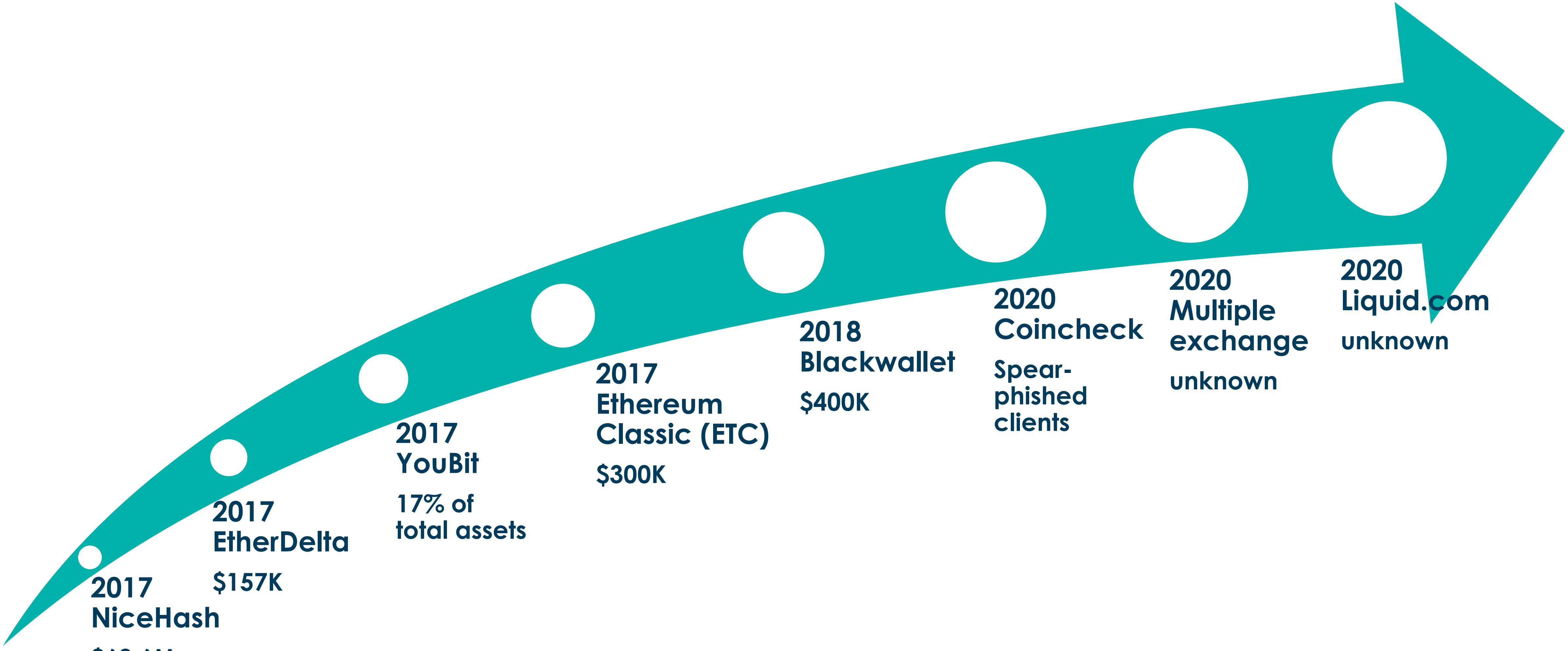
CSC

“It’s always DNS!” – Why DNS is the biggest single point of failure in the New Norm

Hong Kong IS Summit 2021

Security by Design
vs.
Security by Obscurity

Cryptocurrency hacks



2017
NiceHash

$62.6M

2017
EtherDelta

$157K

2017
YouBit

17% of
total assets

2017
Ethereum
Classic (ETC)

$300K

2018
Blackwallet

$400K

2020
Coincheck

Spear-phished
clients

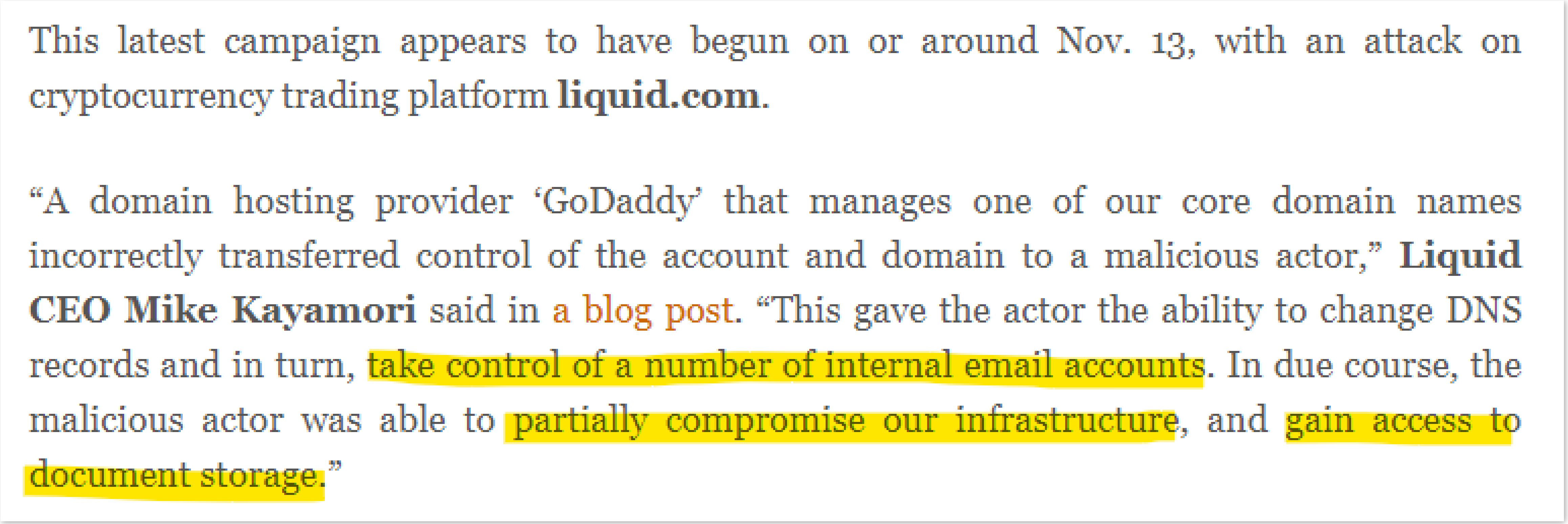
2020
Multiple
exchange

unknown

2020
Liquid.com

unknown

How domain hijacking used to compromise infrastructure and steal emails



This latest campaign appears to have begun on or around Nov. 13, with an attack on cryptocurrency trading platform **liquid.com**.

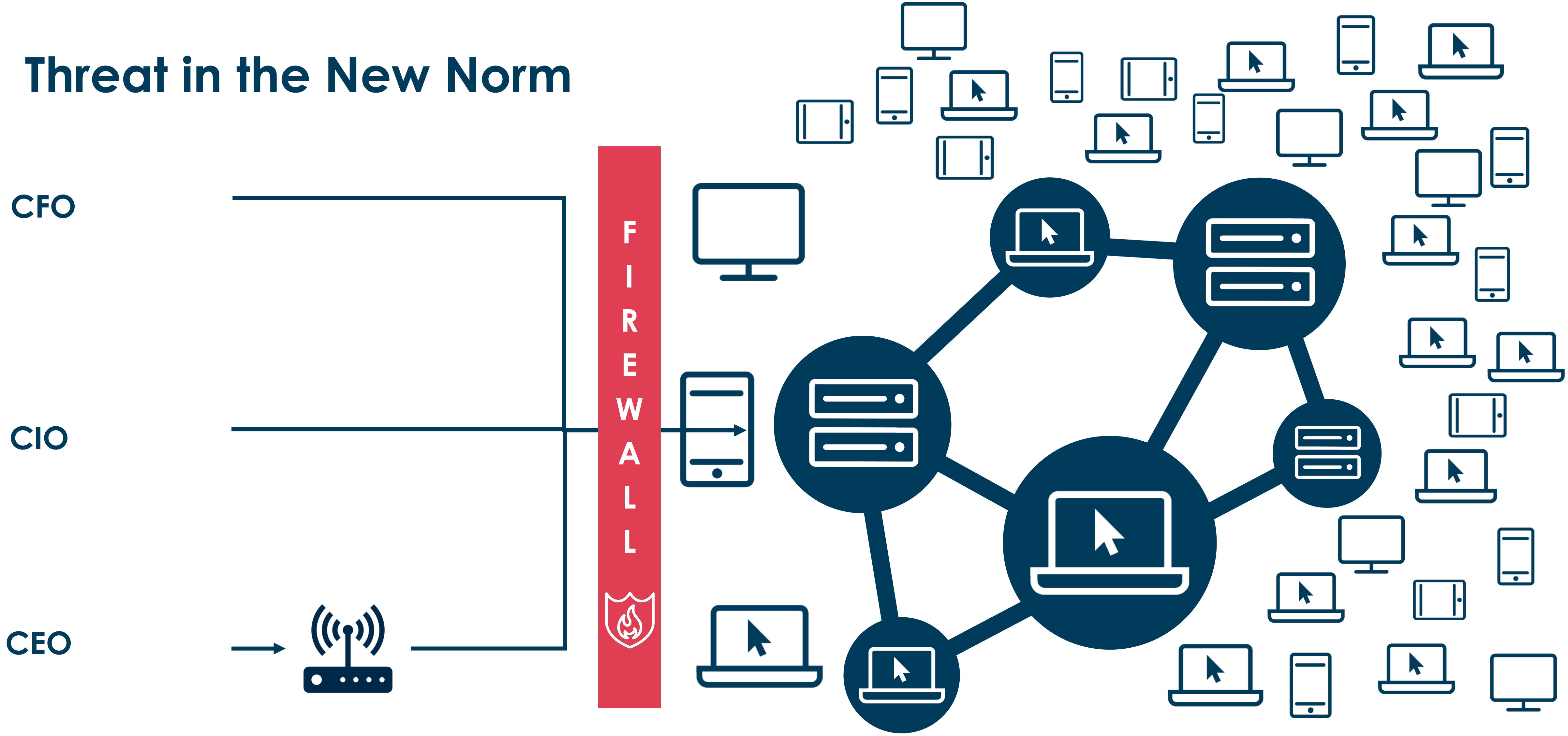
“A domain hosting provider ‘GoDaddy’ that manages one of our core domain names incorrectly transferred control of the account and domain to a malicious actor,” **Liquid CEO Mike Kayamori** said in a blog post. “This gave the actor the ability to change DNS records and in turn, take control of a number of internal email accounts. In due course, the malicious actor was able to partially compromise our infrastructure, and gain access to document storage.”

It’s always DNS!

In the internet age,
“Security by Design”
doesn’t always work because the
internet is INSECURE by design

CSC

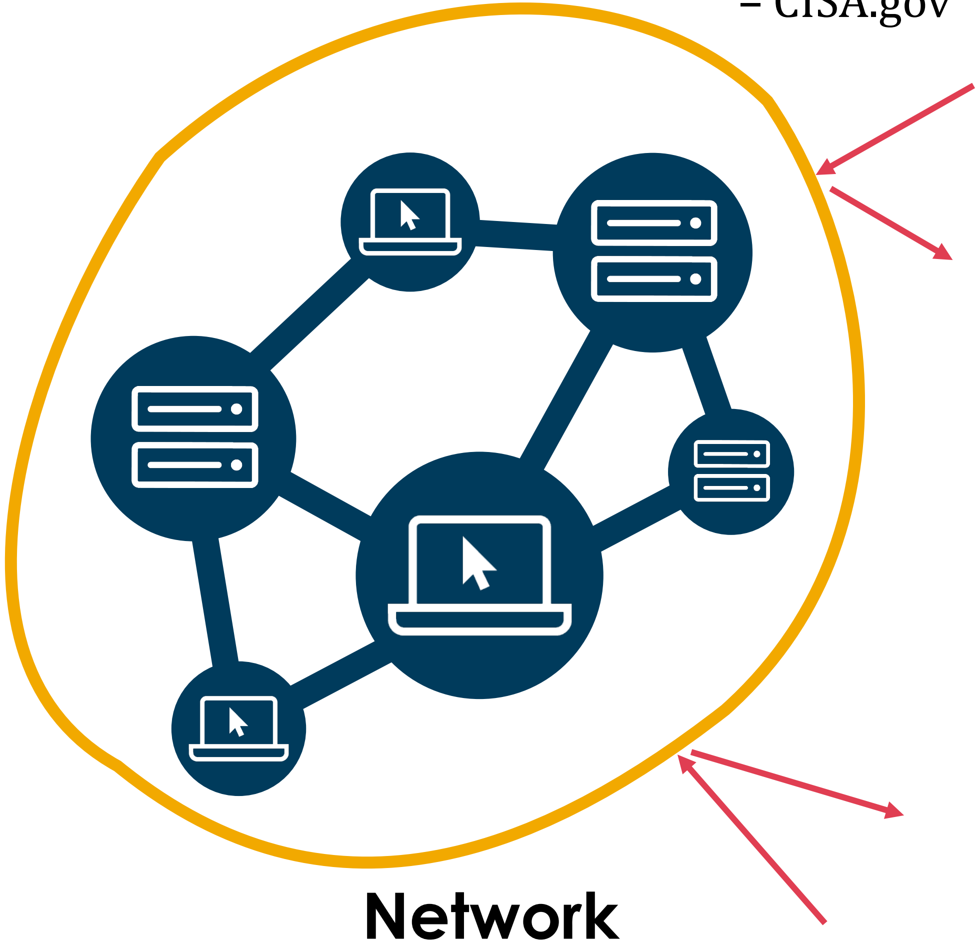
Threat in the New Norm



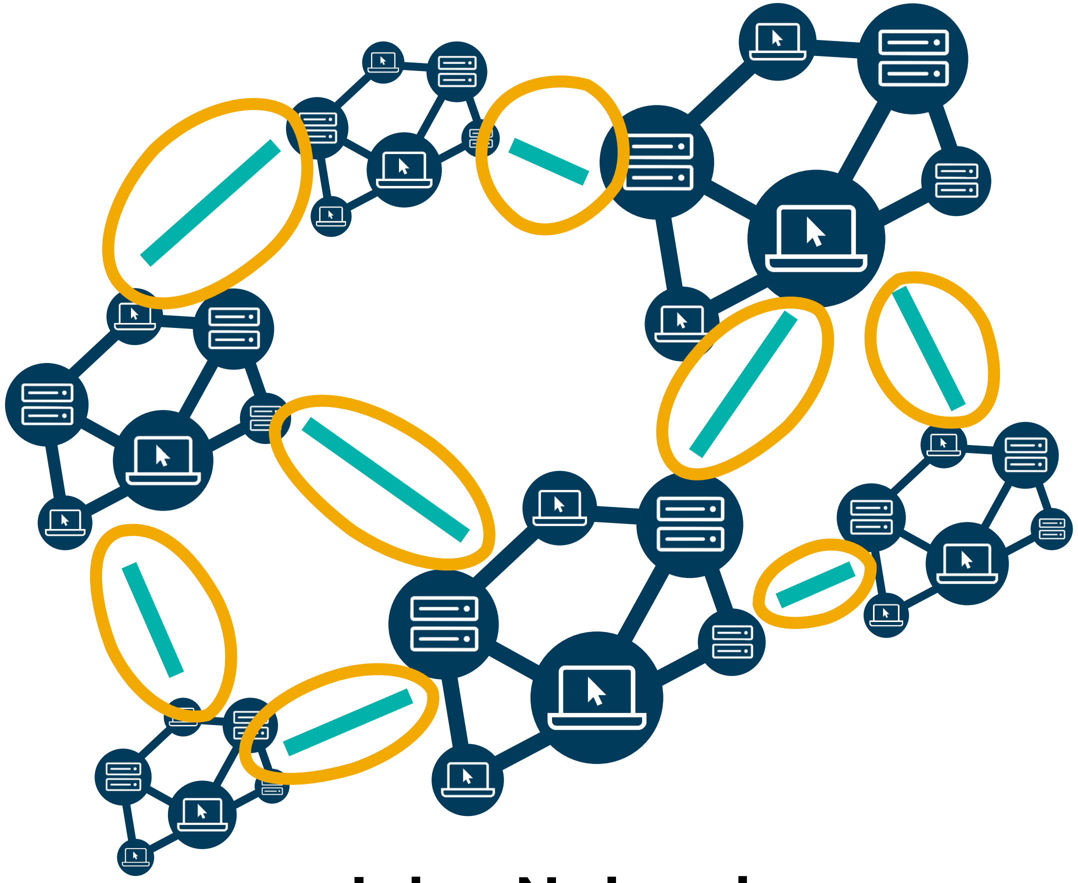
Network security needs to go OUTSIDE your network

Cyber security = network security?

“Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information”
– CISA.gov

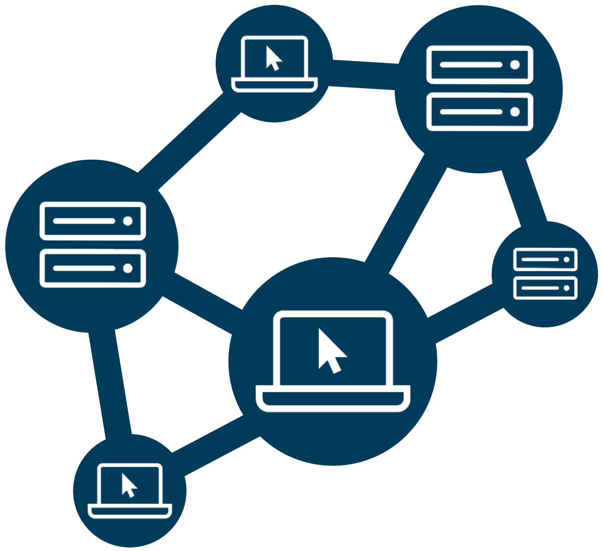


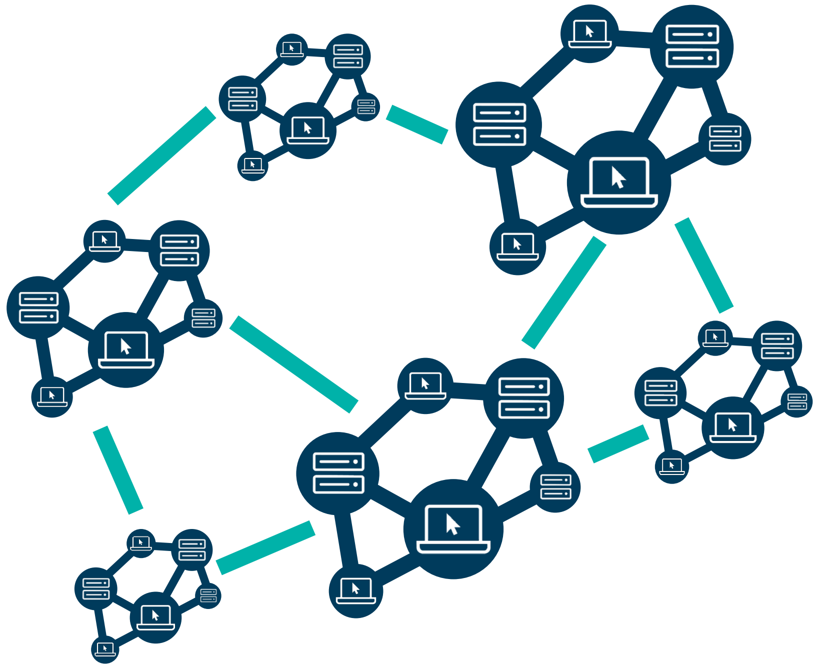
Network



Inter-Network

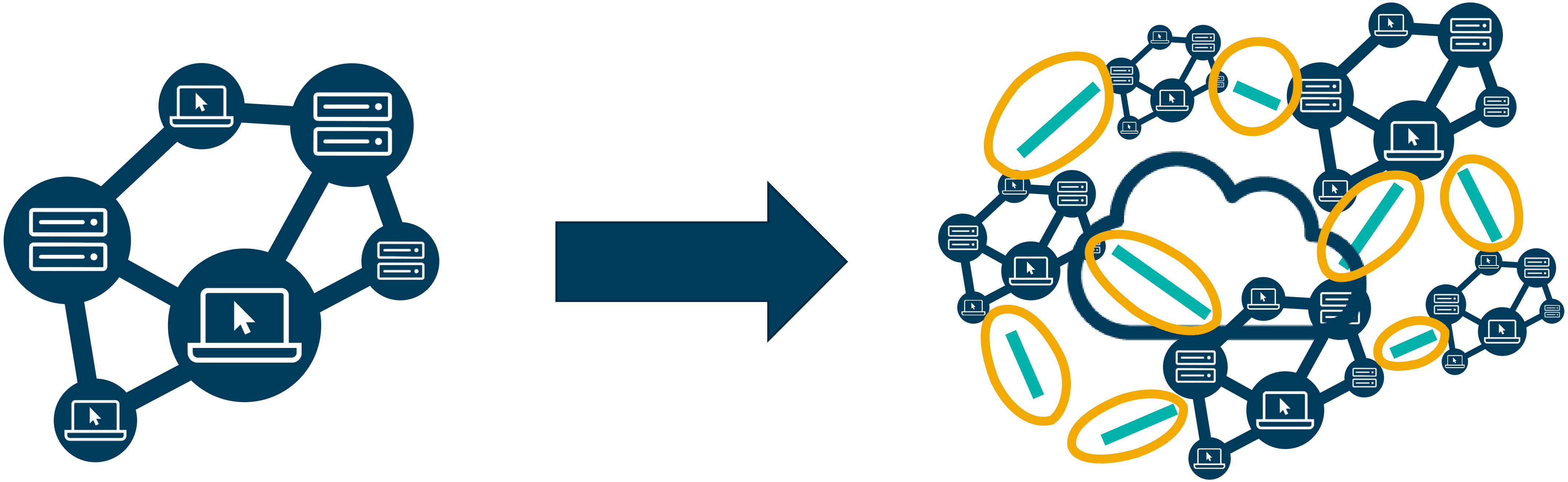
Network vs inter-network





Network	Inter-Network
OSI Model	TCP/IP model
Created by ISO	Created by Department of Defense
7 clearly defined layers	4 loosely defined layers (in fact, some hate the concept of layering)

Cloud/CDN migration = securing the inter-network?



- ‘*Most often, "cloud migration" describes the move from on-premises or legacy infrastructure to the cloud*’ – Cloudflare
- Cloud simplified and enhanced network security, however, it is not designed to resolve the threats from the inter-network

CSC

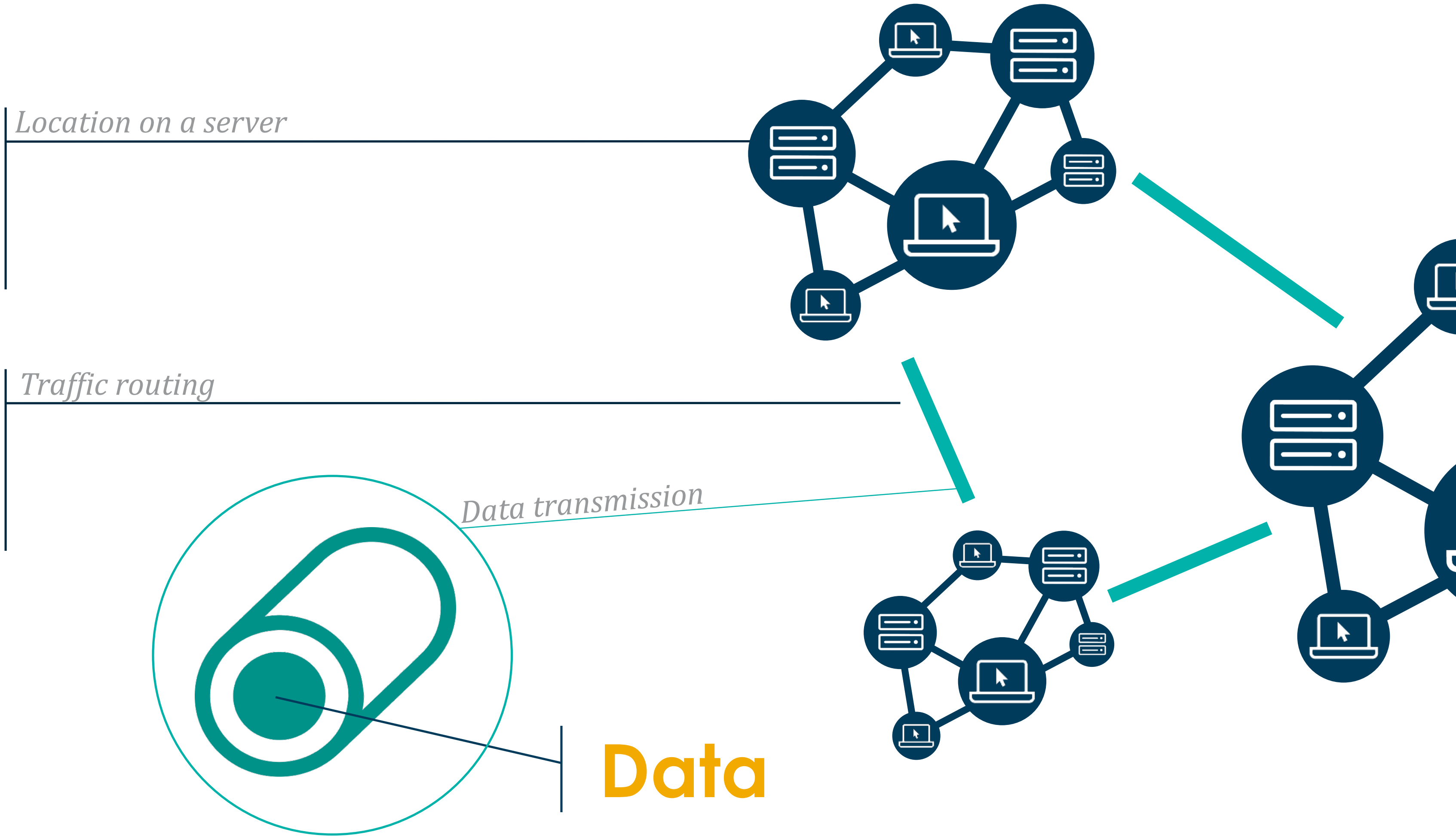
What’s the interconnection between networks?

Domain name

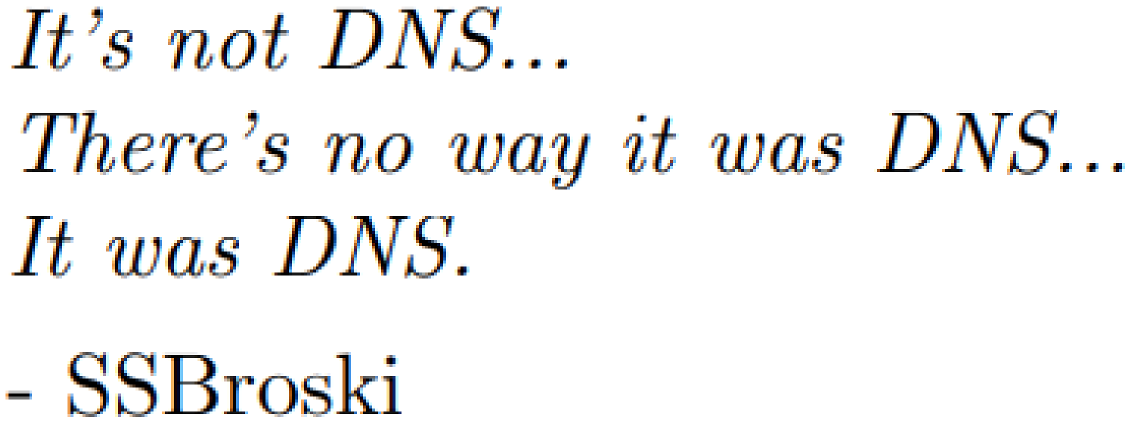
& IP address

DNS

& BGP



It’s always DNS, even if it is not the DNS!



It’s not DNS...
There’s no way it was DNS...
It was DNS.

- SSBroski

What’s the interconnection between networks?

Domain name

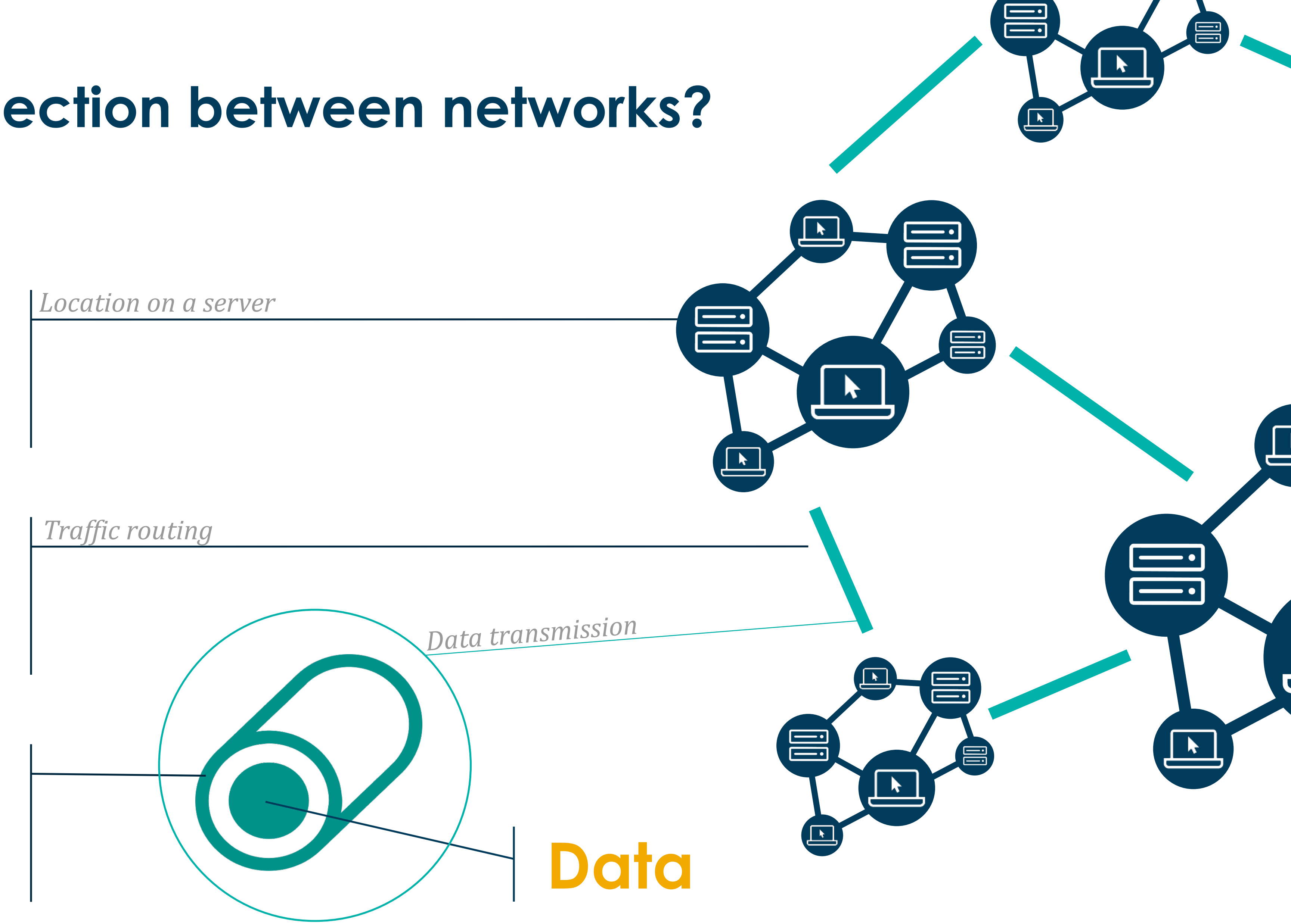
& IP address

DNS

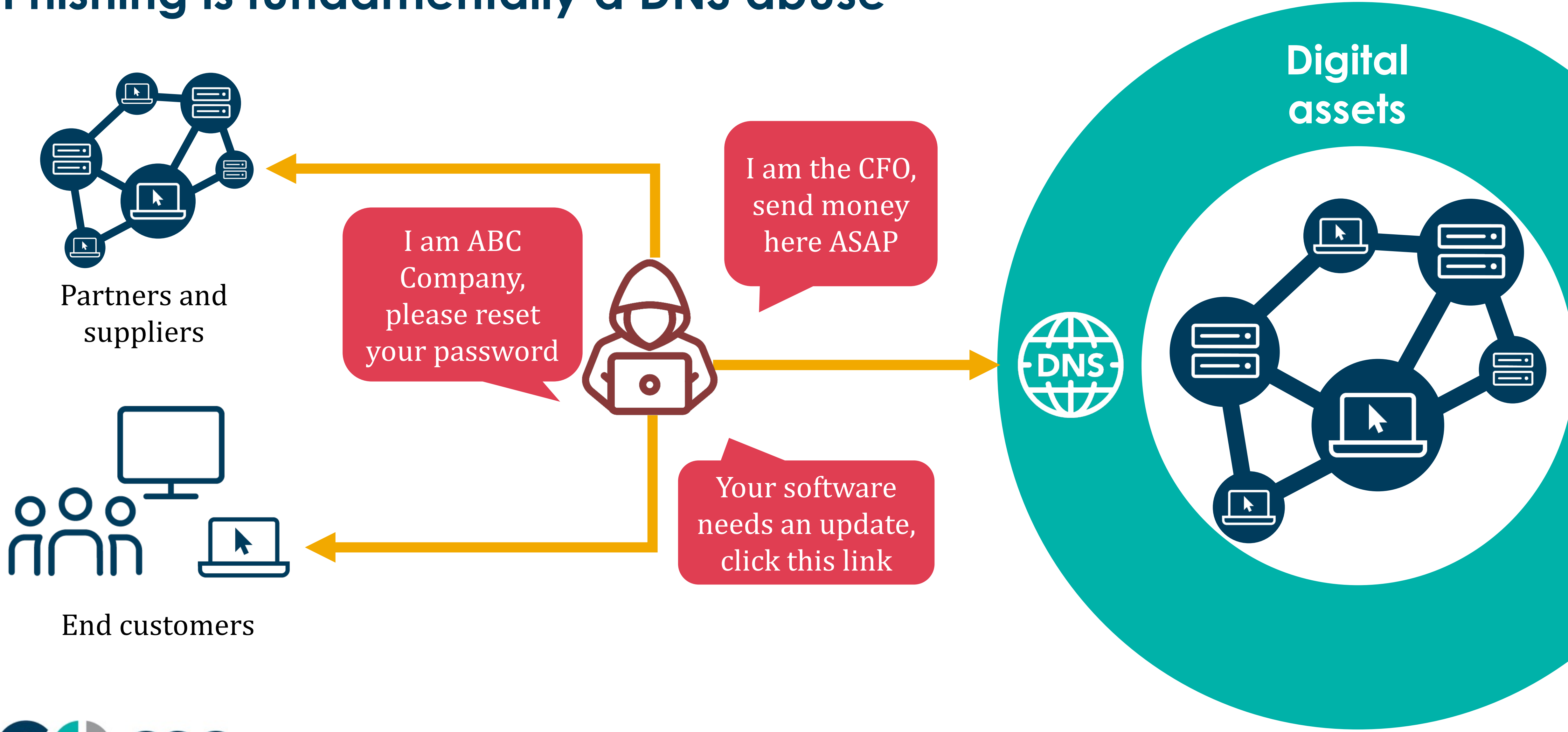
& BGP

Encryption

TLS/SSL



Phishing is fundamentally a DNS abuse



Digital assets

I am the CFO, send money here ASAP

I am ABC Company, please reset your password

Your software needs an update, click this link

Partners and suppliers

End customers

As defined by the internet regulator

- ICANN (Internet Corporation of Assigned Name and Numbers)
- Addressing DNS abuse is one of the highest priority in 2020

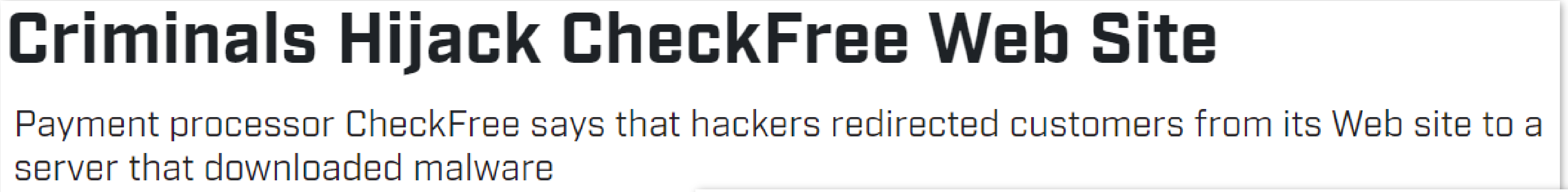
ICANN

DNS abuse =

- Spam
- Phishing
- Malware
- Botnets (i.e. DDoS attacks)
- Pharming (i.e. DNS hijacking)

Wait a minute!
Malware??

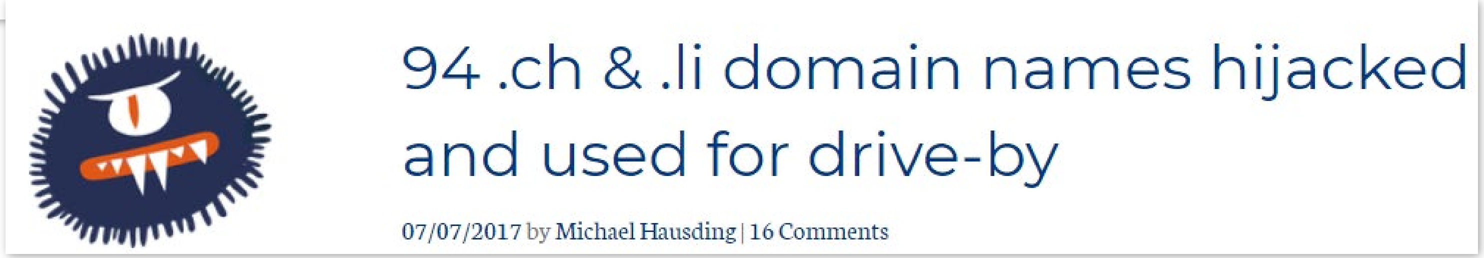
How domain hijacking led to malware



Criminals Hijack CheckFree Web Site

Payment processor CheckFree says that hackers redirected customers from its Web site to a server that downloaded malware

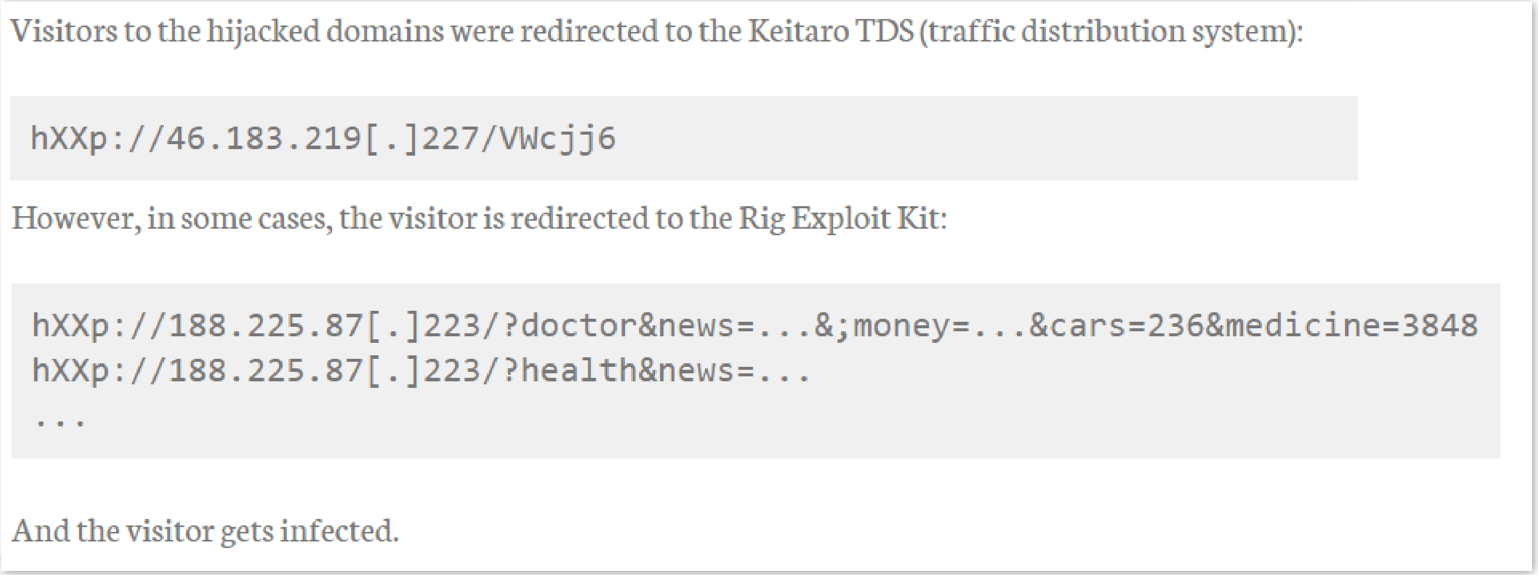
- Compromised Network Solutions
- All customers of CheckFree were redirected to a website server that automatically downloaded malware



94 .ch & .li domain names hijacked and used for drive-by

07/07/2017 by Michael Hausding | 16 Comments

French Registrar Gandi were compromised



Visitors to the hijacked domains were redirected to the Keitaro TDS (traffic distribution system):

```
hXXp://46.183.219[.]227/VWcjj6
```

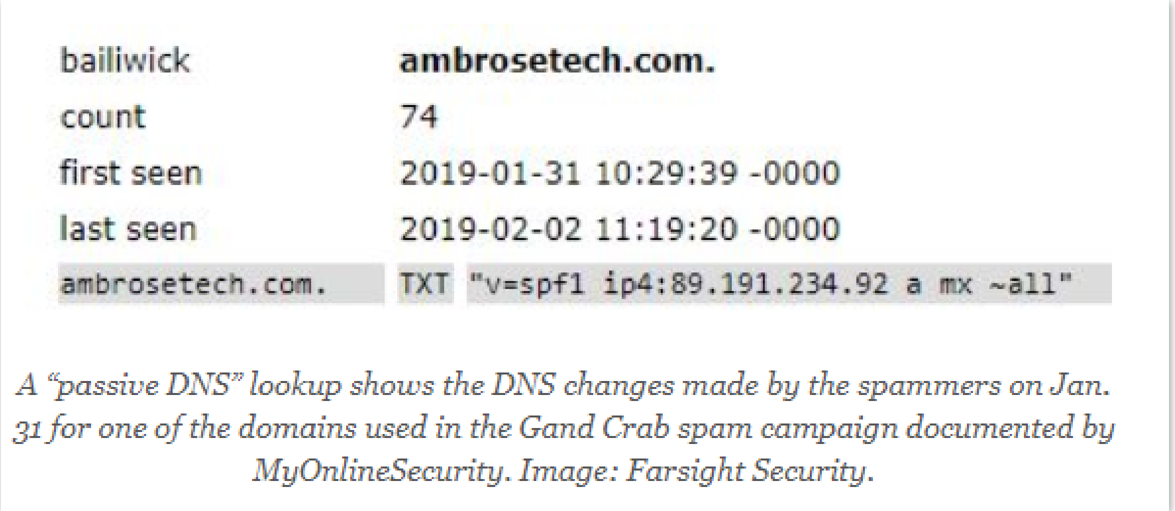
However, in some cases, the visitor is redirected to the Rig Exploit Kit:

```
hXXp://188.225.87[.]223/?doctor&news=...&;money=...&cars=236&medicine=3848
hXXp://188.225.87[.]223/?health&news=...
...
```

And the visitor gets infected.

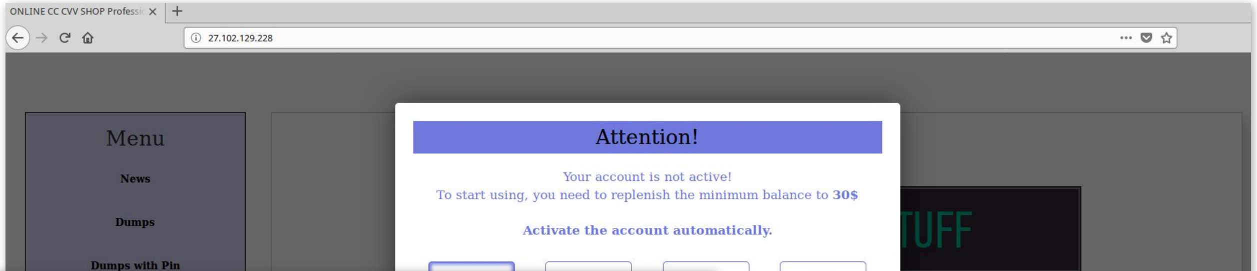
How DNS hijacking led to ransomware

- GandCrab is the most popular ransomware in 2018/19
- Significantly higher ransom – US $600 – 700K
- Research found that DNS hijacking was used to launch the attack



```
bailiwick        ambrosetech.com.
count            74
first seen       2019-01-31 10:29:39 -0000
last seen        2019-02-02 11:19:20 -0000
ambrosetech.com.   TXT  "v=spf1 ip4:89.191.234.92 a mx ~all"
```

A "passive DNS" lookup shows the DNS changes made by the spammers on Jan. 31 for one of the domains used in the Gand Crab spam campaign documented by MyOnlineSecurity. Image: Farsight Security.



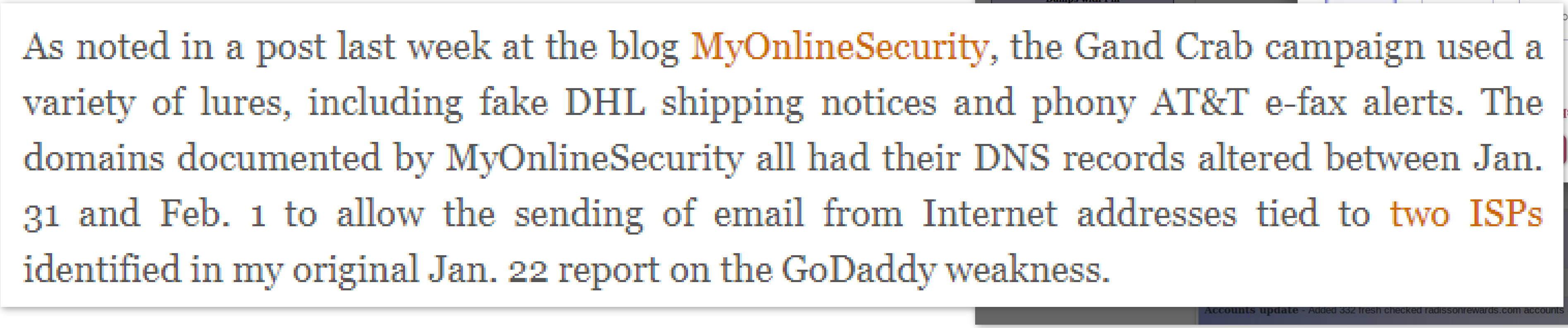
Attention!

Your account is not active!
To start using, you need to replenish the minimum balance to 30$

Activate the account automatically.

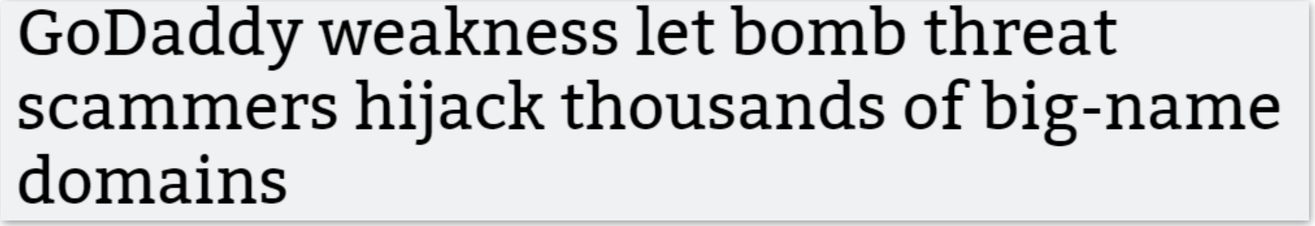
gskMv5wYW

Accounts update - Added 332 fresh checked radissonrewards.com accounts in radi_di base



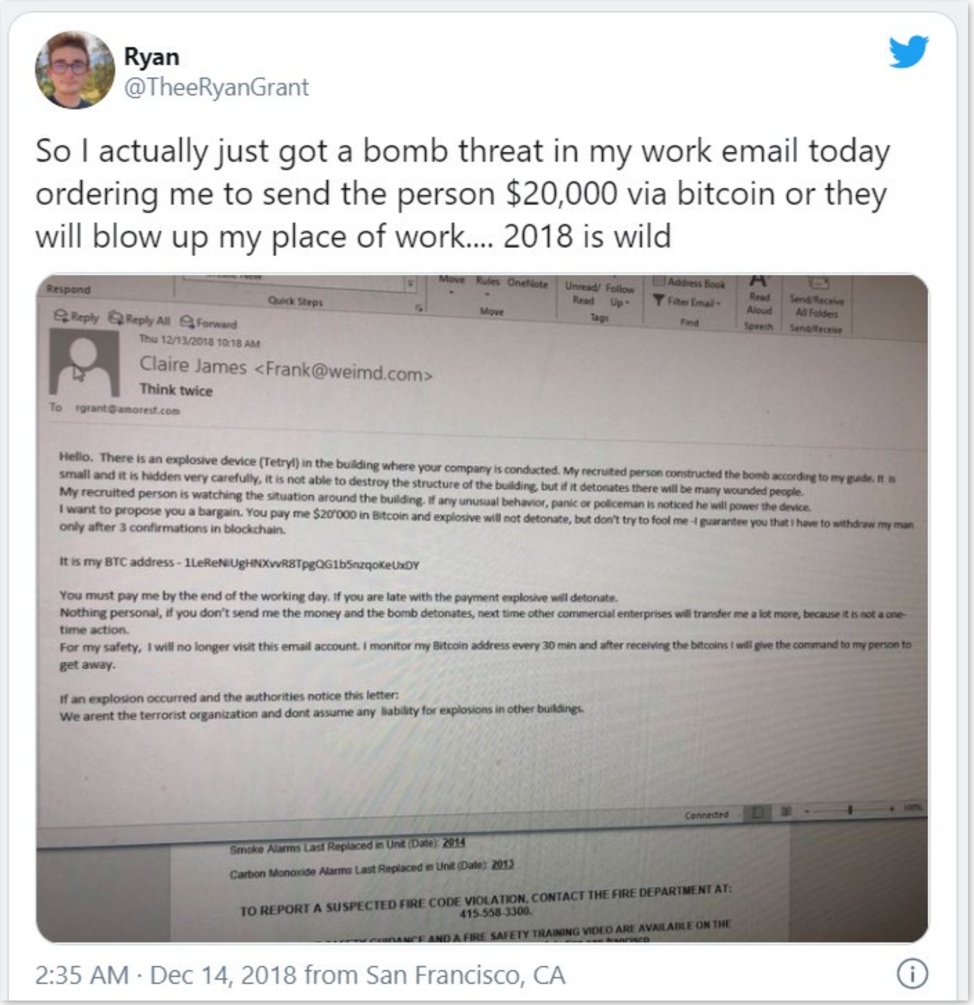
As noted in a post last week at the blog MyOnlineSecurity, the Gand Crab campaign used a variety of lures, including fake DHL shipping notices and phony AT&T e-fax alerts. The domains documented by MyOnlineSecurity all had their DNS records altered between Jan. 31 and Feb. 1 to allow the sending of email from Internet addresses tied to two ISPs identified in my original Jan. 22 report on the GoDaddy weakness.

How DNS hijacking led to phishing and BEC



GoDaddy weakness let bomb threat scammers hijack thousands of big-name domains

- Defensive domains of Expedia, Mozilla, and Yelp with GoDaddy were compromised
  - Research found Facebook, MasterCard, Hilton, ING Bank, Warner Bros, MIT, McDonalds were also hijacked
- Hacker used the name to launch a phishing attack called snowshoe spamming
  - Used domains owned by well-known brands to increase reputation score to bypass spam filters
- Defensive names must be securely managed as well



Ryan
@TheeRyanGrant

So I actually just got a bomb threat in my work email today ordering me to send the person $20,000 via bitcoin or they will blow up my place of work.... 2018 is wild

Thu 12/13/2018 10:18 AM
Claire James <Frank@weimd.com>
Think twice
To rgrant@amorest.com

Hello. There is an explosive device (Tetryl) in the building where your company is conducted. My recruited person constructed the bomb according to my guide. It is small and it is hidden very carefully, it is not able to destroy the structure of the building, but if it detonates there will be many wounded people.
My recruited person is watching the situation around the building. If any unusual behavior, panic or policeman is noticed he will power the device.
I want to propose you a bargain. You pay me $20'000 in Bitcoin and explosive will not detonate, but don't try to fool me -I guarantee you that i have to withdraw my man only after 3 confirmations in blockchain.

It is my BTC address - 1LeReNiUgHNXvvR8TpgQG1b5nzqoKeUxDY

You must pay me by the end of the working day. If you are late with the payment explosive will detonate.
Nothing personal, if you don't send me the money and the bomb detonates, next time other commercial enterprises will transfer me a lot more, because it is not a one-time action.
For my safety, I will no longer visit this email account. I monitor my Bitcoin address every 30 min and after receiving the bitcoins I will give the command to my person to get away.

If an explosion occurred and the authorities notice this letter:
We arent the terrorist organization and dont assume any liability for explosions in other buildings.

Smoke Alarms Last Replaced in Unit (Date): 2014

Carbon Monoxide Alarms Last Replaced in Unit (Date): 2013

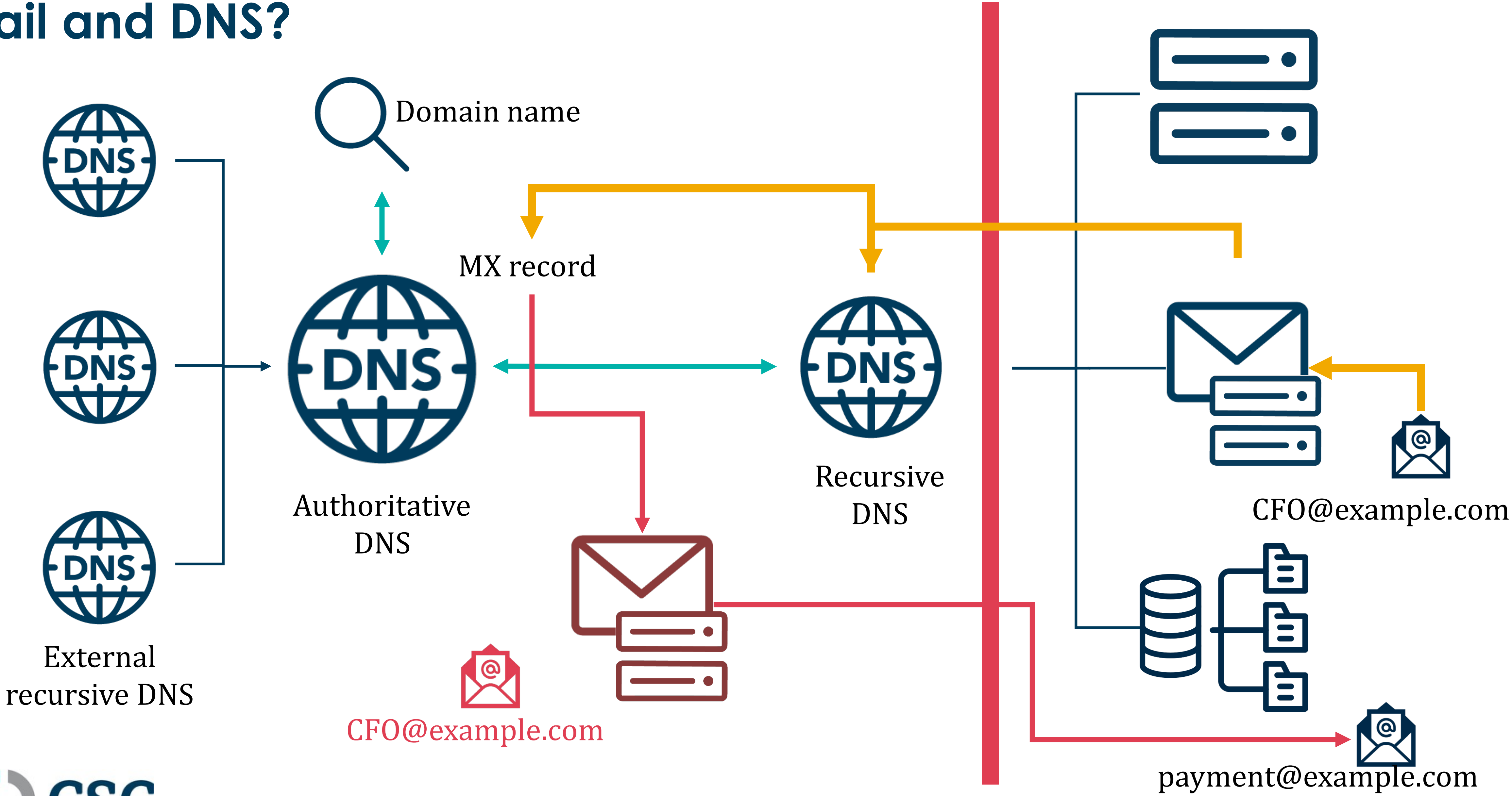
TO REPORT A SUSPECTED FIRE CODE VIOLATION, CONTACT THE FIRE DEPARTMENT AT:
415-558-3300.

FIRE SAFETY TRAINING VIDEO ARE AVAILABLE ON THE

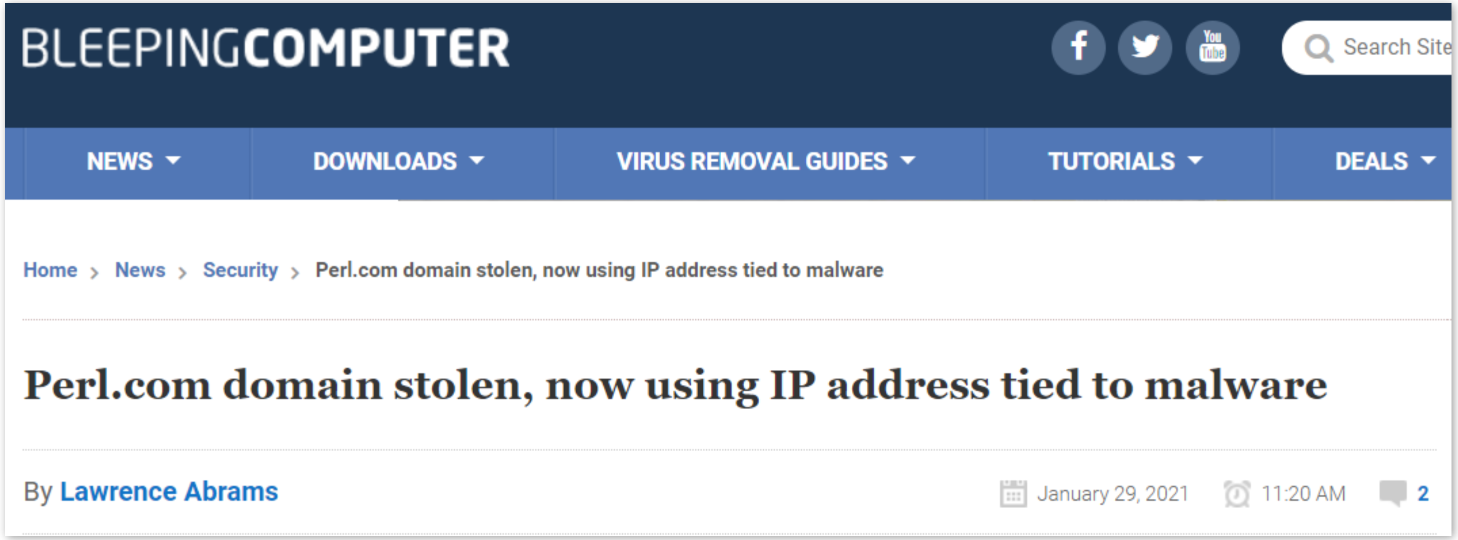
2:35 AM · Dec 14, 2018 from San Francisco, CA

https://arstechnica.com/information-technology/2019/01/godaddy-weakness-let-bomb-threat-scammers-hijack-thousands-of-big-name-domains/

Email and DNS?



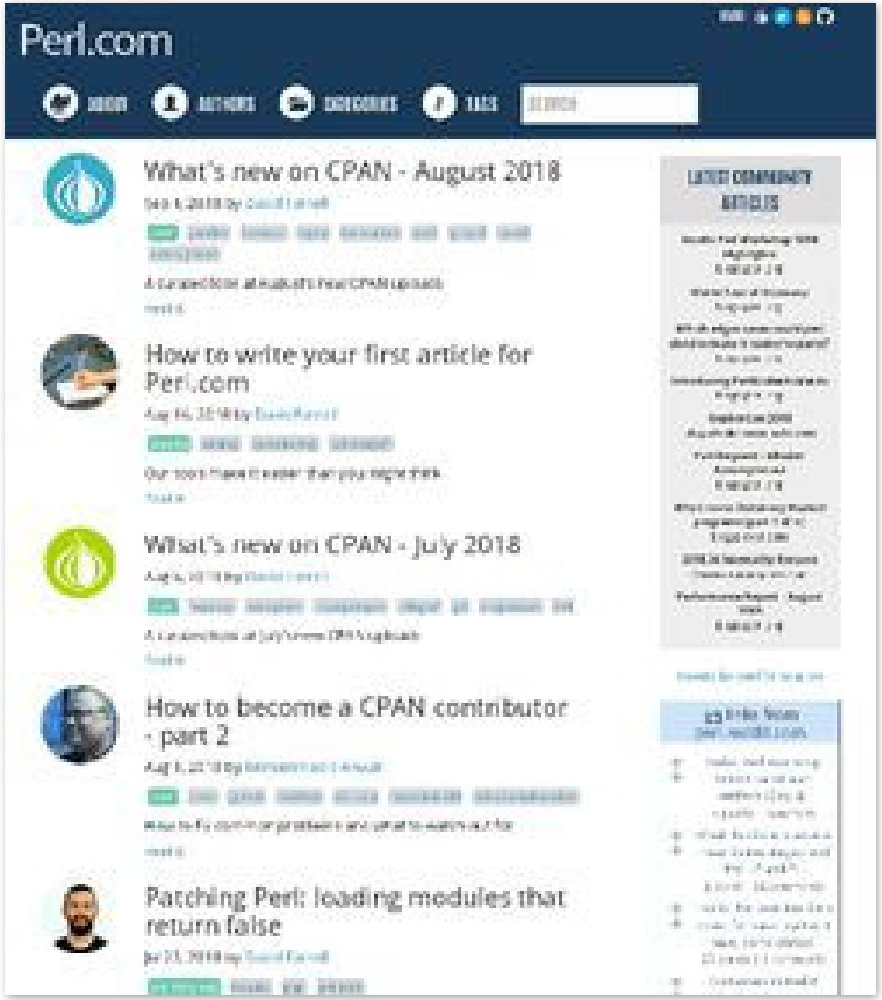
How domain hijacking was linked to C2 control



Home › News › Security › Perl.com domain stolen, now using IP address tied to malware

Perl.com domain stolen, now using IP address tied to malware

By Lawrence Abrams January 29, 2021 11:20 AM 2



What's new on CPAN - August 2018

How to write your first article for Perl.com

What's new on CPAN - July 2018

How to become a CPAN contributor - part 2

Patching Perl: loading modules that return false

- **Perl.com**: site used since 1997 to post news and articles about the Perl programming language.
- **Jan 27, 2021**: discovered that the registrar account was compromised in September 2020 (4 months prior).
- Domain was first transferred to a Chinese registrar, then to Key-Systems.

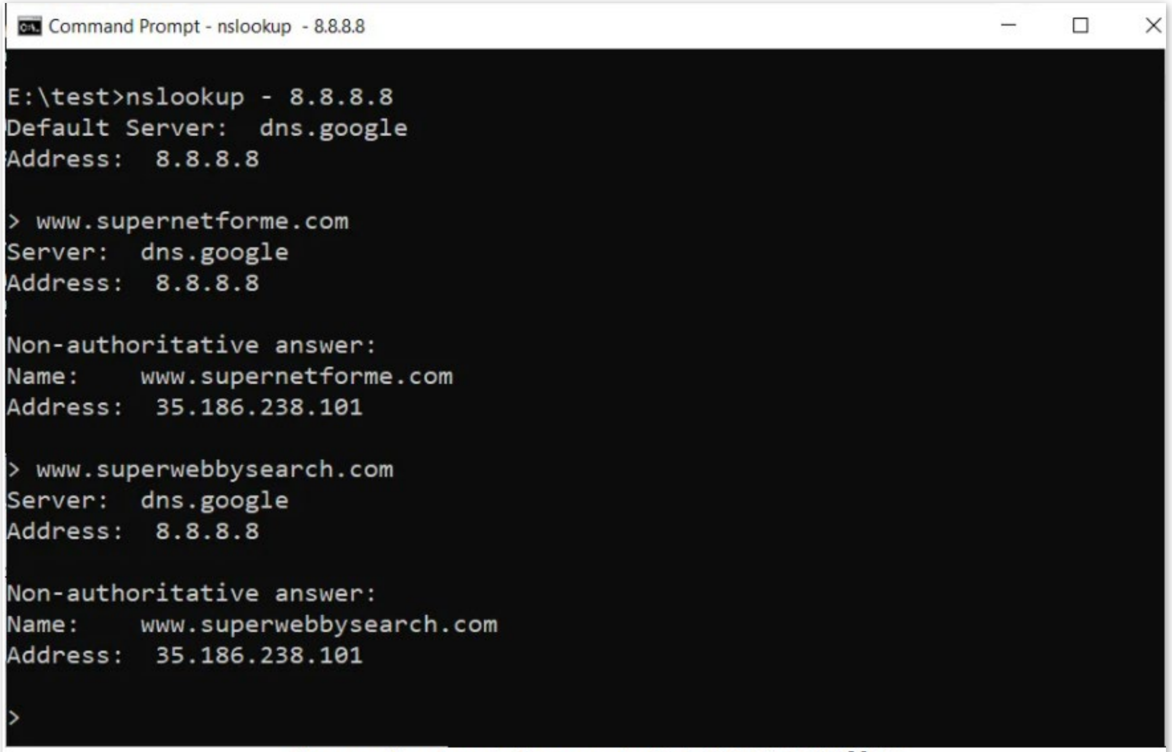
How domain hijacking was linked to C2 control

- **Not discovered earlier**: no change the NS record
- **During second ownership transfer**: IP addresses assigned to the domain were changed from 151.101.2.132 to the Google Cloud IP address 35.186.238[.]101.
- Blank page with a GoDaddy park domain script

- In 2019, the IP address 35.186.238[.]101 was tied to a domain distributing a malware executable [VirusTotal] for the now-defunct Locky ransomware.
- More recently, a malware [VirusTotal] that appears to be an ad clicker is using the following domains as command and control (C2) servers.

```
www.supernetforme[.]com
www.superwebbysearch[.]com
```

So…is there no threat???

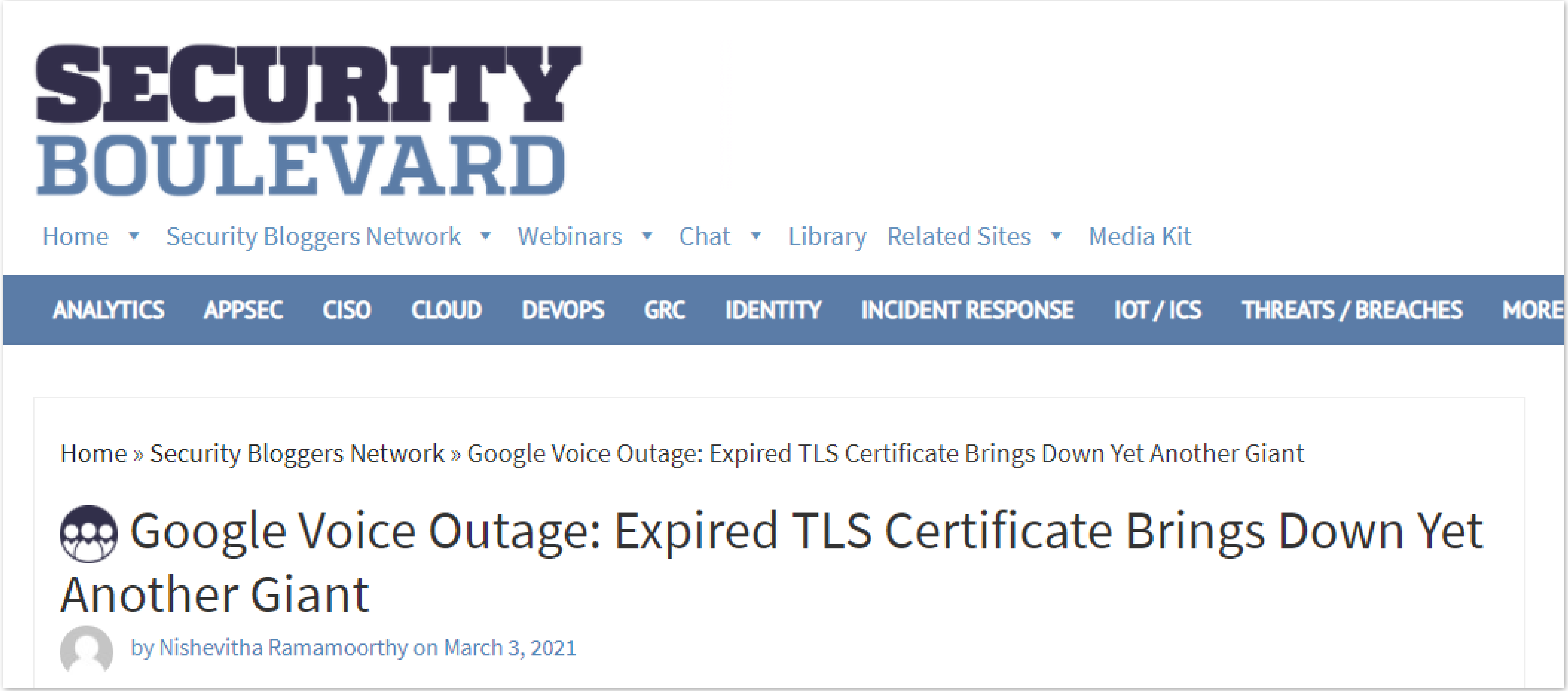


```
E:\test>nslookup - 8.8.8.8
Default Server:  dns.google
Address:  8.8.8.8

> www.supernetforme.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.supernetforme.com
Address:  35.186.238.101

> www.superwebbysearch.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.superwebbysearch.com
Address:  35.186.238.101

>
```

Command and control servers hosted at 35.186.238[.]101

What can be exposed, if maindomain.com is pointed to a C2 server?

How SSL mismanagement led to outages

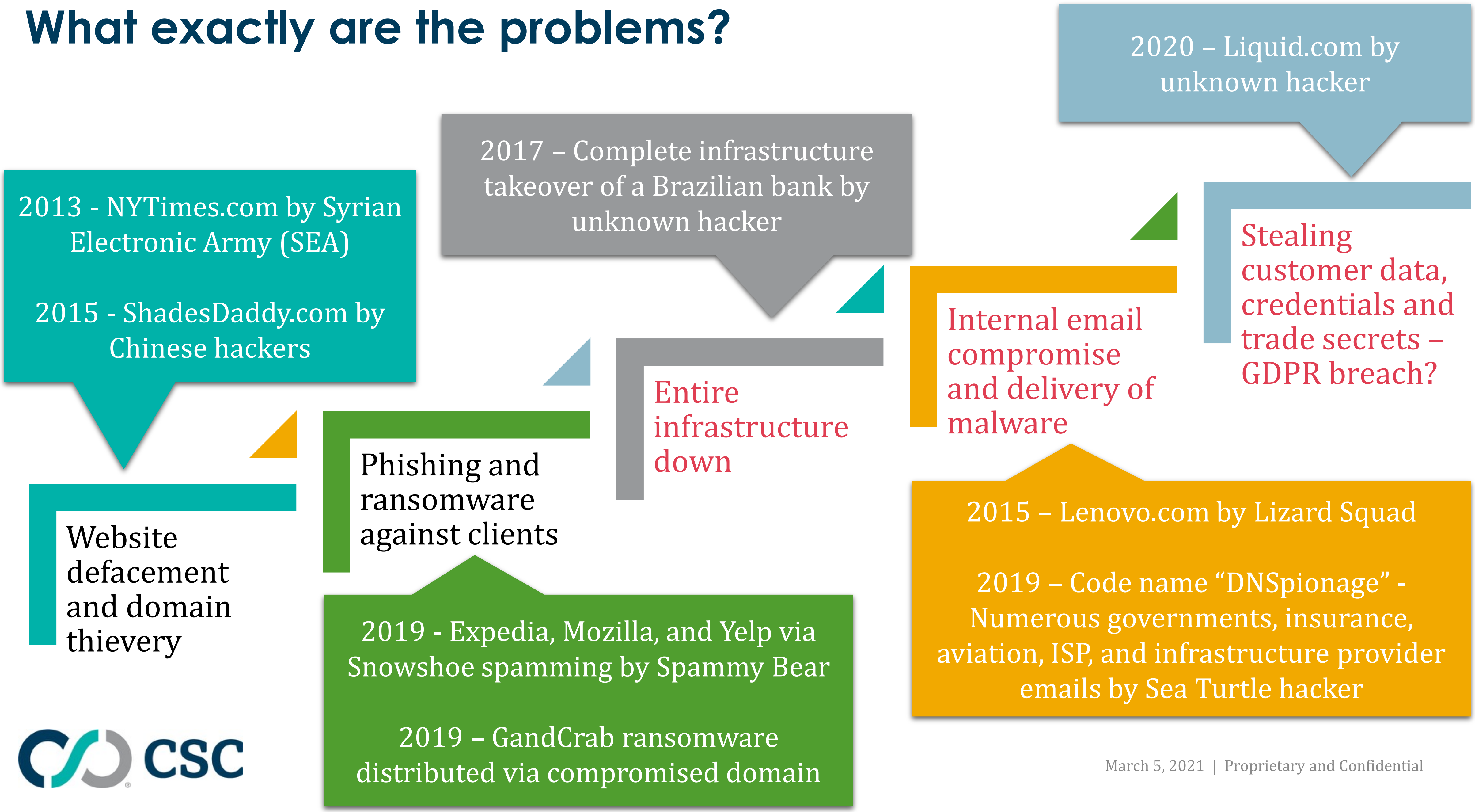


Home » Security Bloggers Network » Google Voice Outage: Expired TLS Certificate Brings Down Yet Another Giant

Google Voice Outage: Expired TLS Certificate Brings Down Yet Another Giant

by Nishevitha Ramamoorthy on March 3, 2021

What exactly are the problems?



Website defacement and domain thievery

2013 - NYTimes.com by Syrian Electronic Army (SEA)

2015 - ShadesDaddy.com by Chinese hackers

Phishing and ransomware against clients

2019 - Expedia, Mozilla, and Yelp via Snowshoe spamming by Spammy Bear

2019 – GandCrab ransomware distributed via compromised domain

Entire infrastructure down

2017 – Complete infrastructure takeover of a Brazilian bank by unknown hacker

Internal email compromise and delivery of malware

2015 – Lenovo.com by Lizard Squad

2019 – Code name “DNSpionage” - Numerous governments, insurance, aviation, ISP, and infrastructure provider emails by Sea Turtle hacker

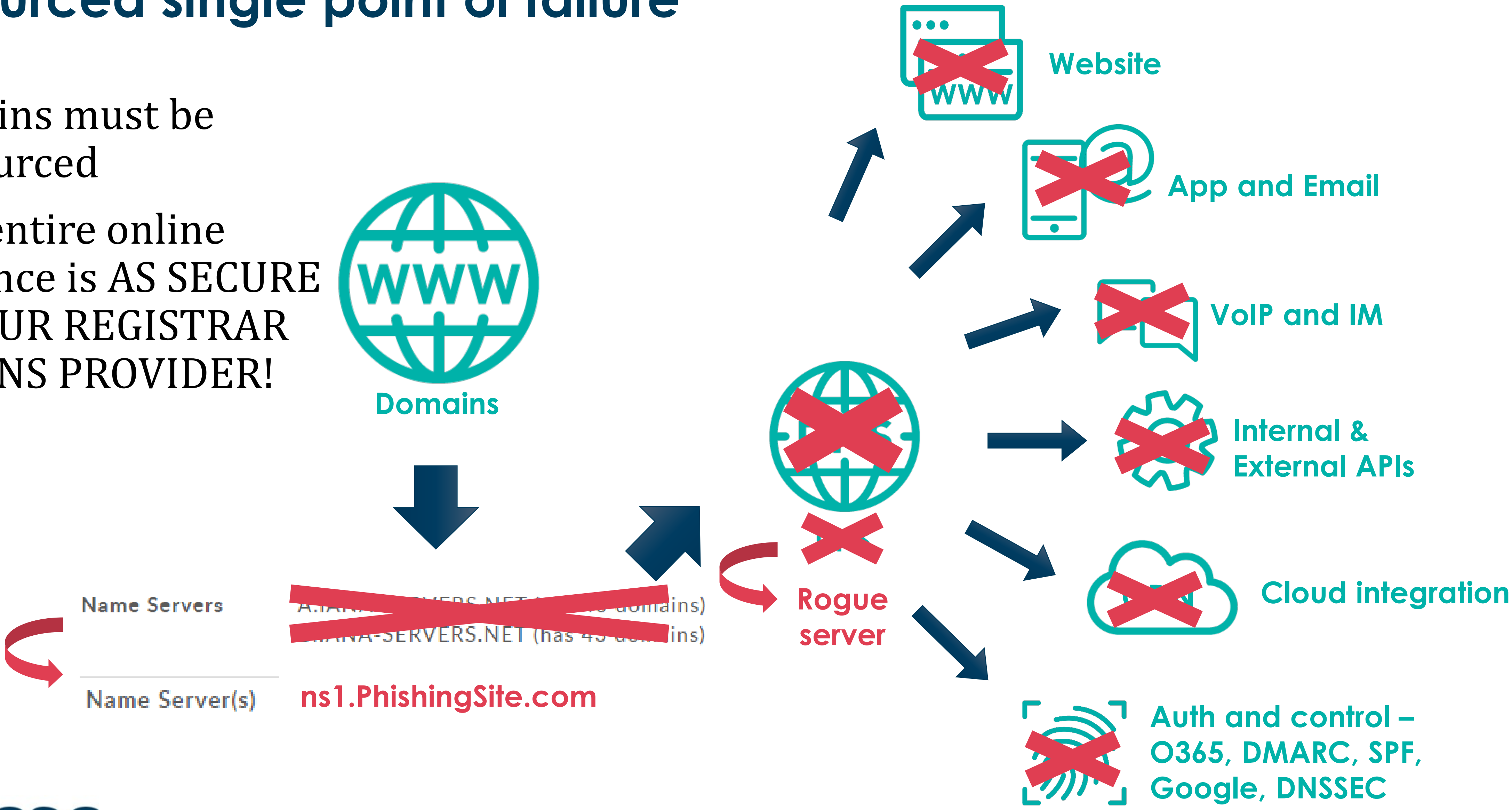
Stealing customer data, credentials and trade secrets – GDPR breach?

2020 – Liquid.com by unknown hacker

Cyber security at the inter-network level

Outsourced single point of failure

- Domains must be outsourced
- Your entire online presence is AS SECURE AS YOUR REGISTRAR and DNS PROVIDER!



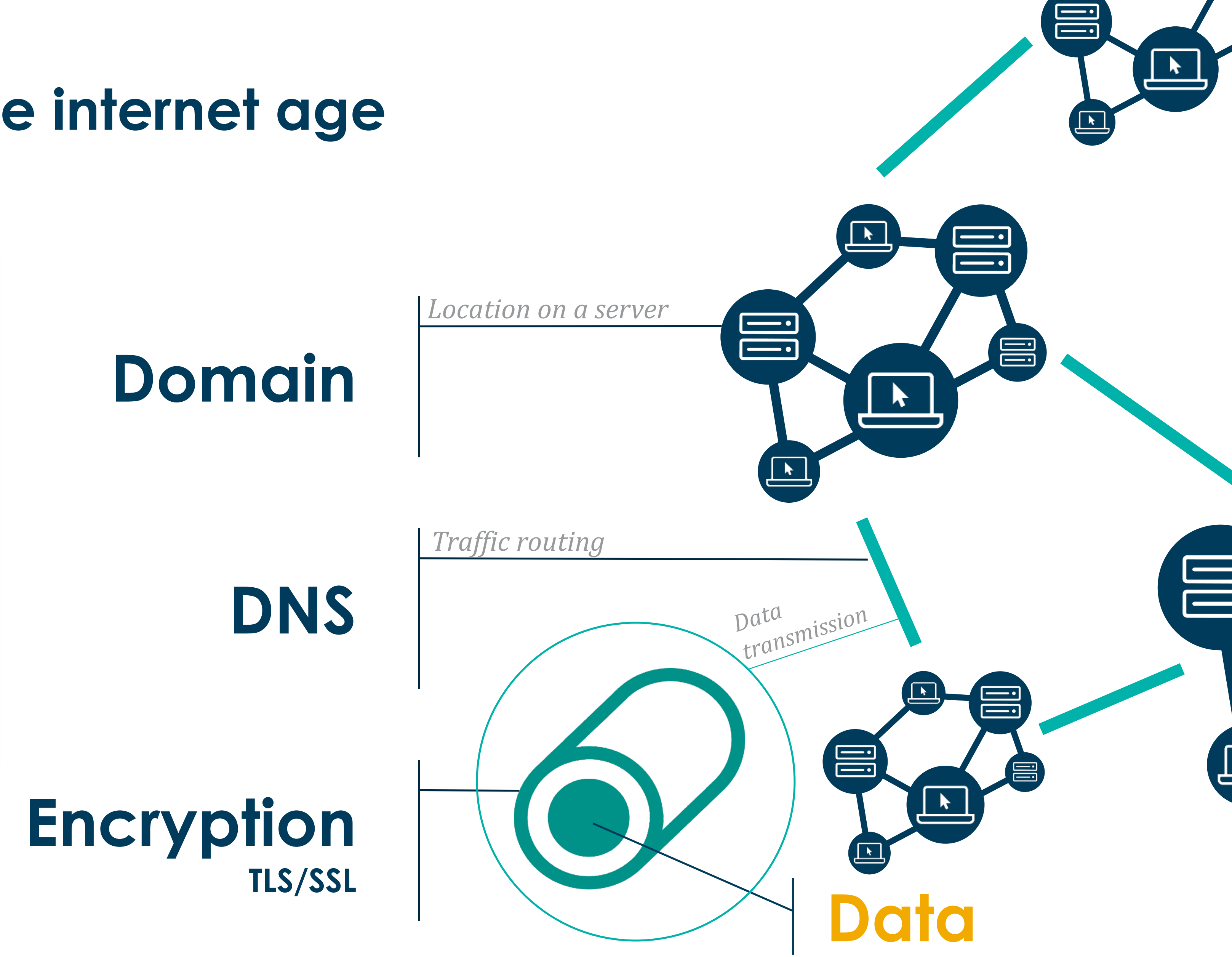
Name Servers ~~A.IANA-SERVERS.NET (has 45 domains)~~
~~B.IANA-SERVERS.NET (has 45 domains)~~

Name Server(s) ns1.PhishingSite.com

“Security maturity” in the internet age

1st Commandment:

Treat domain names as critical assets – implement registry locks and conduct 3rd party security assessments

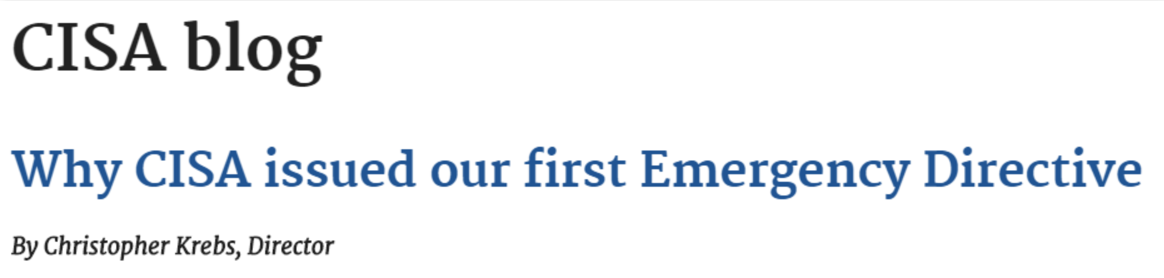


Many authorities have warned you

- **CISA** (Cybersecurity and Infrastructure Security Agency) and **DHS** (Department of Homeland Security) issued a **RARE** Emergency Directive in Jan 2019, against DNS infrastructure tampering by the Sea Turtle hacking group
- DNS is so important that they issued a 2nd warning on DNS in 2020

Who else warned you?

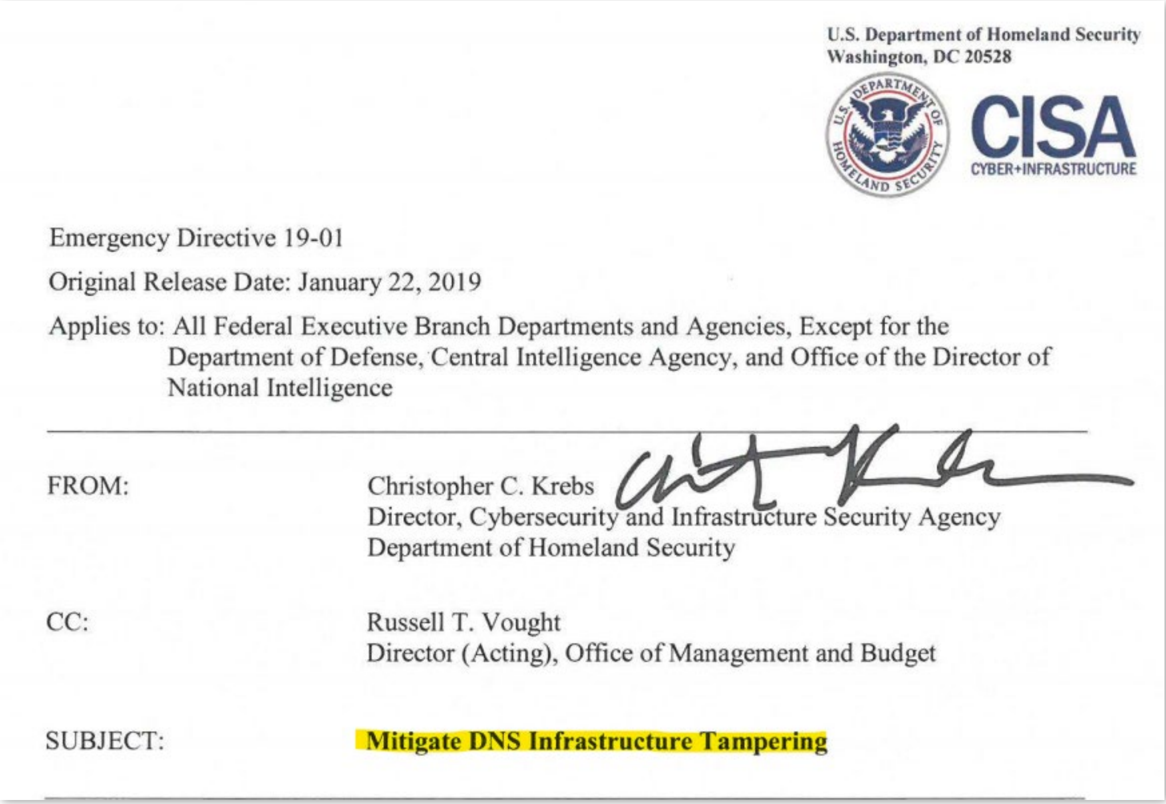
NCSC (UK), JPRS (Japan), HKIRC (HK), ICANN, FireEye, Cisco Talos, CrowdStrike, KrebsOnSecurity



CISA blog

Why CISA issued our first Emergency Directive

By Christopher Krebs, Director



U.S. Department of Homeland Security
Washington, DC 20528

CISA
CYBER+INFRASTRUCTURE

Emergency Directive 19-01

Original Release Date: January 22, 2019

Applies to: All Federal Executive Branch Departments and Agencies, Except for the Department of Defense, Central Intelligence Agency, and Office of the Director of National Intelligence

FROM: Christopher C. Krebs
Director, Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

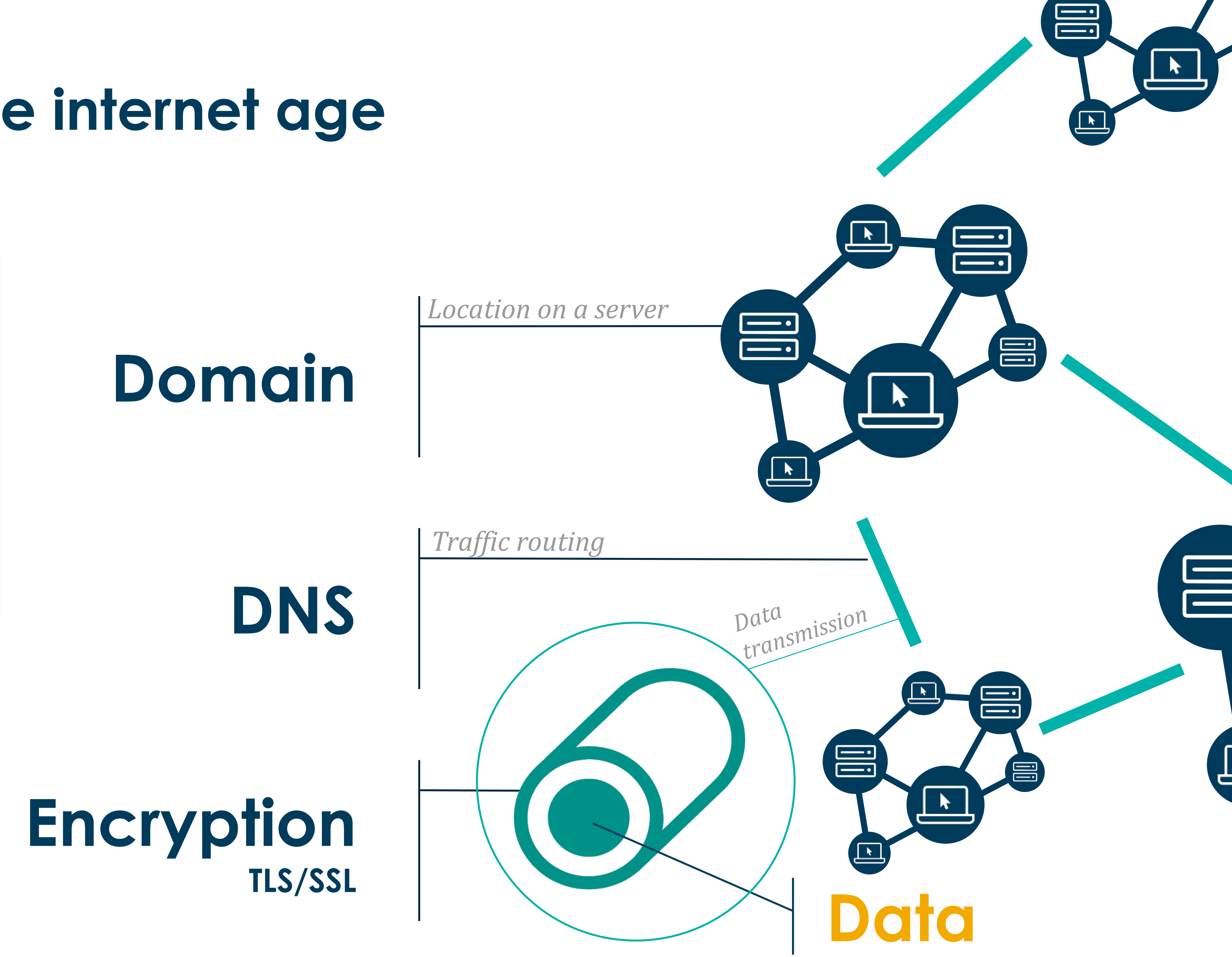
CC: Russell T. Vought
Director (Acting), Office of Management and Budget

SUBJECT: **Mitigate DNS Infrastructure Tampering**

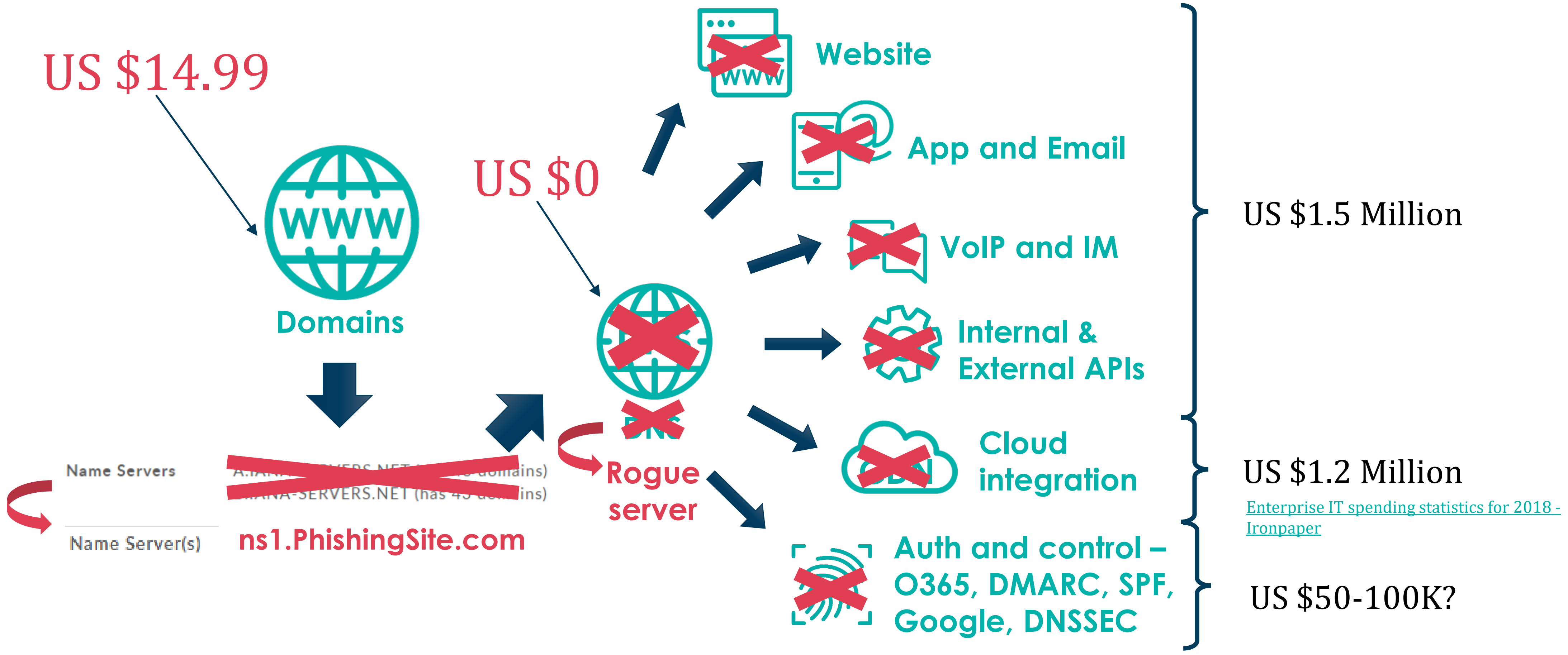
“Security maturity” in the internet age

2nd Commandment:

Avoid free and cheap DNS and implement DNSSEC



How much do you spend to protect everything?



US $14.99

Domains

Name Servers ~~A.IANA-SERVERS.NET (has 45 domains)~~
~~B.IANA-SERVERS.NET (has 45 domains)~~

Name Server(s) ns1.PhishingSite.com

US $0

DNS

Rogue server

Website

App and Email

VoIP and IM

Internal & External APIs

Cloud integration

Auth and control – O365, DMARC, SPF, Google, DNSSEC

US $1.5 Million

US $1.2 Million

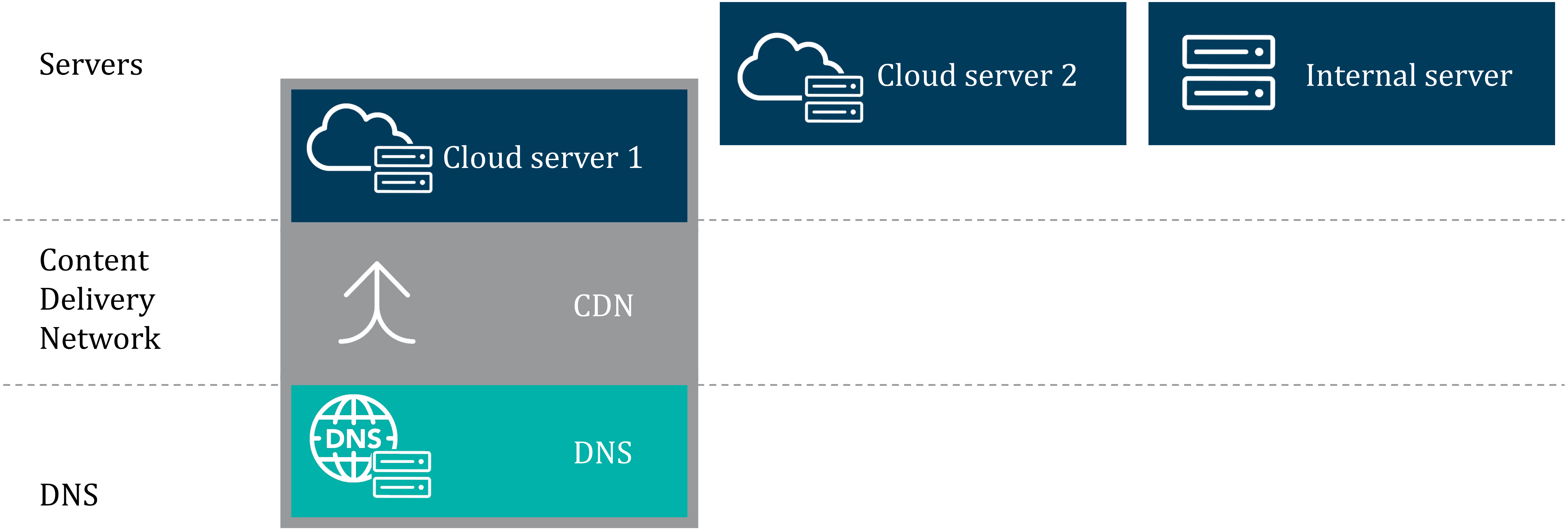
Enterprise IT spending statistics for 2018 - Ironpaper

US $50-100K?

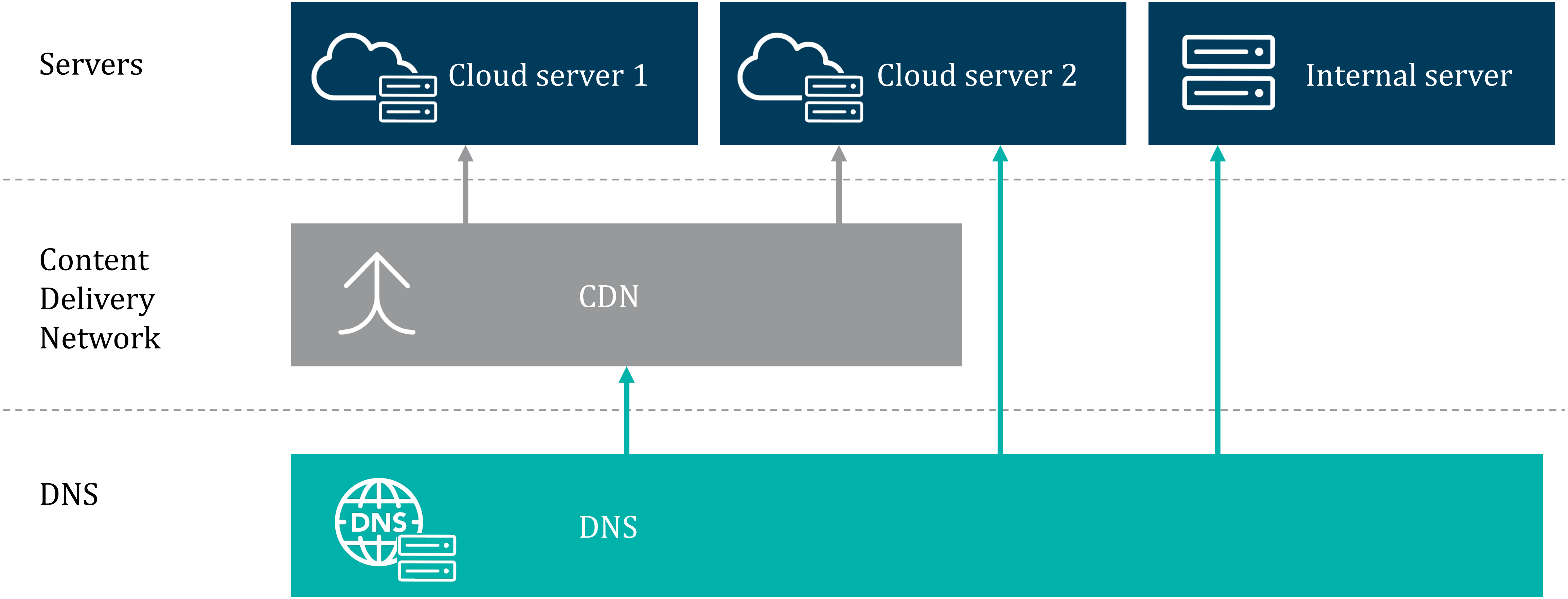
What is considered a mature enterprise DNS setup

Criteria	Why
Dedicated infrastructure	• Not a “by the way” we have DNS too – these are the free DNS • Separate DDoS defense pipe
True DDoS defence with Anycast and huge pipe	• DNS DDoS took down some CDN/clouds • The service should support DDoS scrubbing without extra cost
Don’t mix it	• Infrastructure can be a mix of in-house and cloud, or multi-cloud, while DNS must work for all • DNS should not be bounded to one cloud and must be able to have minimal interruption if changed
If you are secured, use one more.	• Use of a secondary DNS provider recommended
Support DNSSEC and GSLB on DNS	1. DNSSEC for security 2. Alias record for integration with cloud 3. DNS-based GSLB and IP failover to prevent single point of failure 4. EDNS0 Subnet to enhance intelligence for marketing
Global single network	• DNS network should be able to work as a single network to ensure global delivery (even in China)

Limitations when default DNS servers are used…



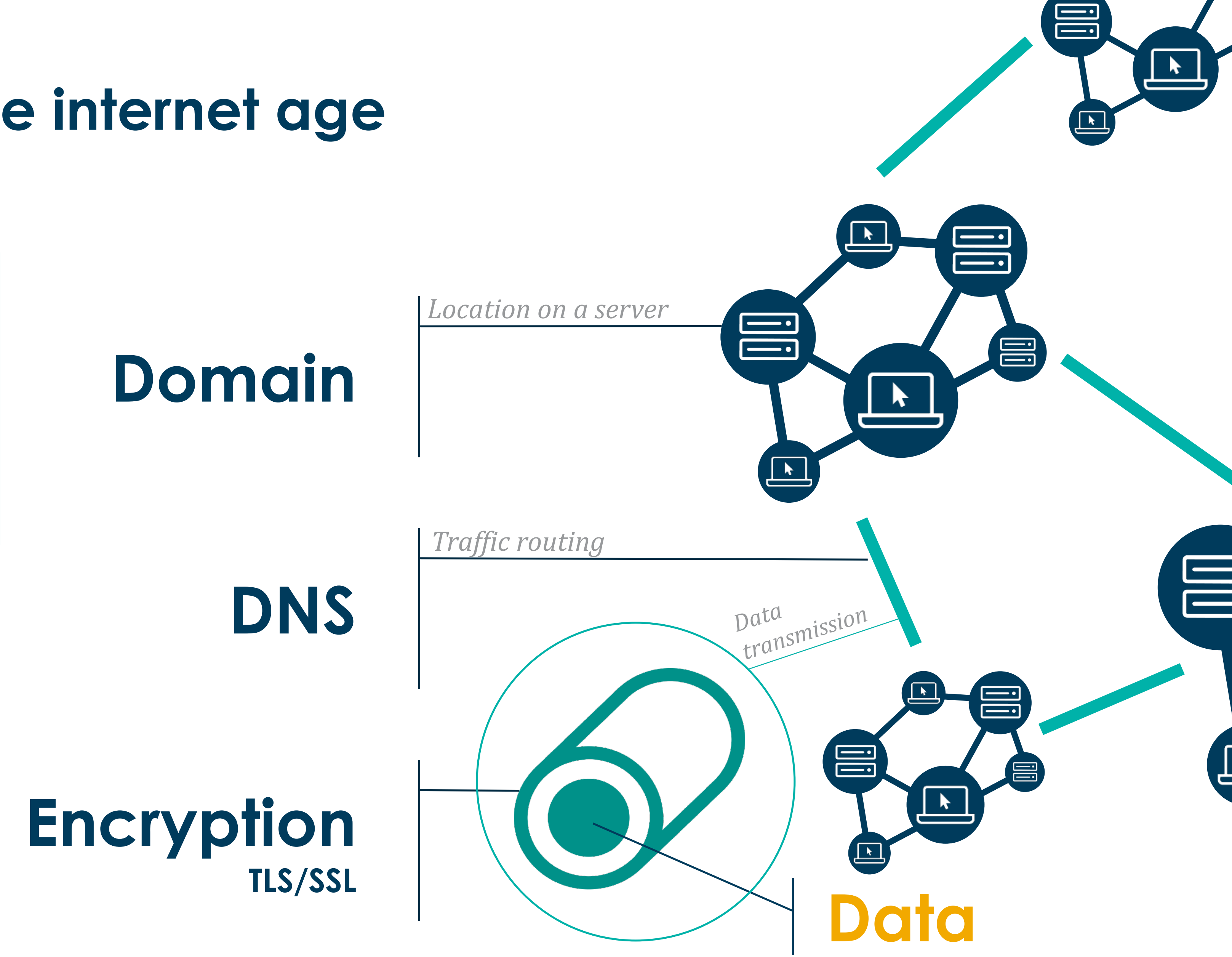
Independent setup for configurability



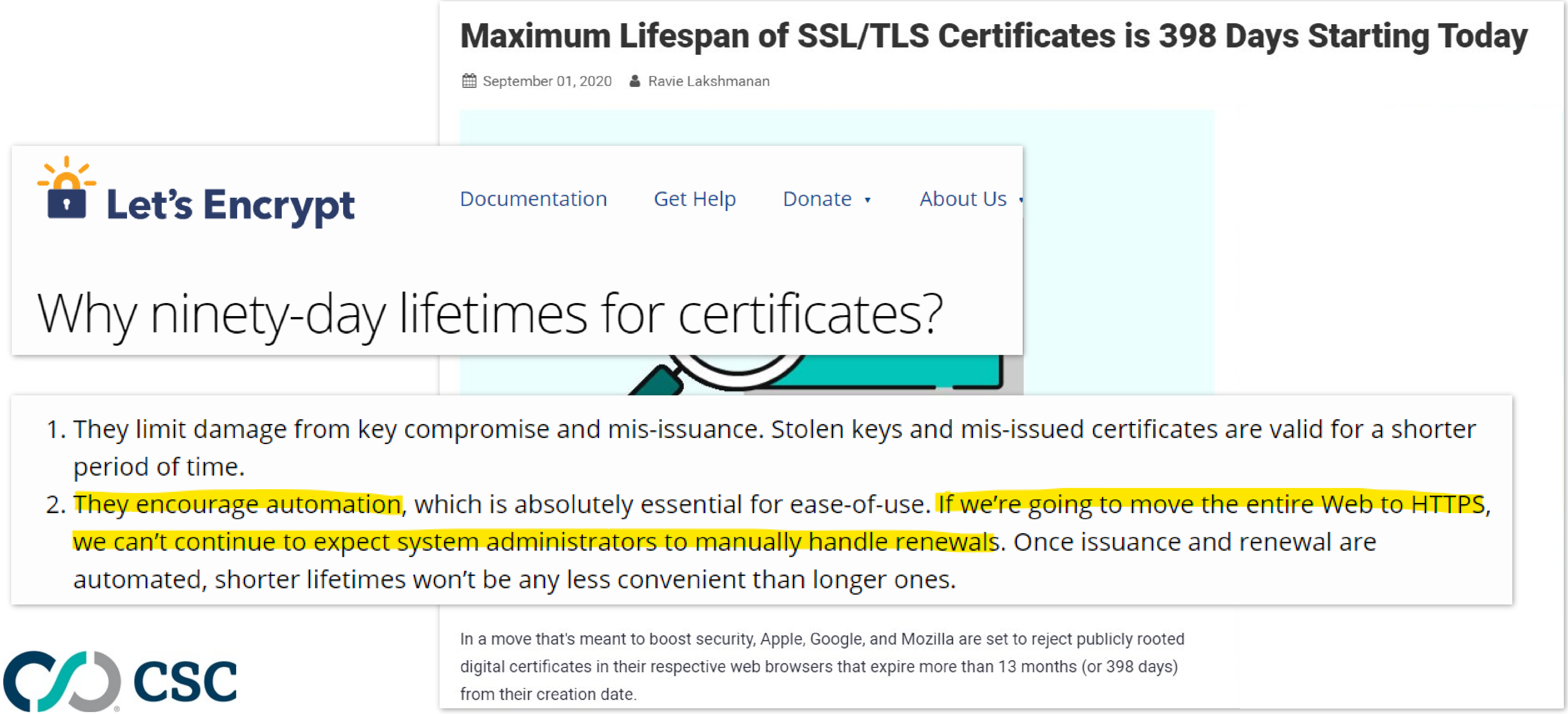
“Security maturity” in the internet age

3rd Commandment:

Automate SSL renewals



SSL/TLS certificate lifespans will get shorter



Maximum Lifespan of SSL/TLS Certificates is 398 Days Starting Today

September 01, 2020 Ravie Lakshmanan

Why ninety-day lifetimes for certificates?

1. They limit damage from key compromise and mis-issuance. Stolen keys and mis-issued certificates are valid for a shorter period of time.
2. They encourage automation, which is absolutely essential for ease-of-use. If we're going to move the entire Web to HTTPS, we can't continue to expect system administrators to manually handle renewals. Once issuance and renewal are automated, shorter lifetimes won't be any less convenient than longer ones.

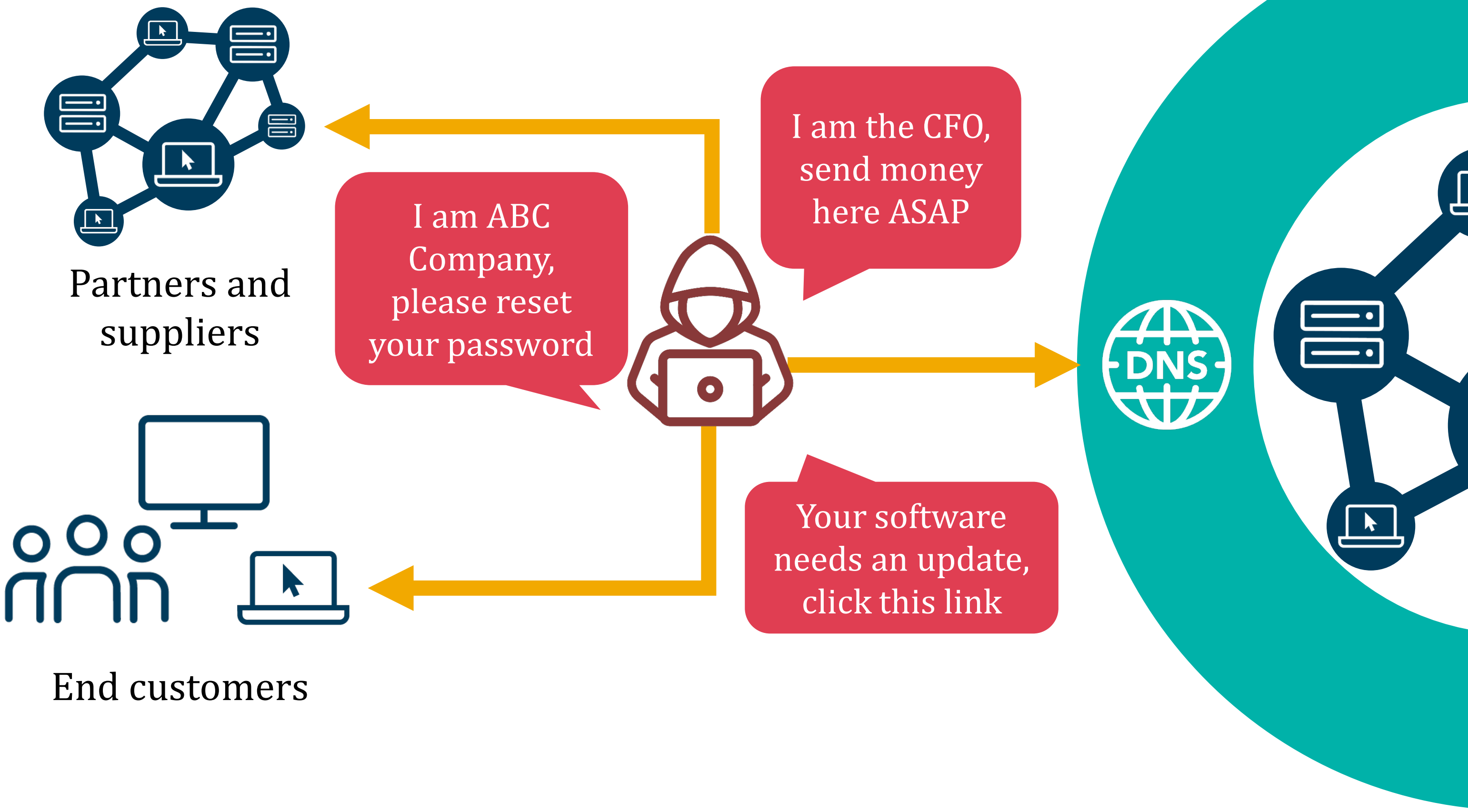
In a move that's meant to boost security, Apple, Google, and Mozilla are set to reject publicly rooted digital certificates in their respective web browsers that expire more than 13 months (or 398 days) from their creation date.

“Security maturity” in the internet age

4th Commandment:

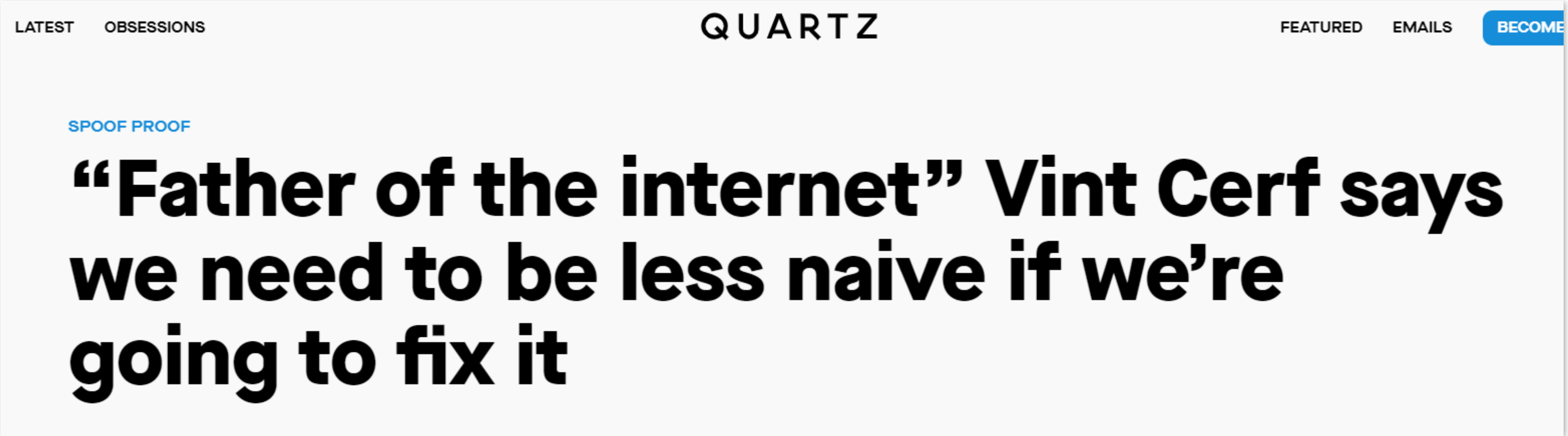
Spoof-proofing not only yourself but also **your customers:**

1. DNSSEC
2. DNS Abuse –
   Anti-phishing for your clients



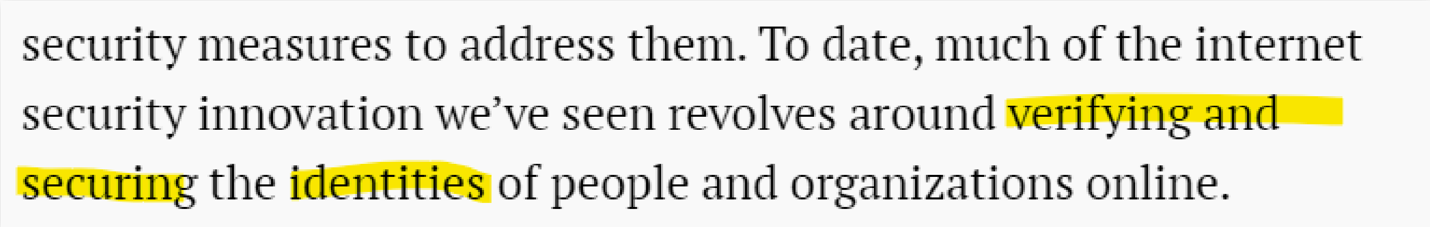
Partners and suppliers
I am the CFO, send money here ASAP
I am ABC Company, please reset your password
DNS
Your software needs an update, click this link
End customers

Recommended by Vint Cerf



SPOOF PROOF

"Father of the internet" Vint Cerf says we need to be less naive if we're going to fix it



security measures to address them. To date, much of the internet security innovation we've seen revolves around verifying and securing the identities of people and organizations online.

Spoof-proofing the web

DNS is not sexy

Most consider domains, DNS, and SSL low level

Not a Zero-Day attack

It’s so foundational, so NO excuses!

CSC

Questions?

Alban Kwan

✉ alban.kwan@cscglobal.com

in linkedin.com/in/albankwan/

www cscdbs.com

in CSC Digital Brand Services

@cscdbs