table>

The dashboard displays the status of various applications and their associated risk levels, identities, DNS requests, and blocked statuses. The applications include Flickr, Snapfish, Fileserve, and LinkedIn SlideShare, and their statuses range from approved to unreviewed.