



# Blocking Ransomware: Real World Example with a Locky Domain

ISSA – SLC Chapter, Fall Seminar

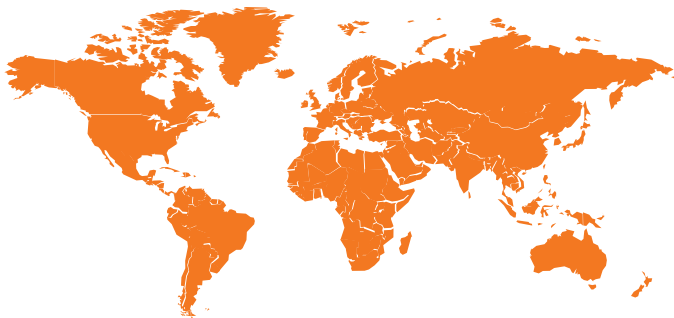
Jordan Gackowski  
Consulting Systems Engineer  
September 22<sup>nd</sup> 2016

# What is OpenDNS?

DNS Services Built for World's Largest Security Platform

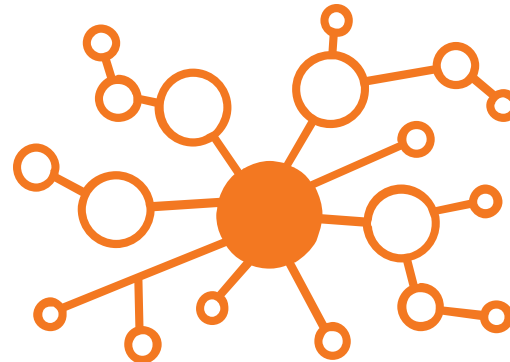
## GLOBAL NETWORK

- 80B+ DNS requests/day
- 65M+ biz & home users
- 25 Data Centers
- 100% uptime
- Any port, protocol, app



## UNIQUE ANALYTICS

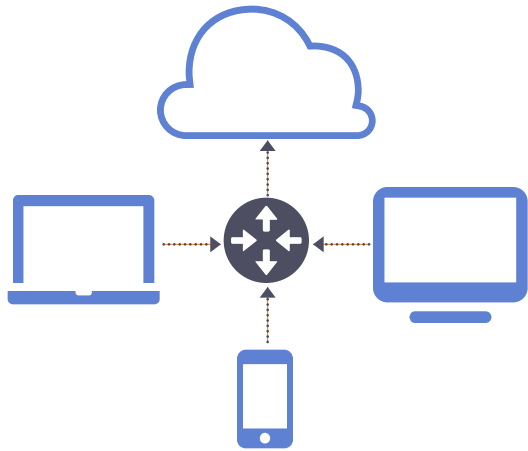
- security research team
- automated classification
- BGP peer relationships
- 3D visualization engine



**80M+**

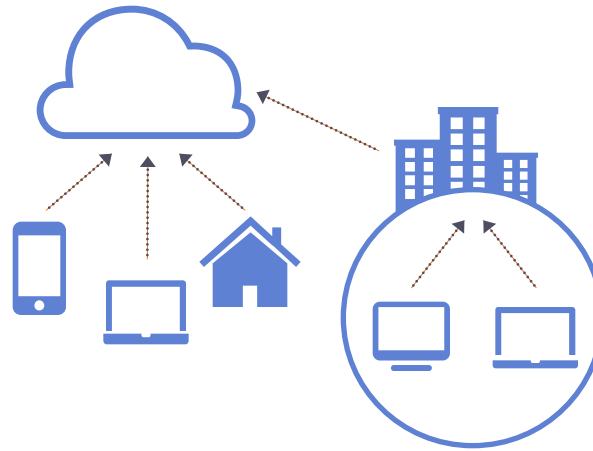
malicious requests  
blocked/day

# DNS is Used by Every Device on Your Network



## ANY OWNER

network's DHCP tells  
every connected device  
where to point DNS



## ANY TOPOLOGY

no matter how your  
LAN or WAN is set up,  
it simply works



## ANY OPERATING SYSTEM

Win, Mac, iOS, Android,  
Linux, custom app  
servers, and even IoT

# Leveraging a Single Global Recursive DNS Service

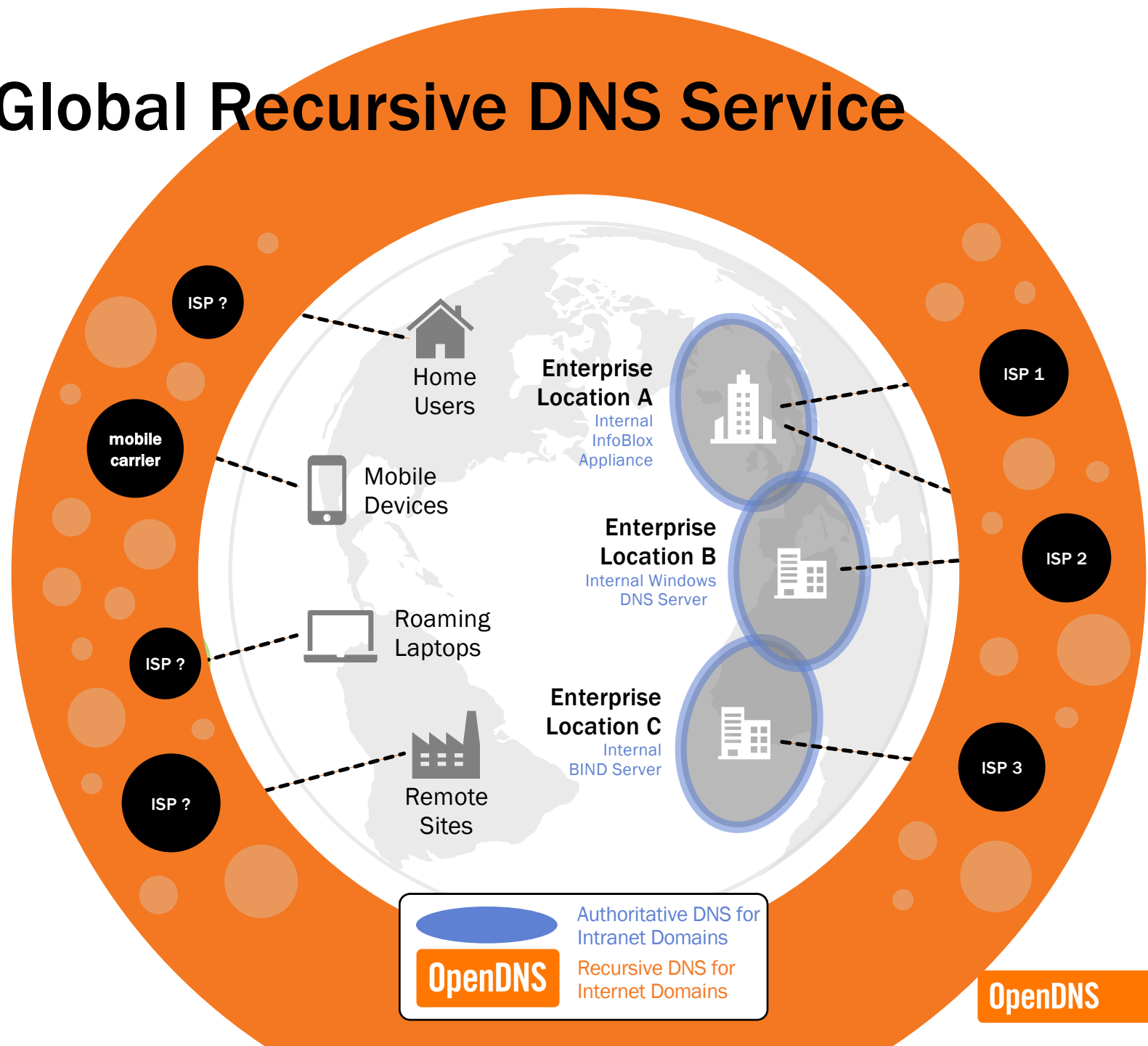
## BENEFITS

Global Internet  
Activity Visibility

Network Security  
w/o Adding Latency

Consistent Policy  
Enforcement

Internet-Wide  
Cloud App Visibility

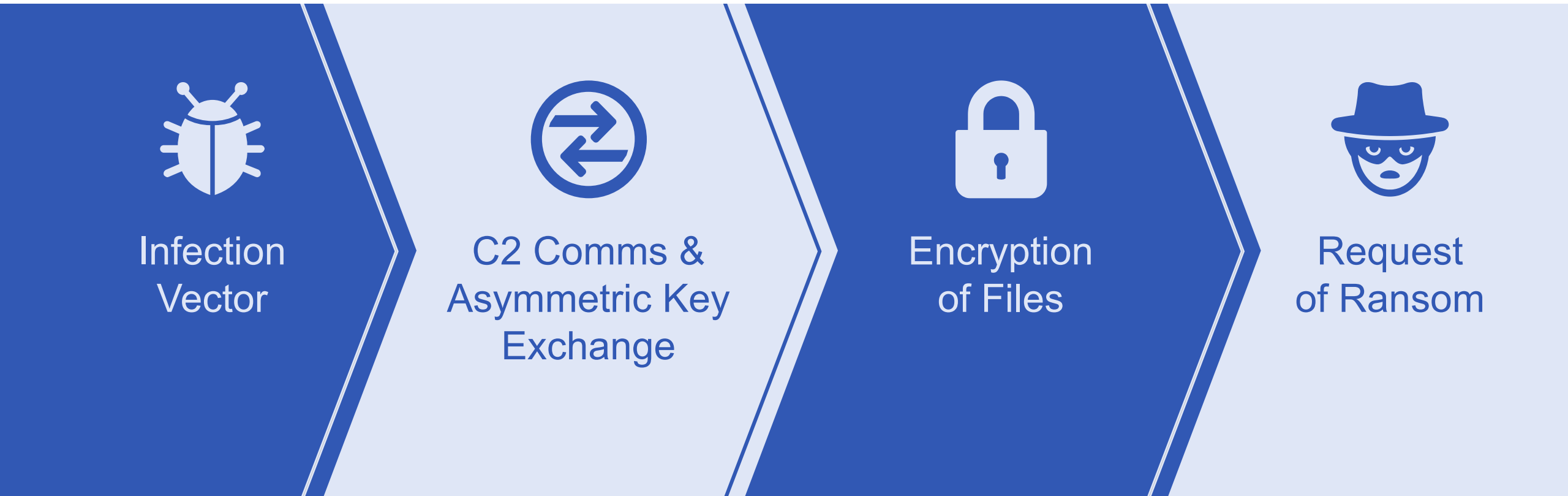


# Predictive Detectors Used by OpenDNS

- SecureRank
- Co-Occurrences
- NLPRank
- DGA Detectors
- Traffic Spike Detectors
- IP Space Monitoring



# Typical Ransomware Infection





## Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

**You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.**

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.



**WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.**

View

95:59:29

Next >>

# Most Ransomware Relies on C2 Callbacks

NAME	Encryption Key				Payment MSG
	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



# Feeling Locky?

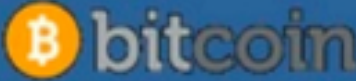
- Encrypts & renames the infected device's important files with .locky extension
- Appx 90,000 victims per day <sup>[1]</sup>
- Ransom ranges from 0.5 – 1.0 BTC (1 BTC ~ 799 USD)

[1] Forbes [Ransomware Crisis](#)

We present a special software - **Locky Decrypter** - which allows to decrypt and return control to all your encrypted files.

How to buy Locky decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.



2. You should register BitCoin wallet ([simplest online wallet](#) OR [some other methods of creating wallet](#))
3. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

*Here are our recommendations:*

- [LocalBitcoins.com \(WU\)](#) - Buy Bitcoins with Western Union
- [Coincafe.com](#) - Recommended for fast, simple service.

Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person

# Blocking Ransomware: Real World Example with a Locky Domain

## dqtfhkgskushlum[.]org (detection date: March 15<sup>th</sup> 2016)

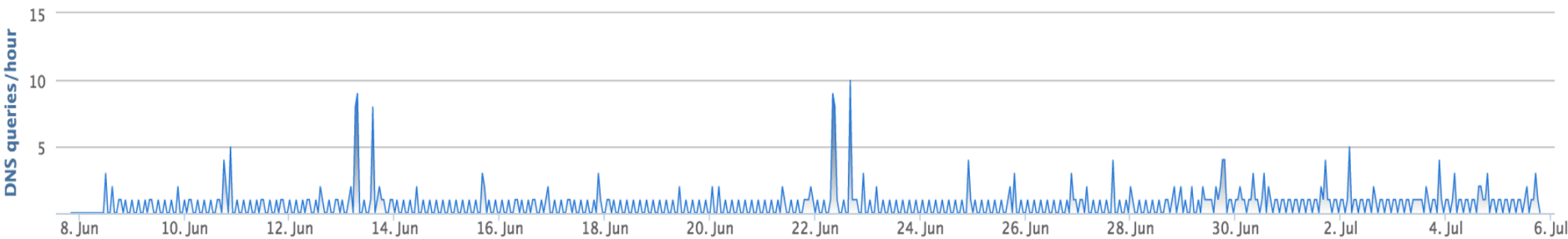
### DETAILS FOR DQTFHKGSKUSHLUM.ORG

This domain is currently in the OpenDNS Security Labs block list

Search in Google

Search in VirusTotal

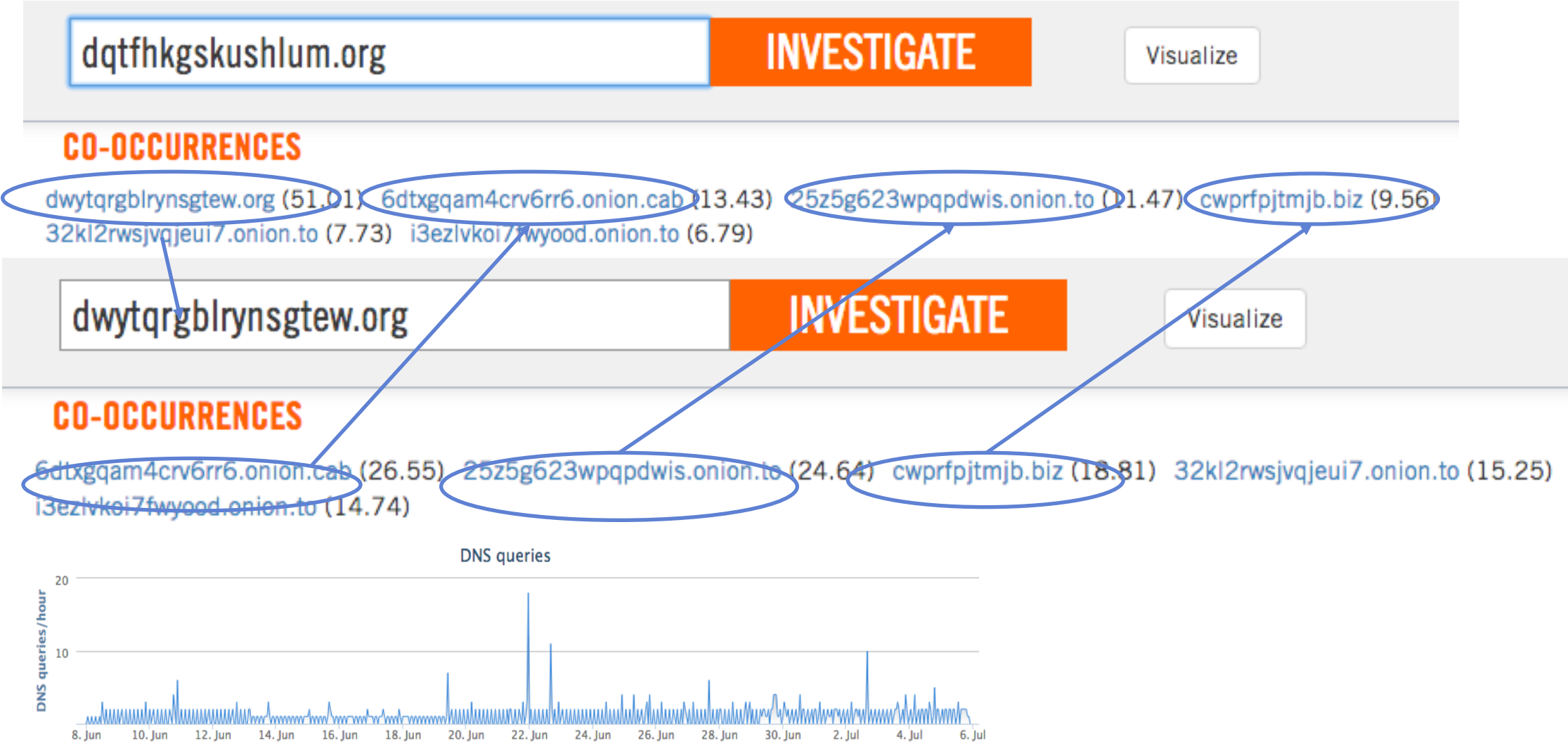
This domain is associated with the following attack: Locky Ransomware



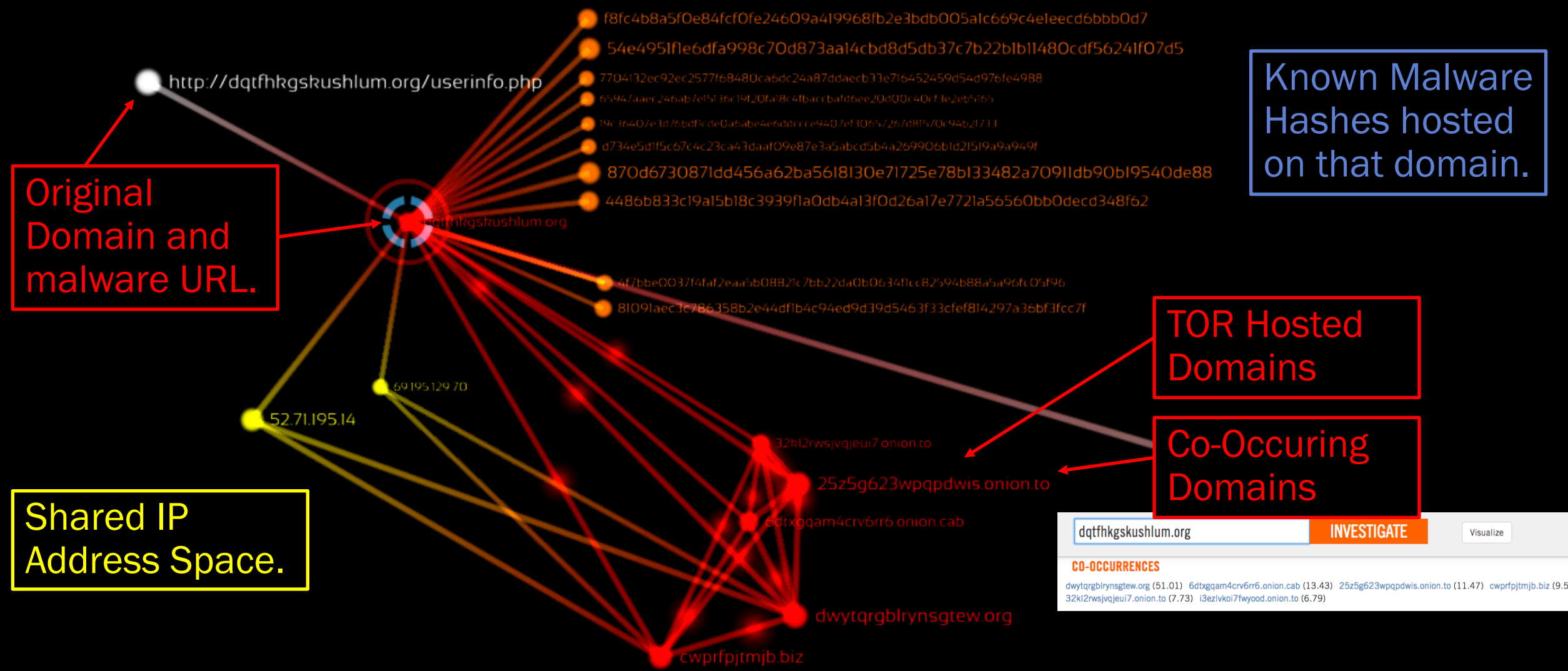
### DOMAIN TAGGING

Period	Category	URL
Jun 27, 2016 - Current	Malware	
May 15, 2016 - Current	Malware	

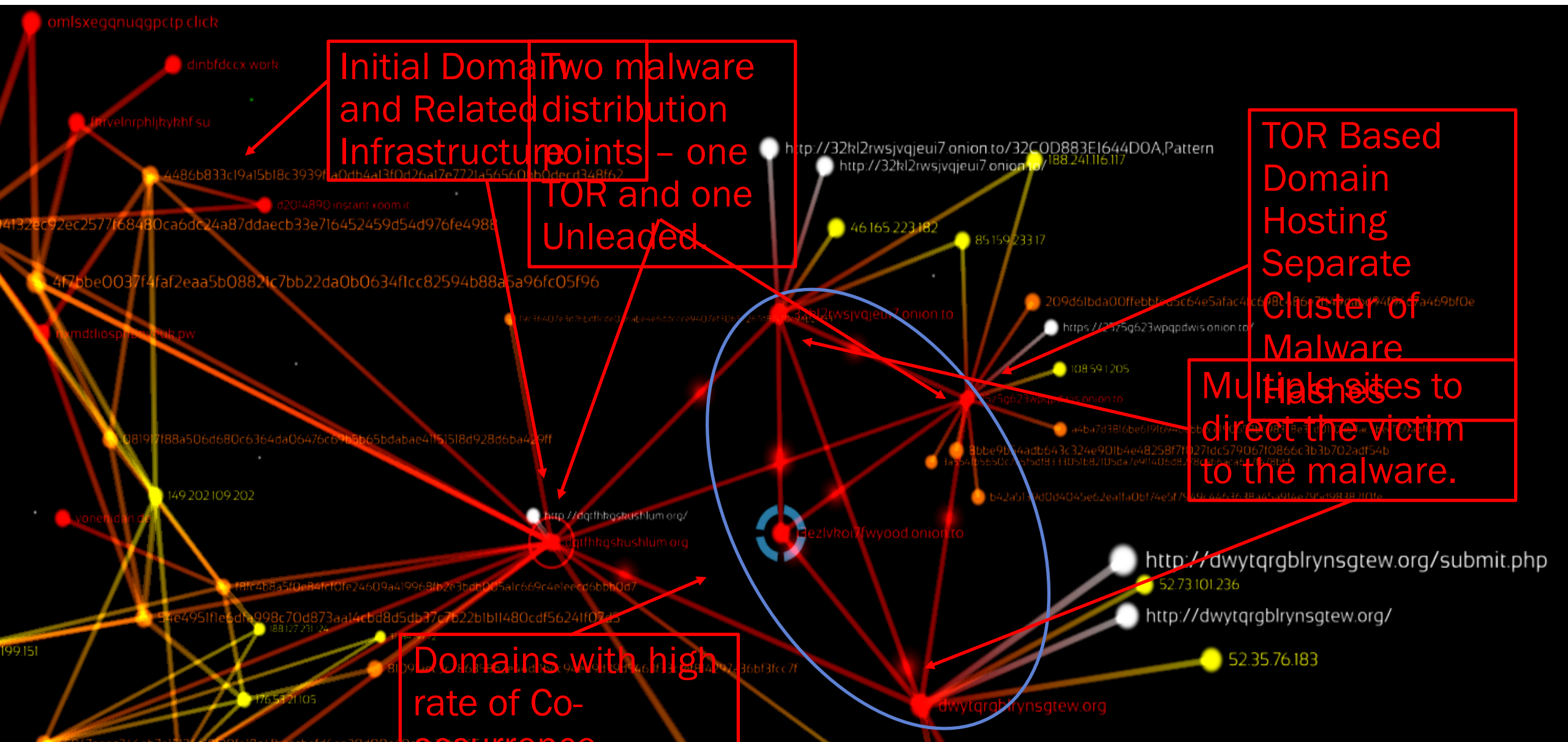
# What do we know about this domain?



# Locky – Blocking a Ransomware Domain



# Locky – Blocking a Ransomware Domain





# Discover the Threats Before They Happen!

TG Link:

<https://panacea.threatgrid.com/samples/67172aee0c03ef6bfeea05f0362b5753>

(detection date: 5/18/16 18:31:09)

## Analysis Report

Resubmit

ID	67172aee0c03ef6bfeea05f0362b5753	Filename	1449223560.docm
OS	2600.xpsp.080413-2111	Magic Type	Microsoft Office 2007+ - DOCM
Started	5/18/16 18:31:09	Analyzed As	docx
Ended	5/18/16 18:37:10	SHA256	4f7bbe0037f4faf2eaa5b08821c7bb22da0b0634f1cc82594b88a5a96fc05f96
Duration	0:06:01	SHA1	4098127ced6e6eb55dff5851699f00b8e95f6249
Sandbox	phl-work-10 (pilot-d)	MD5	39e53abce7b2d073bc5dfb0e5fe020ce
		Tags	<div><div>tag</div><div>Locky</div></div>

## Behavioral Indicators

Threat Score: 100

⊕ Document Created an Executable File	Severity: 100 Confidence: 100
⊕ A Document File Established Network Communications	Severity: 100 Confidence: 90

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

# Discover the Threats Before They Happen

VT Link:

[https://www.virustotal.com/en/file/4f7bbe0037f4faf2eaa5b08821c7bb22da0b0634f1cc82594b88a5a96fc05f96/analysis/](https://www.virustotal.com/en/file/4f7bbe0037f4faf2eaa5b08821c7bb22da0b0634f1cc82594b88a5a96fc05f96/analysis/96/analysis/)

(first analysis: 5-28-2016, 10 days after first sample hit ThreatGrid, see previous slide)



SHA256: 4f7bbe0037f4faf2eaa5b08821c7bb22da0b0634f1cc82594b88a5a96fc05f96

File name: c2bf0842f0c0c4545181d4c08508d1142d9b5a30

Detection ratio: 34 / 57

Analysis date: 2016-05-28 08:08:04 UTC ( 1 month, 1 week ago )





An aerial photograph of a city at sunrise. The sun is low on the horizon, creating a bright, hazy glow over the city. The sky is filled with soft, golden clouds. In the foreground, several tall buildings are visible, partially obscured by a thick layer of fog or low clouds. A dark, rounded rectangular banner is centered over the image, containing the text "#DemoTime!".

**#DemoTime!**