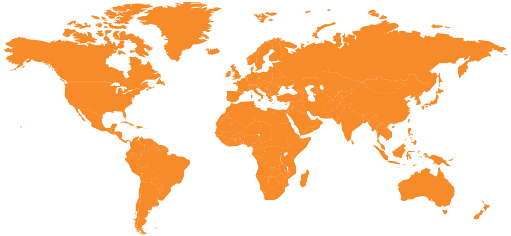
Blocking Ransomware
A Real World Example

Why OpenDNS

DNS Services Built for World's Largest Security Platform

GLOBAL NETWORK

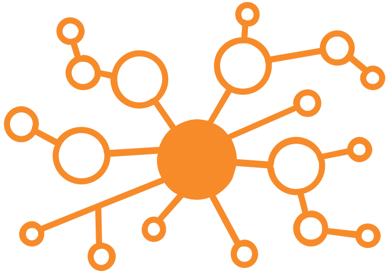
- 90B+ DNS requests/ day
- 65M+ biz & home users
- 100% uptime
- Any port, protocol, app



+

UNIQUE ANALYTICS

- security research team
- automated classification
- BGP peer relationships
- 3D visualization engine



= **80M+** malicious requests blocked/day

Problems We Solve

Breach and Malware Protection

Prevent data exfiltration and compromised systems by blocking C2 callbacks and malicious sites

Internet-wide Visibility

Speed up incident response with a live, up-to-date view of the Internet

Web Filtering and Cloud/IoT Visibility

Enforce acceptable use, see cloud services & IoT devices in use, and keep guest Wi-Fi safe

OpenDNS

PRODUCTS & TECHNOLOGIES

UMBRELLA

Enforcement

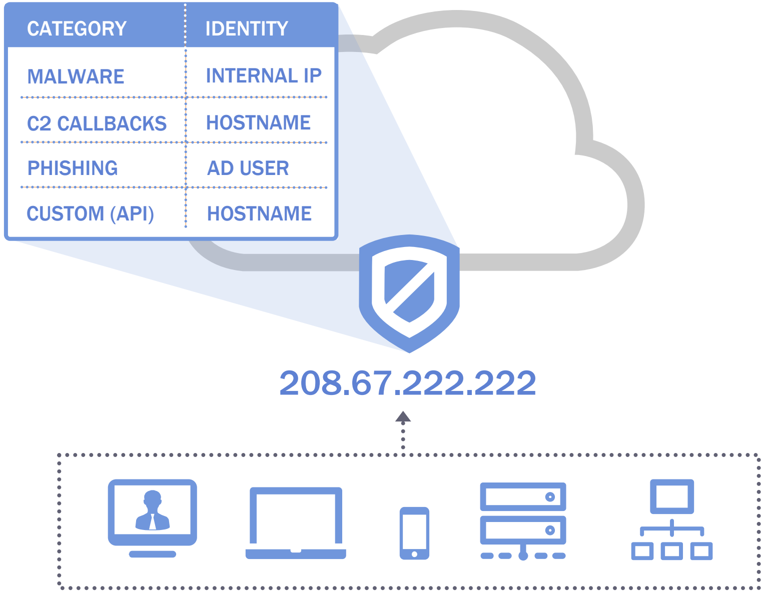
Network security service
protects any device, anywhere

INVESTIGATE

Intelligence

Threat intelligence on domains
and IPs across the Internet

UMBRELLA: The Fastest & Easiest Way To Prevent Threats Before They Reach You



CATEGORY	IDENTITY
MALWARE	INTERNAL IP
C2 CALLBACKS	HOSTNAME
PHISHING	AD USER
CUSTOM (API)	HOSTNAME

BENEFITS

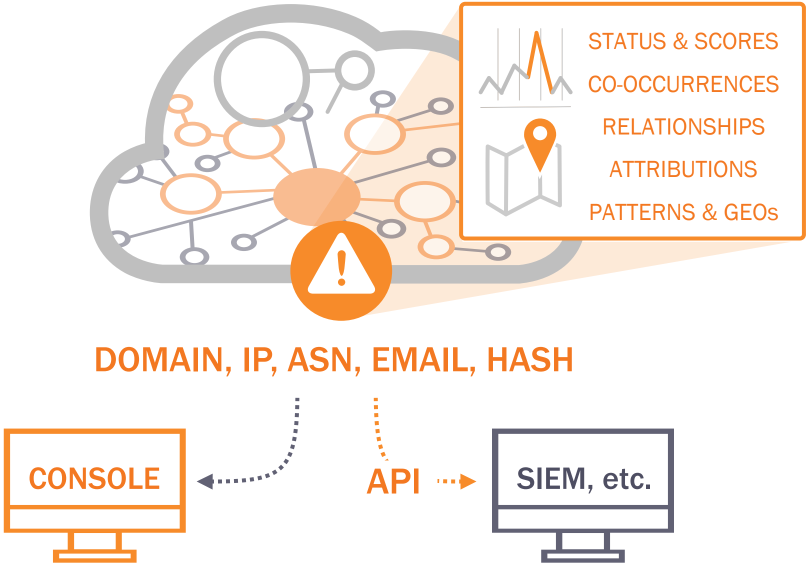
Simple to point DNS w/o technical or pro services

No hardware to install
No software to maintain

Provision globally in under 30 minutes

Infinitely scalable enforcement platform

INVESTIGATE: The Most Powerful Way To Uncover Threats Before They Happen



KEY POINTS

Intelligence about domains and IPs across the Internet

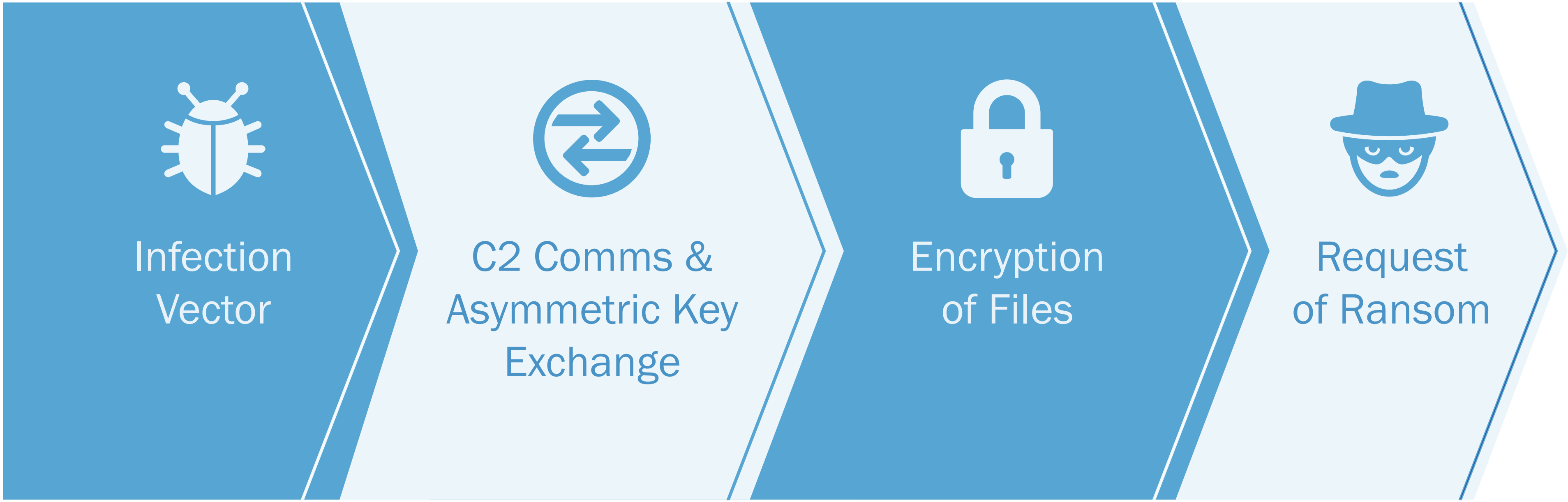
Live graph of DNS requests and other contextual data

Correlated against statistical models

Discover & predict malicious domains & IPs

Enrich security data with global intelligence

Typical Ransomware Infection



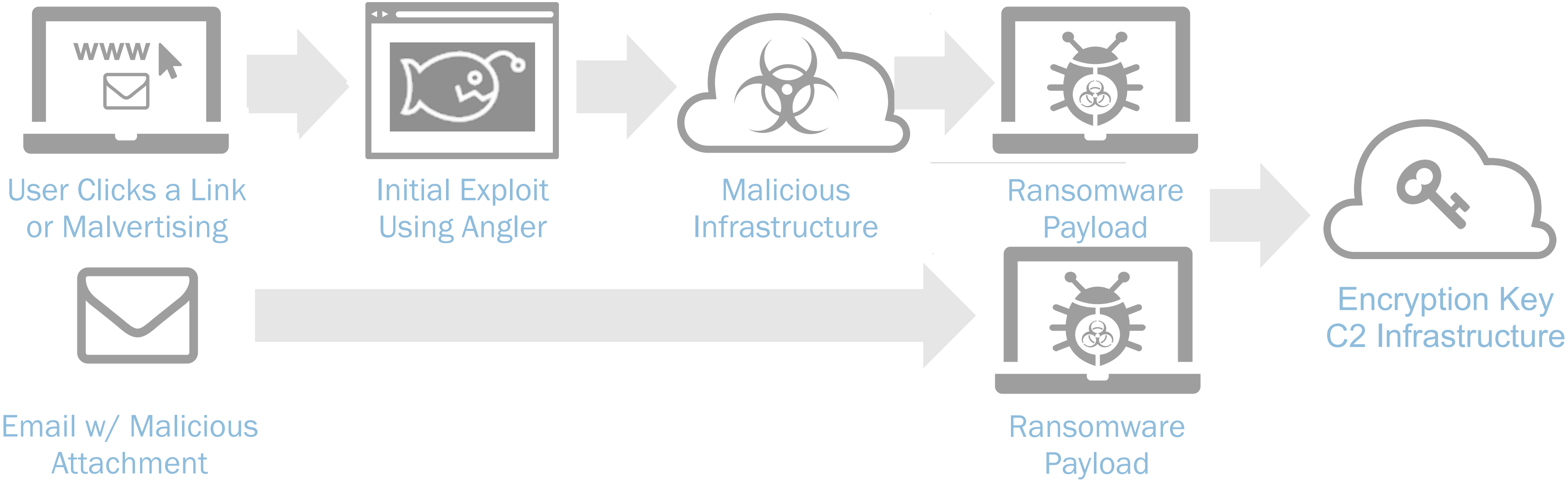
Infection Vector

C2 Comms & Asymmetric Key Exchange

Encryption of Files

Request of Ransom

Ransomware Kill Chain in Detail



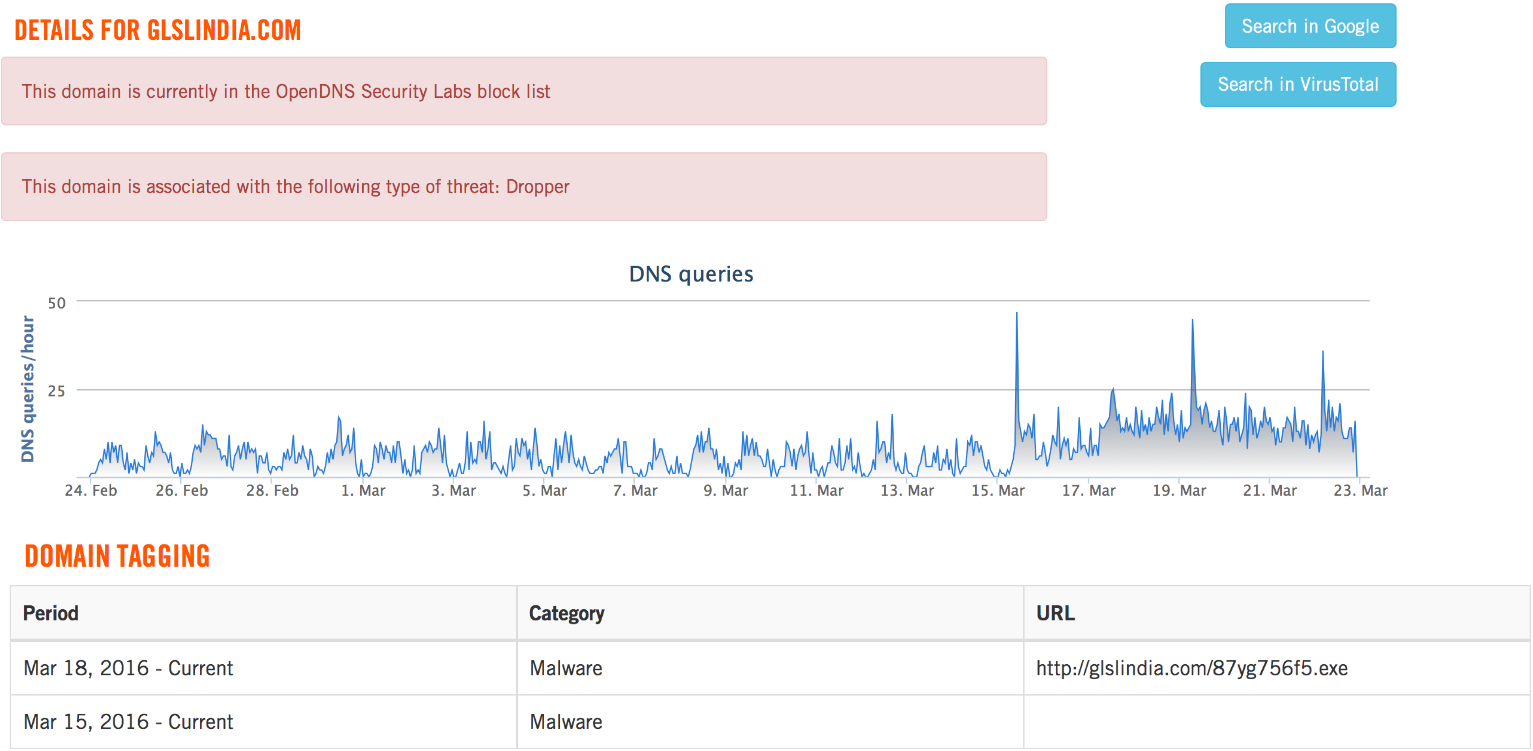
www
User Clicks a Link or Malvertising
Initial Exploit Using Angler
Malicious Infrastructure
Ransomware Payload
Encryption Key C2 Infrastructure
Email w/ Malicious Attachment
Ransomware Payload

Most Ransomware Relies on C2 Callbacks

	Encryption Key				Payment MSG
NAME	DNS	IP	NO C2	TOR	PAYMENT
Locky	●	●			DNS
SamSam			●		DNS (TOR)
TeslaCrypt	●				DNS
CryptoWall	●				DNS
TorrentLocker	●				DNS
PadCrypt	●				DNS (TOR)
CTB-Locker	●			●	DNS
FAKBEN	●				DNS (TOR)
PayCrypt	●				DNS
KeyRanger	●			●	DNS

Blocking Ransomware: Real World Example with a Locky Domain

glslindia[.]com (detection Date: 15/03/2016)



DETAILS FOR GLSLINDIA.COM

This domain is currently in the OpenDNS Security Labs block list

This domain is associated with the following type of threat: Dropper

DNS queries

DOMAIN TAGGING

Period	Category	URL
Mar 18, 2016 - Current	Malware	http://glslindia.com/87yg756f5.exe
Mar 15, 2016 - Current	Malware	

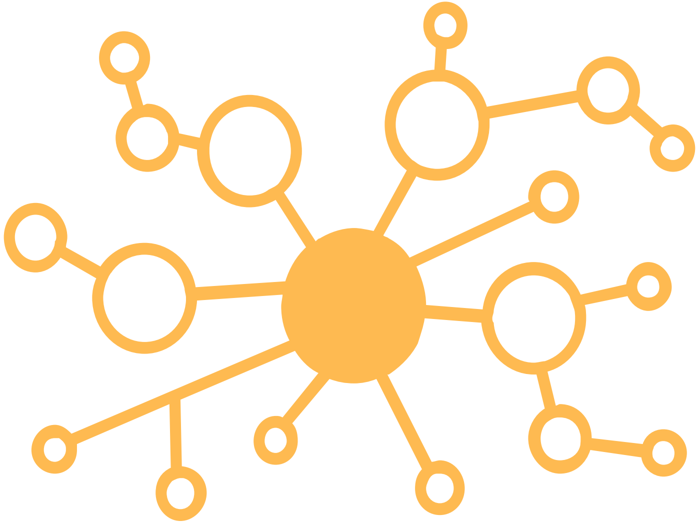
OpenDNS

OpenDNS is now part of Cisco.

Using Semantic Networks to Visualize Threats

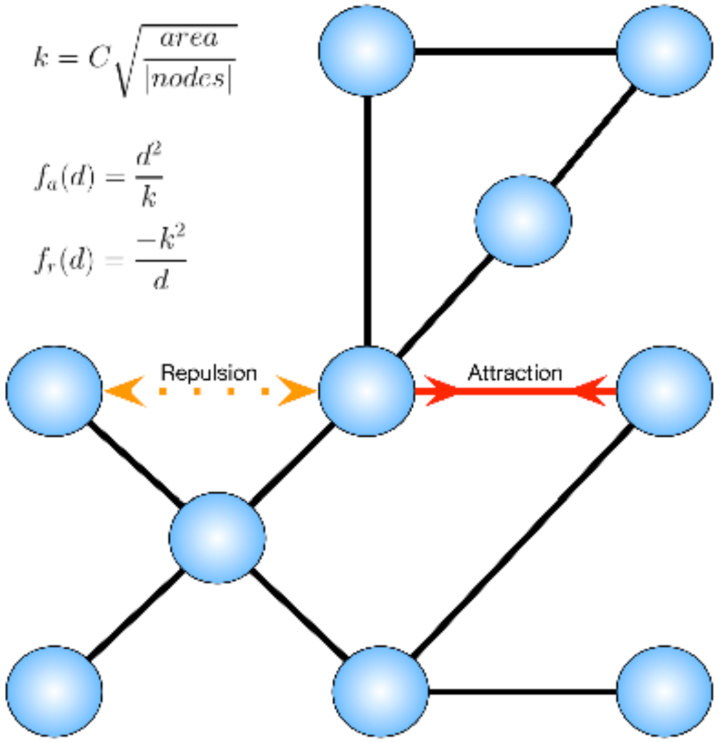
OpenGraphiti is the 3D engine used by OpenDNS researchers to visualise threats.

- Graph = Set of Nodes
- Node = Concept, Edge = Relationship
- Agents populate the graph
- A semantic network can be represented as a graph connecting any kind of information by any kind of relationship
- They can be used to model nearly everything and can be applied to a wide range of problems



May the Force Be with You

- OpenGraphiti, uses Particle Physics to turn data into a visual representation.
- Force Directed Layout
- Different sets of nodes: connected nodes attract each other, disconnected nodes repel each other
- A node can be an IP, a Domain, an Autonomous System or a WHOIS record
- Edges and Clusters pinpoint the relationships between the nodes of the Graph



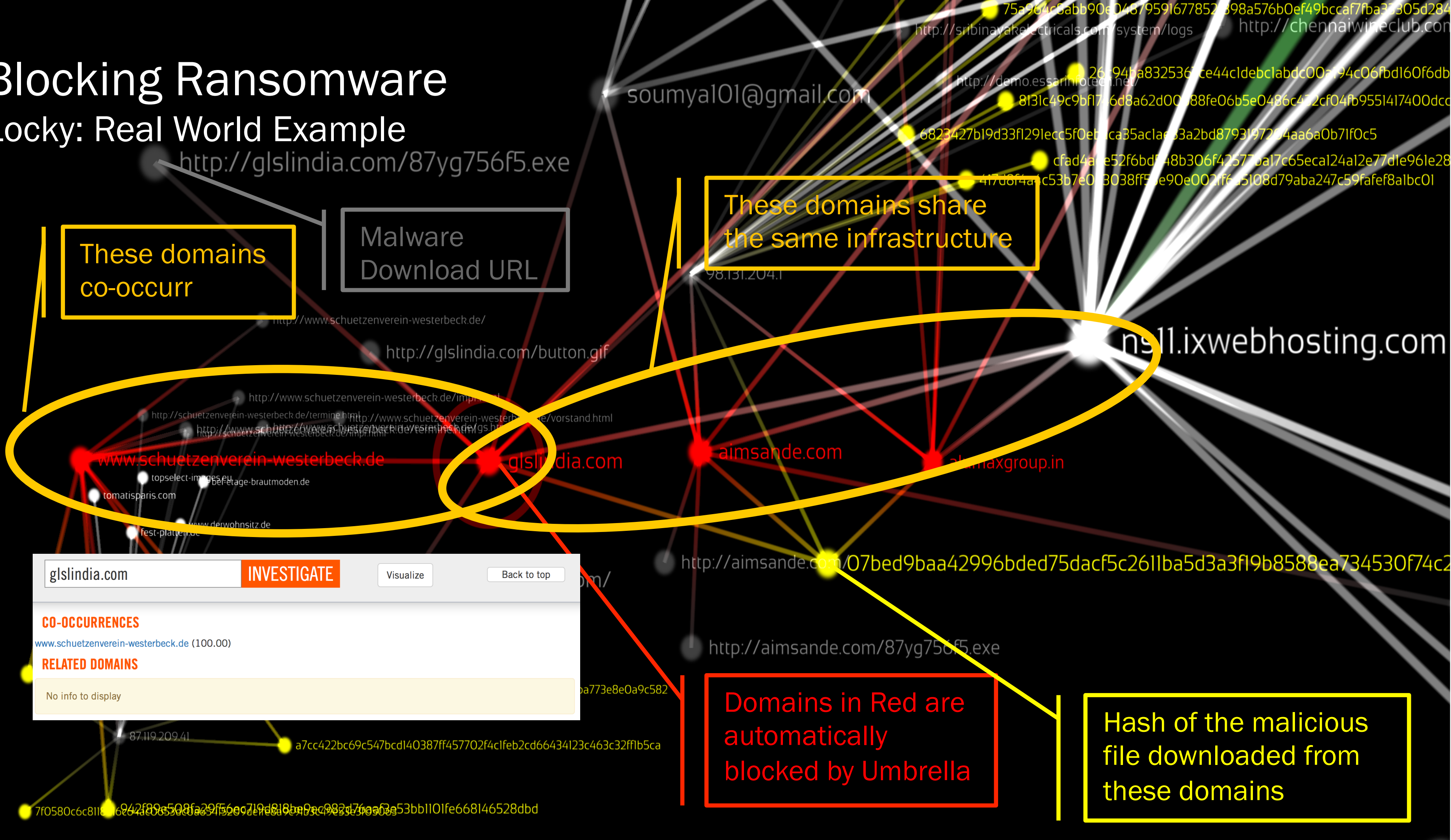
$$k = C\sqrt{\frac{area}{|nodes|}}$$

$$f_a(d) = \frac{d^2}{k}$$

$$f_r(d) = \frac{-k^2}{d}$$

Blocking Ransomware

Locky: Real World Example



http://glslindia.com/87yg756f5.exe
soumya101@gmail.com
http://sribinayakelectricals.com/system/logs
http://chennaiwineclub.com
http://demo.essarinfotech.net/
98.131.204.1
ns11.ixwebhosting.com
http://www.schuetzenverein-westerbeck.de/
http://glslindia.com/button.gif
http://www.schuetzenverein-westerbeck.de/impressum.html
http://schuetzenverein-westerbeck.de/termine.html
http://www.schuetzenverein-westerbeck.de/vorstand.html
www.schuetzenverein-westerbeck.de
glslindia.com
aimsande.com
alumaxgroup.in
topselect-images.eu
bel-etage-brautmoden.de
tomatisparis.com
www.derwohnsitz.de
fest-platten.de
http://aimsande.com/
07bed9baa42996bded75dacf5c2611ba5d3a3f19b8588ea734530f74c2
http://aimsande.com/87yg756f5.exe
6823427b19d33f1291ecc5f0eb
8131c49c9bf17
a7cc422bc69c547bcd140387ff457702f4c1feb2cd66434123c463c32ff1b5ca
87.119.209.41
7f0580c6c811
53bb1101fe668146528dbd

These domains co-occurr

Malware Download URL

These domains share the same infrastructure

Domains in Red are automatically blocked by Umbrella

Hash of the malicious file downloaded from these domains

glslindia.com INVESTIGATE Visualize Back to top

CO-OCCURRENCES

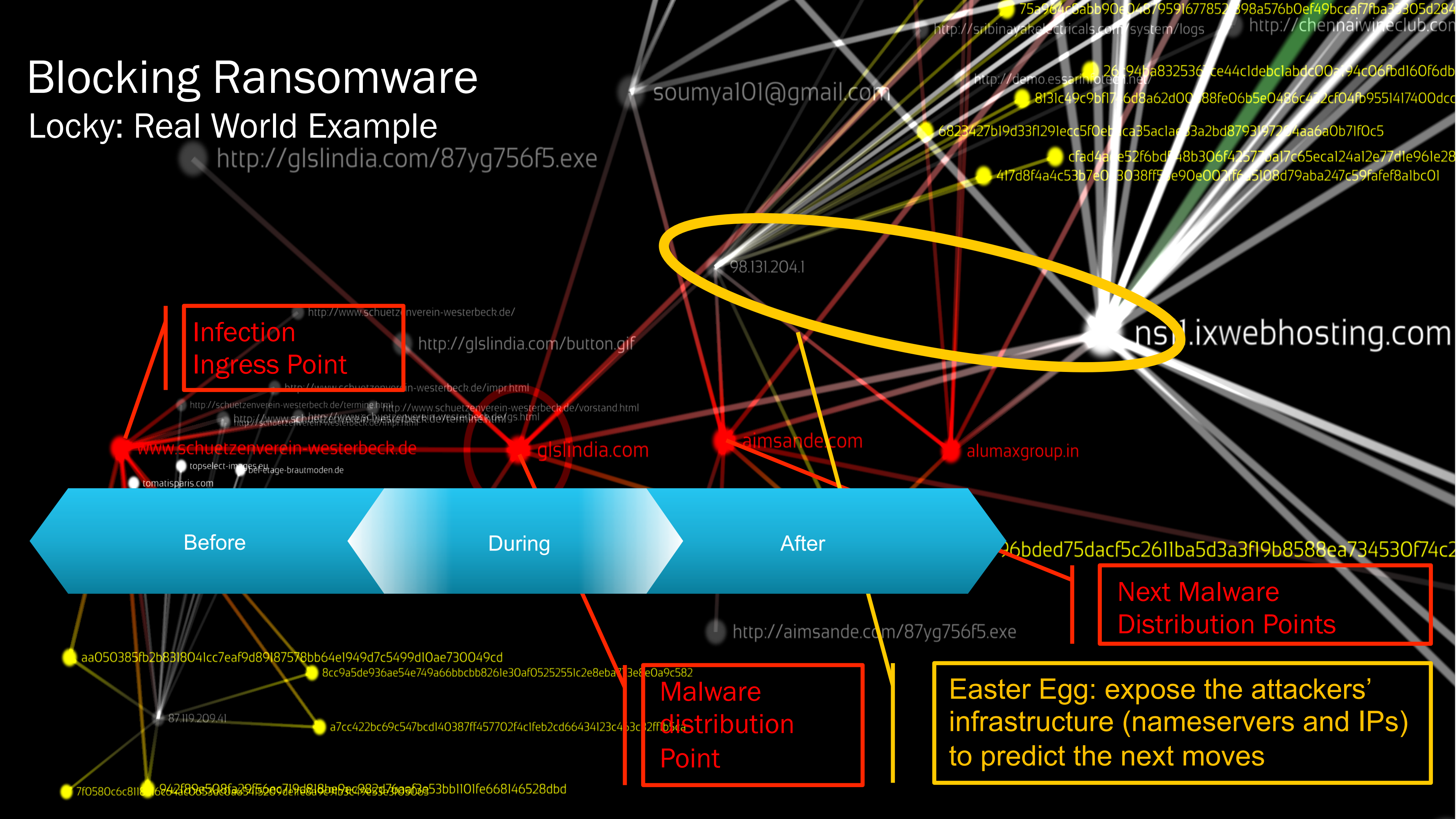
www.schuetzenverein-westerbeck.de (100.00)

RELATED DOMAINS

No info to display

Blocking Ransomware

Locky: Real World Example


http://glslindia.com/87yg756f5.exe
soumya101@gmail.com
75a964c6abb90e0487959167785298a576b0ef49bccaf7fba33305d284
http://sribinayakelectricals.com/system/logs
http://chennaiwineclub.com
http://demo.essarinfotech.net/
26794fa8325367ce44c1debc1abdc00a794c06fbd160f6db
8131c49c9bf1746d8a62d00388fe06b5e0486c432cf04fb9551417400dc
6823427b19d33f1291ecc5f0eb1ca35ac1ae3a2bd879319724aa6a0b71f0c5
cfad4ae52f6bdf48b306f42577a17c65eca124a12e77d1e961e28
417d8f4a4c53b7e013038ff5e90e002ff6d5108d79aba247c59fafef8a1bc01
98.131.204.1
ns1.ixwebhosting.com
http://www.schuetzenverein-westerbeck.de/
http://glslindia.com/button.gif
http://www.schuetzenverein-westerbeck.de/impr.html
http://schuetzenverein-westerbeck.de/termine.html
http://www.schuetzenverein-westerbeck.de/vorstand.html
http://www.schuetzenverein-westerbeck.de/termine.html
http://www.schuetzenverein-westerbeck.de/gs.html
http://schuetzenverein-westerbeck.de/impr.html
www.schuetzenverein-westerbeck.de
glslindia.com
aimsande.com
alumaxgroup.in
topselect-images.eu
bel-etage-brautmoden.de
tomatisparis.com
96bded75dacf5c2611ba5d3a3f19b8588ea734530f74c2
http://aimsande.com/87yg756f5.exe
aa050385fb2b8318041cc7eaf9d89187578bb64e1949d7c5499d10ae730049cd
8cc9a5de936ae54e749a66bbcbb8261e30af0525255 1c2e8eba713e8e0a9c582
87.119.209.41
a7cc422bc69c547bcd140387ff457702f4c1feb2cd66434123c4b3c32ffb5da
7f0580c6c811
942f89e508fa29f56ec719d818be9ec982d76aef3e53bb1101fe668146528dbd

Infection Ingress Point

Before

During

After

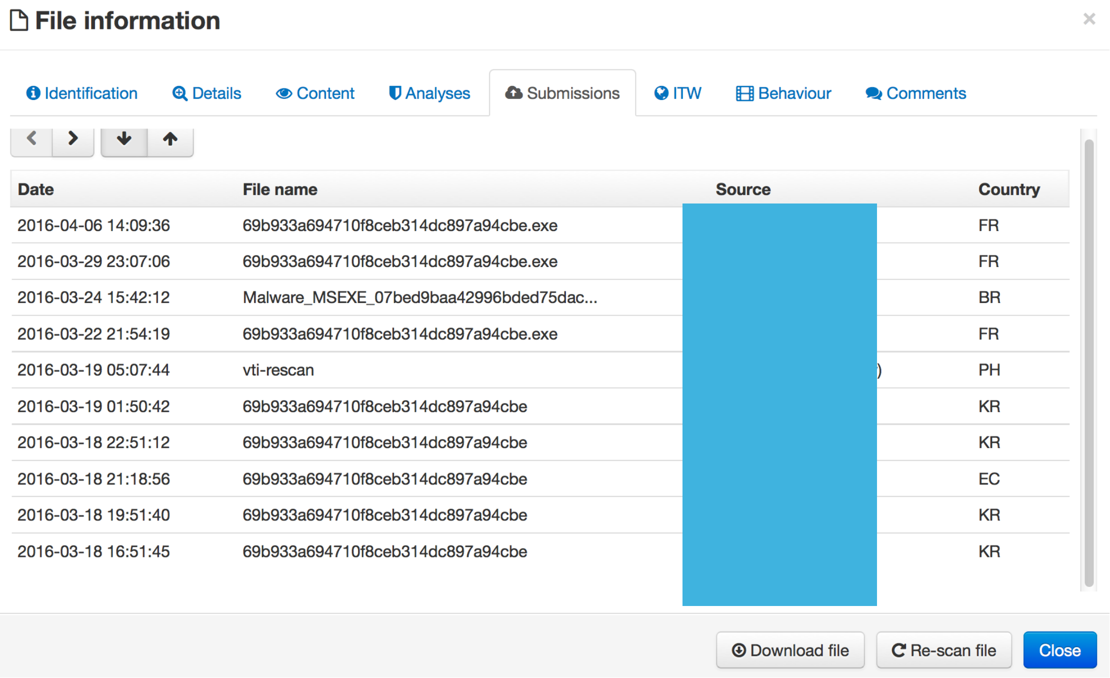
Next Malware Distribution Points

Malware distribution Point

Easter Egg: expose the attackers' infrastructure (nameservers and IPs) to predict the next moves

Discover the Threats Before They Happen (1)

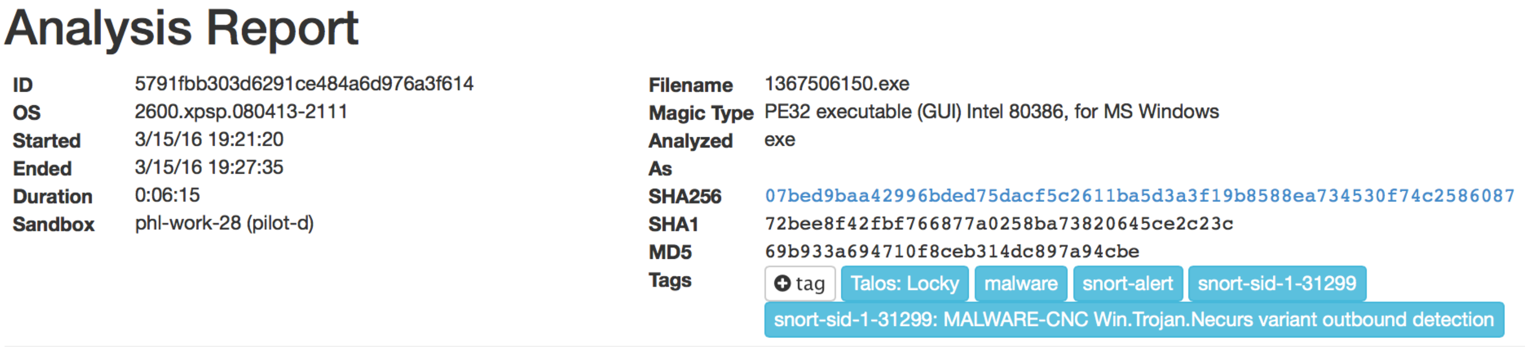
VT Link:
https://virustotal.com/en/file/07bed9baa42996bded75dacf5c2611ba5d3a3f19b8588ea734530f74c2586087/analysis/
(first submission: 2016-03-18 16:51:45 three days after ThreatGrid, see next slide)



Date	File name	Source	Country
2016-04-06 14:09:36	69b933a694710f8ceb314dc897a94cbe.exe	[redacted]	FR
2016-03-29 23:07:06	69b933a694710f8ceb314dc897a94cbe.exe	[redacted]	FR
2016-03-24 15:42:12	Malware_MSEXE_07bed9baa42996bded75dac...	[redacted]	BR
2016-03-22 21:54:19	69b933a694710f8ceb314dc897a94cbe.exe	[redacted]	FR
2016-03-19 05:07:44	vti-rescan	[redacted]	PH
2016-03-19 01:50:42	69b933a694710f8ceb314dc897a94cbe	[redacted]	KR
2016-03-18 22:51:12	69b933a694710f8ceb314dc897a94cbe	[redacted]	KR
2016-03-18 21:18:56	69b933a694710f8ceb314dc897a94cbe	[redacted]	EC
2016-03-18 19:51:40	69b933a694710f8ceb314dc897a94cbe	[redacted]	KR
2016-03-18 16:51:45	69b933a694710f8ceb314dc897a94cbe	[redacted]	KR

Discover the Threats Before They Happen (2)

TG Link: https://panacea.threatgrid.com/samples/5791fbb303d6291ce484a6d976a3f614
(detection date: 3/15/16 19:21:20)



Analysis Report

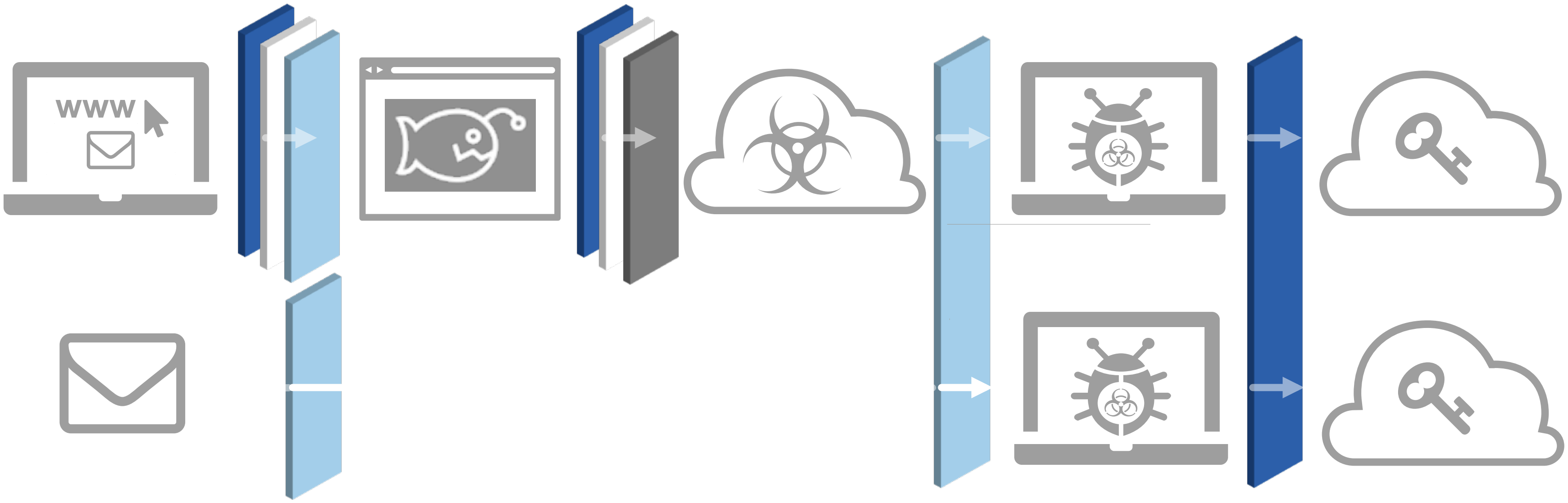
ID	5791fbb303d6291ce484a6d976a3f614
OS	2600.xpsp.080413-2111
Started	3/15/16 19:21:20
Ended	3/15/16 19:27:35
Duration	0:06:15
Sandbox	phl-work-28 (pilot-d)

Filename	1367506150.exe
Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
Analyzed As	exe
SHA256	07bed9baa42996bded75dacf5c2611ba5d3a3f19b8588ea734530f74c2586087
SHA1	72bee8f42fbf766877a0258ba73820645ce2c23c
MD5	69b933a694710f8ceb314dc897a94cbe
Tags	⊕ tag · Talos: Locky · malware · snort-alert · snort-sid-1-31299 · snort-sid-1-31299: MALWARE-CNC Win.Trojan.Necurs variant outbound detection

As you may see from the tags, the protection is enforced across all Cisco products

OpenDNS is now part of Cisco.

How Cisco Protects Customers from Ransomware



Umbrella blocks the request

Web or Email Security w/**AMP** blocks the file

Umbrella blocks the request

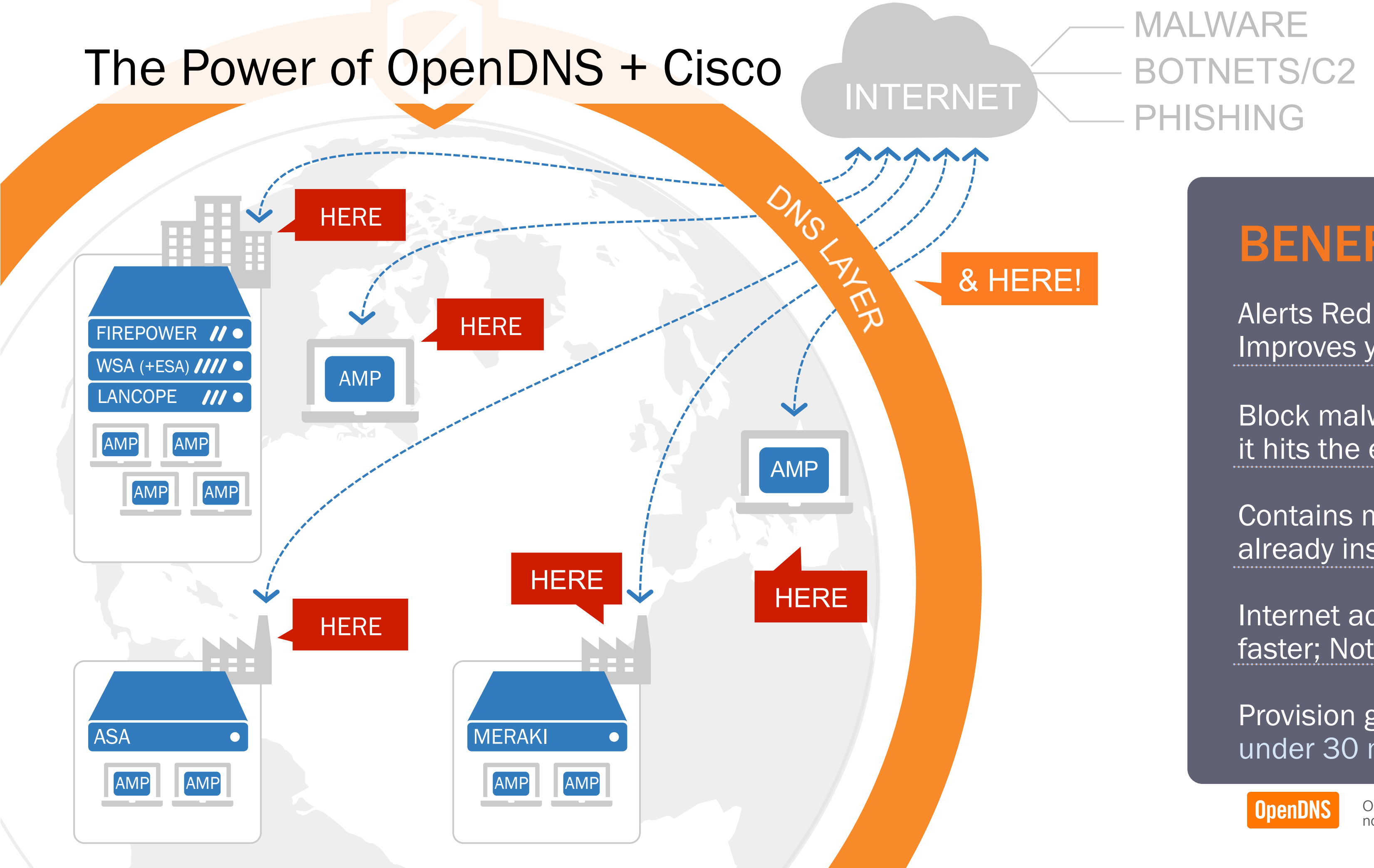
Lancope detects the activity

AMP for Endpoints blocks the file

Umbrella blocks the request

● Umbrella   Next-Gen Firewall   ● AMP   ● Lancope

The Power of OpenDNS + Cisco



BENEFITS

Alerts Reduced 2x; Improves your SIEM

Block malware before it hits the enterprise

Contains malware if already inside

Internet access Is faster; Not slower

Provision globally in under 30 minutes

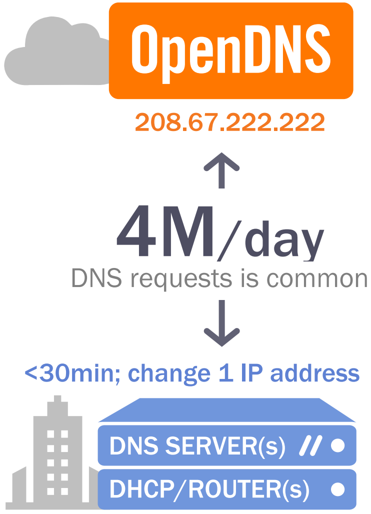
OpenDNS

OpenDNS is now part of Cisco.

cisco

The Fastest & Easiest Security POV You've Ever Done

FORWARD DNS REQUESTS OR LOGS



OpenDNS

208.67.222.222

↑

4M/day

DNS requests is common

↓

<30min; change 1 IP address

DNS SERVER(s)

DHCP/ROUTER(s)

SECURITY REPORT AFTER ~30 DAYS

1 in 1000

requests are typically malicious

OpenDNS Security Report

Select Security Incidents

Threat Information

3D Visualization

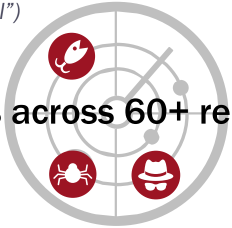
of attackers' infrastructures & selectively, your infrastructure

THREAT OCCURRENCES WE COMMONLY SEE

66%
RANSOMWARE
(e.g. "CryptoWall")

61%
EXPLOIT KIT
(e.g. "Angler")

39%
BANK TROJAN
(e.g. "Dyre")



averages across 60+ recent POV

100%
WIDESPREAD ATTACK
(i.e. typo-squatted domain)

17%
TARGETED ATTACK
(i.e. spear phishing)

OpenDNS

cisco

TOMORROW starts here.