
WELCOME
CISCO UMBRELLA TRAINING

INTRODUCTIONS

ROBIN WOODSOME, FIELD OPERATIONS MANAGER

CONSORTIUM UPDATE

ESSAM EL-BEIK, K-12 PROJECT LEAD

Illinois Century Network - Benefits

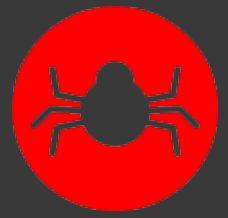
- Secure Internet Access
- Broadband Circuits
- Routers
- Security Services

To Connect to ICN email DoIT.ICN.K12@illinois.gov

DoIT
Illinois Department of Innovation & Technology

Cisco Umbrella

Secure access to the internet



Agenda: Session #1

- Introduction to Umbrella DNS security via the Illinois Century Network
  - What is it, how does it work/protect?
  - What features?
- Console overview
  - Security reports
  - Content filtering
  - Application Discovery
- Q & A

Starting with DNS

Domain registrar

Maps and records names to #s in “phone books

Authoritative DNS

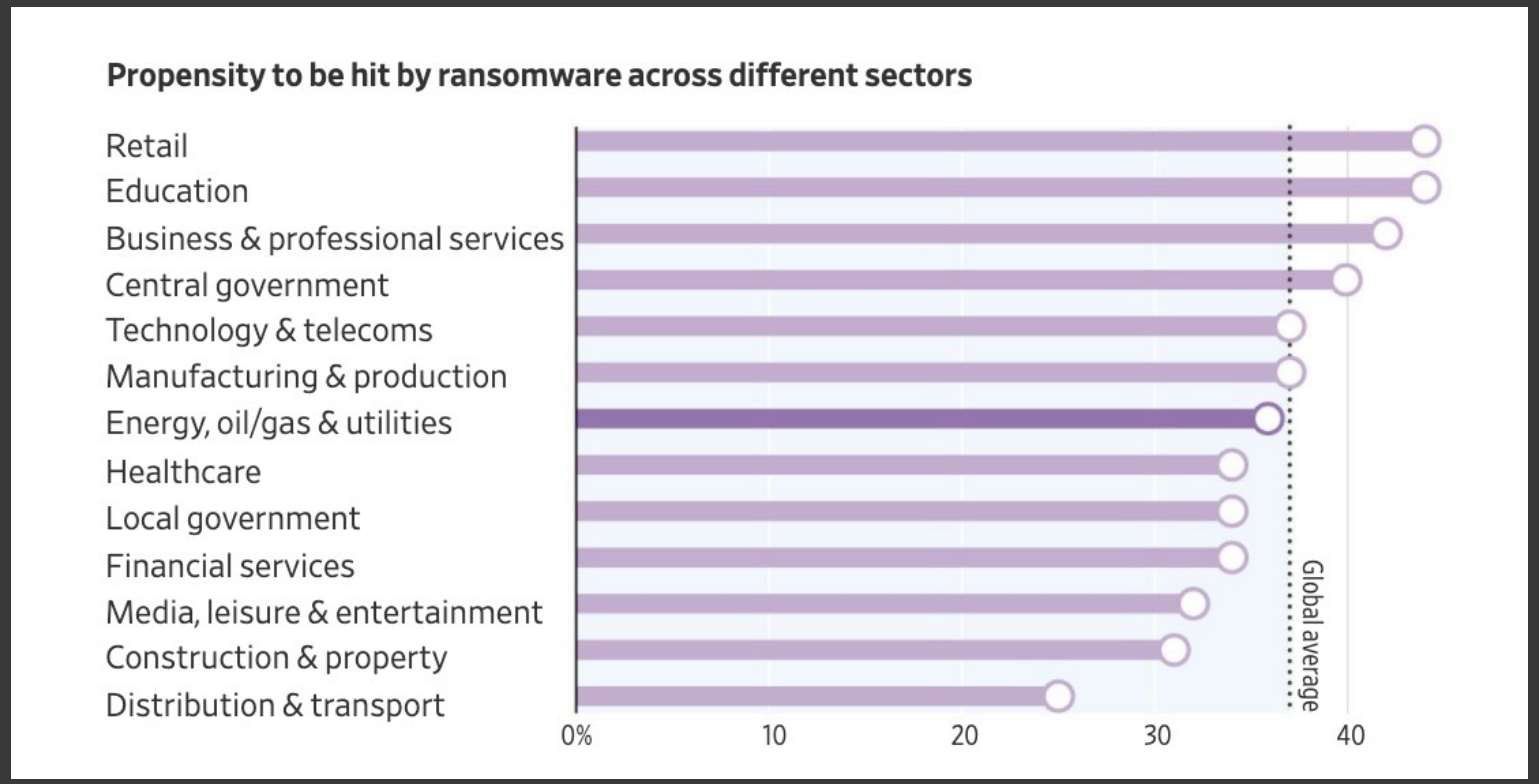
Owns and publishes the “phone books

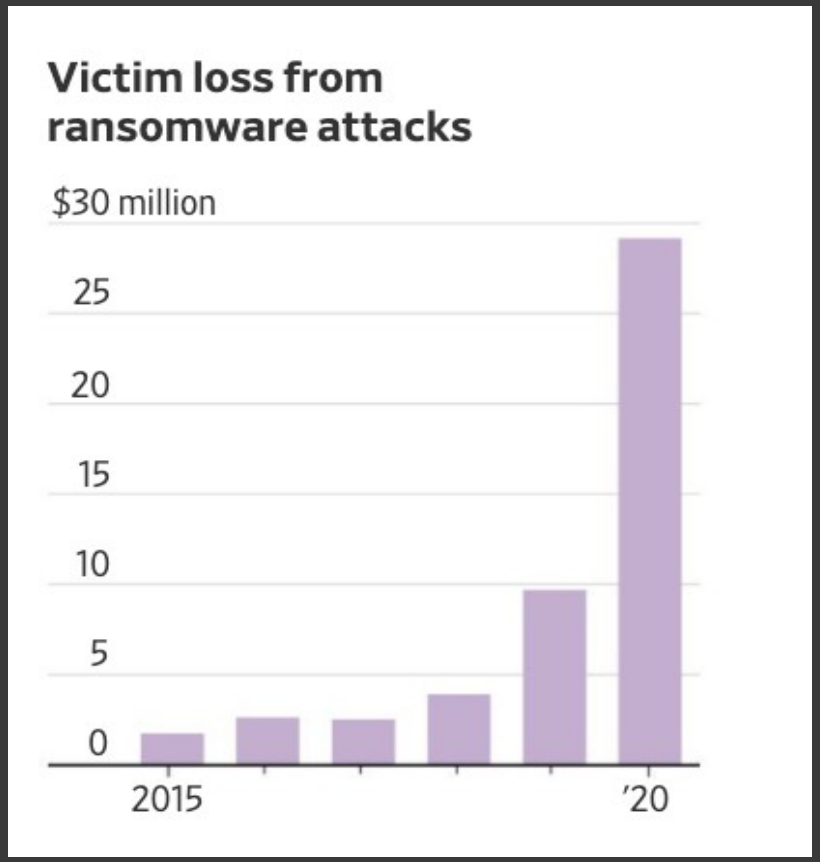
Recursive DNS

Looks up and remembers the #s for each name

Formerly know as OpenDNS

Ransomware in Education





December 2020: FBI, CISA and MS-ISAC Advisory

The number of reported ransomware incidents involving K-12 schools jumped from 28% – from January through July – to 57% in the Fall

The average ransom payment in the first quarter of 2021 was $220,298, a 43% increase from the previous quarter. - WSJ

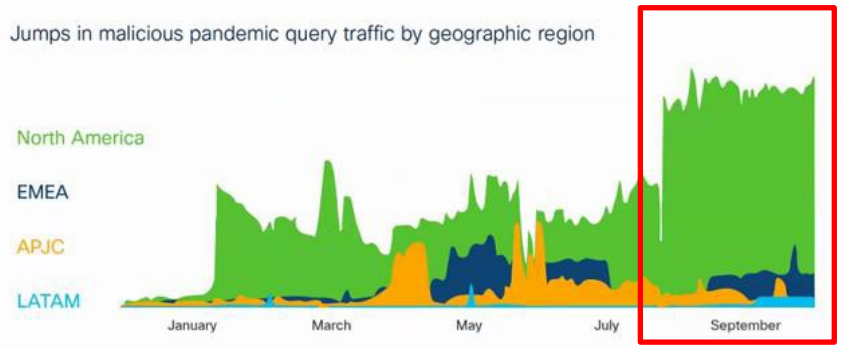
https://www.wsj.com/articles/ransomware-now-seen-as-threat-to-national-security-11619728378?mod=article_relatedinline

Pandemic-related phishing

2020 top threats for customers

1. 91% of Umbrella customers saw a domain linked to malware
2. Phishing jumped from 46% in 2019 to 83% in 2020
3. Pandemic-related phishing drove the increase
4. Cryptomining was twice as large as the next greatest attack type

#4: Pandemic themes drive phishing activity



- Malicious actors have taken advantage of our interest in the topic and have set up numerous sites to phish for credentials and drop malware
- 38% of Umbrella's customer base have visited malicious COVID-19 domains
- At its peak, there was a 7.2X increase in COVID-19 query volume in North America from Feb - Aug and a 25.3X growth outside of North America

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
KeRanger	●			●	DNS

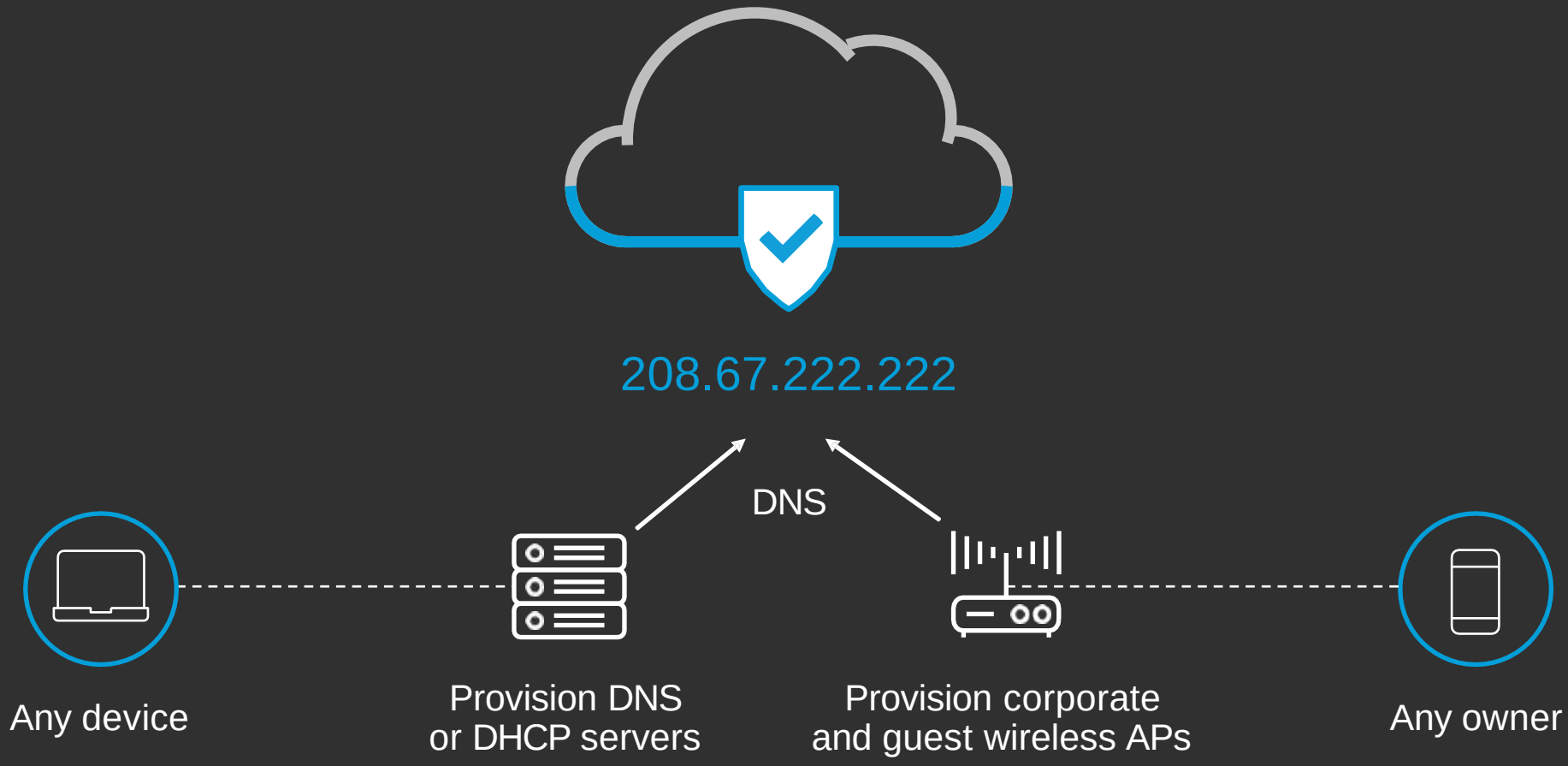
AV-TEST Security Efficacy Report

Featuring Cisco Umbrella

- Security efficacy is one of the top competitive differentiators for Umbrella
- This report validates that Umbrella is #1 in security efficacy!
- The test was performed by AV-TEST a third party independent tester in Nov-Dec 2019 with their own malicious samples (not Cisco's)
- Umbrella consistently performed better than the competition in DNS protection!

Simplest way to protect any device

Point external DNS traffic to Umbrella



Umbrella via the Illinois Century Network

- Phishing, malware, command & control (malicious things on the Internet) protection
- Content filtering from the DNS-layer
  - Can keep existing content filtering and deploy just DNS Security ** in most cases **
- Application visibility and control
- Active directory integration for user identity
- On-network protection
- Off-network protection (laptops, Chromebooks, iOS devices, etc.)
- Can migrate your existing Umbrella environment over to ICN
- Access to SecureX platform

Agenda: Session #2

- Configuration and policy creation
  - Protecting a network
  - Roaming Client
    - AnyConnect / Stand-alone client
    - MDM integration for devices
  - Virtual appliance discussion
- Short SecureX demo with Umbrella
- Q & A