TRUSTED
INTERNET

Once you're connected, you're protected.(R)

Who is this guy? Why should we put our phones away?

Mr. Stutzman is a cyber security expert with over 30 years of experience. He oversees information security operations and Virtual Chief Information Security Officers protecting several high net worth families, and small and medium sized companies. He personally serves as the Virtual Chief Information Security Officer for a Manhattan based Private Equity firm, a $3.5bn Oil and Gas, and for the US and LATAM risk operations for a 600,000-employee diversified services company.

Past positions include:

- **Chief Intelligence Officer –** Wapack Labs, Cyber Threat Intelligence
- **DCISE Director - GS15** at DoD Cyber Crime Center
- **Principal Engineer**, Carnegie Mellon, Software Engineering Institute
- **Chief Information Security Officer** Northrop Grumman Electronics
- **Chief, Cyber Threat Intelligence and Analysis** Northrop Grumman Corporate
- Cisco Systems, **Sr. Manager Global IT Risk Management**
- **Navy Intelligence Officer**, Information Warfare (cyber)

Built and ran DoD/DIB Information Sharing and Analysis Environment

Built and ran Northrop Grumman's anti-cyber espionage team (to chase Chinese spies out of Northrop Grumman's Global Networks).

- Awarded Presidents Award for IT Innovation, 2008
- Information Security Program of the year.

Built and ran Cisco's global IT Risk Management practice. Authored risk and integration for Cisco's M&A processes.

Founding member: Honeynet Project (the home to many of today's current security tools.

Certified Information System Security Professional (2002 – Pres), BS Excelsior College, MBA Worcester Polytechnic Institute, Senior Executive Fellow, Harvard Kennedy School

TRUSTED INTERNET

Who is Trusted Internet?

- Cyber Security Monitoring Company
- Think “ADT” for your computers

Global Tracking & Emergency Response

Personal Protection & Transportation

Travel & Real-Time Intelligence

Real-Time Medical Care & Case Management

Emergency Aviation & Evacuation

Cyber Security

4 days

Why is this important? You’ll see.

18 months ago a company’s IT personnel noticed an ‘anomaly’ in datacenters in the Middle East and Asia.

Two hours later, over 1000 servers had been encrypted, crippling the company and its ability to communicate.

Dead in the water…

Backup systems and data were encrypted.

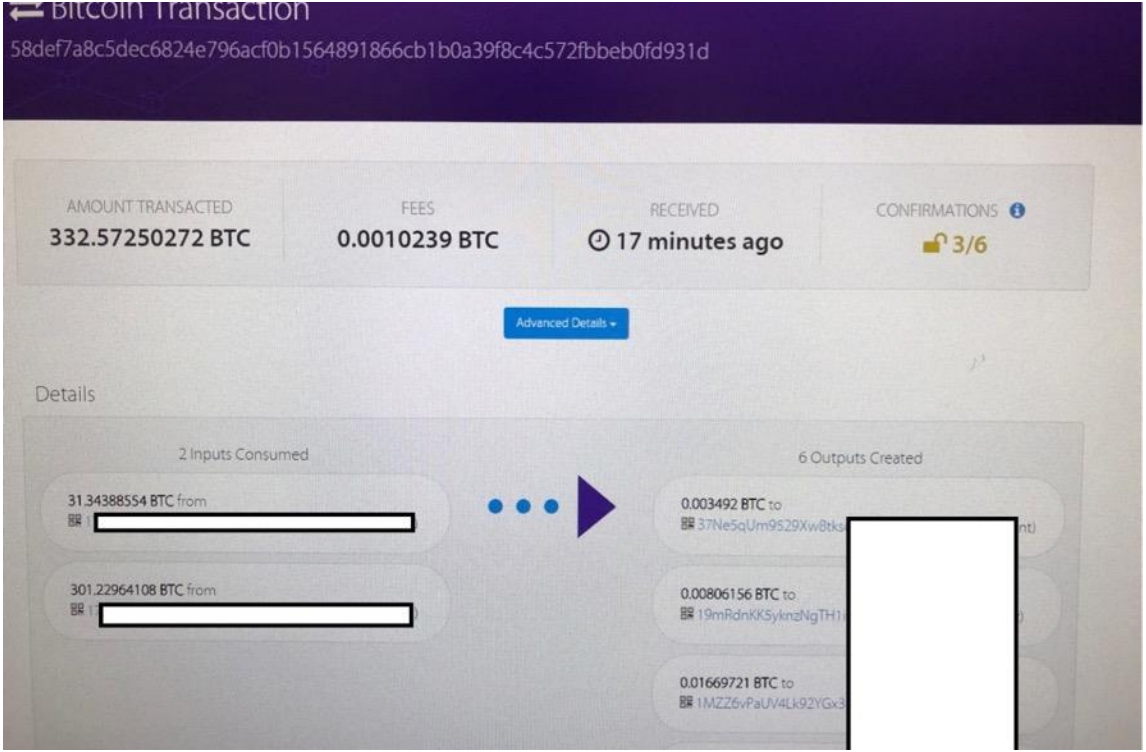
Had no communications;

Had no idea of the true extent of the damage.

They were losing approximately $25 mil per day.

They were facing an extinction event and had run out of hope.

This is what a $100,000 Bitcoin transaction looks like.



58def7a8c5dec6824e796acf0b1564891866cb1b0a39f8c4c572fbbeb0fd931d

AMOUNT TRANSACTED	FEES	RECEIVED	CONFIRMATIONS
332.57250272 BTC	0.0010239 BTC	17 minutes ago	3/6

Details

2 Inputs Consumed

31.34388554 BTC from
[redacted]

301.22964108 BTC from
[redacted]

6 Outputs Created

0.003492 BTC to
37Ne5qUm9S29Xw8tks [redacted]

0.00806156 BTC to
19mRdnKKSyknzNgTH1

0.01669721 BTC to
1MZZ6vPaUV4Lk92YGx3

Incident

Day 1

First Detection
IT Team unable to contain

- Polymorphic
- Reboots halted computers
- Spread through backup system

Day 2-3

Day 2 - Extent of damage and scope of attack still unknown

Day 4-6

Day 4 – Trusted Internet engaged
- Board notified.
- FBI Notified.
- Ransom paid.

10:00 PM EST – Decryptor received; first tests performed successfully

Day 5 – Priority of Restoration

Day 6 – Decryption and restoration of services in full swing.

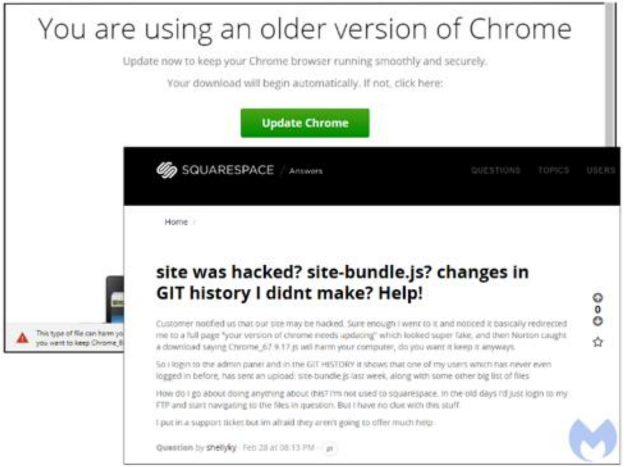
Day 7+

Day 7 – Decryptor operations validated

June – October - recovery

Here’s how it all started:
They came through the front door…

- An authorized user mistakenly believed a “software update” was legitimate
- Visited a compromised website,and was subsequently infected with the malware.
- The infection spread through the backup system.



You are using an older version of Chrome

Update now to keep your Chrome browser running smoothly and securely.

Your download will begin automatically. If not, click here:

site was hacked? site-bundle.js? changes in GIT history I didnt make? Help!

Customer notified us that our site may be hacked. Sure enough I went to it and noticed it basically redirected me to a full page "your version of chrome needs updating" which looked super fake, and then Norton caught a download saying Chrome_67.9.17.js will harm your computer, do you want it keep it anyways.

So i login to the admin panel and in the GIT HISTORY it shows that one of my users which has never even logged in before, has sent an upload: site-bundle.js last week, along with some other big list of files

How do I go about doing anything about this? I'm not used to squarespace. In the old days I'd just login to my FTP and start navigating to the files in question. But I have no clue with this stuff

I put in a support ticket but im afraid they aren't going to offer much help.

Question by shellyky · Feb 28 at 08:13 PM

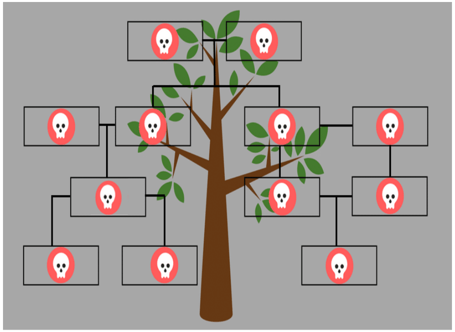
FakeUpdates Malware Campaign

Malware: Dridex, Bitpaymer and PowerShell Empire

- Dridex – Steal credentials.
  - Installed by botnet
  - Steals credentials

- Bitpaymer - Ramsomware
  - Inserted using stolen credentials
  - Encrypts systems

- PowerShell Empire – Uses Windows tools to move around
  - Post exploitation framework used to run modules
  - Used to download Bitpaymer



Two hours later, the company was crippled, operations halted worldwide.

Immediate Actions to Enhance & Harden IT Protections – First 24 hours after decrypt

- Deployed endpoint protection to all endpoints
- Global Password Reset on all privileged accounts
- Imposed restrictions
  - Social media, Cloud storage applications, etc.
  - USB devices

Immediate Actions to Enhance & Harden IT Protections

- Baseline hardening completed
- Retained third party security operations center to monitor global network
- Added over 25,000 pieces of intelligence to current defenses
- Implemented additional advanced security tools to further harden the environment
- Penetration tested

Lessons Learned

- Seconds count
- This can happen to anyone
- Be ready
- These won’t be stopped, but can be managed

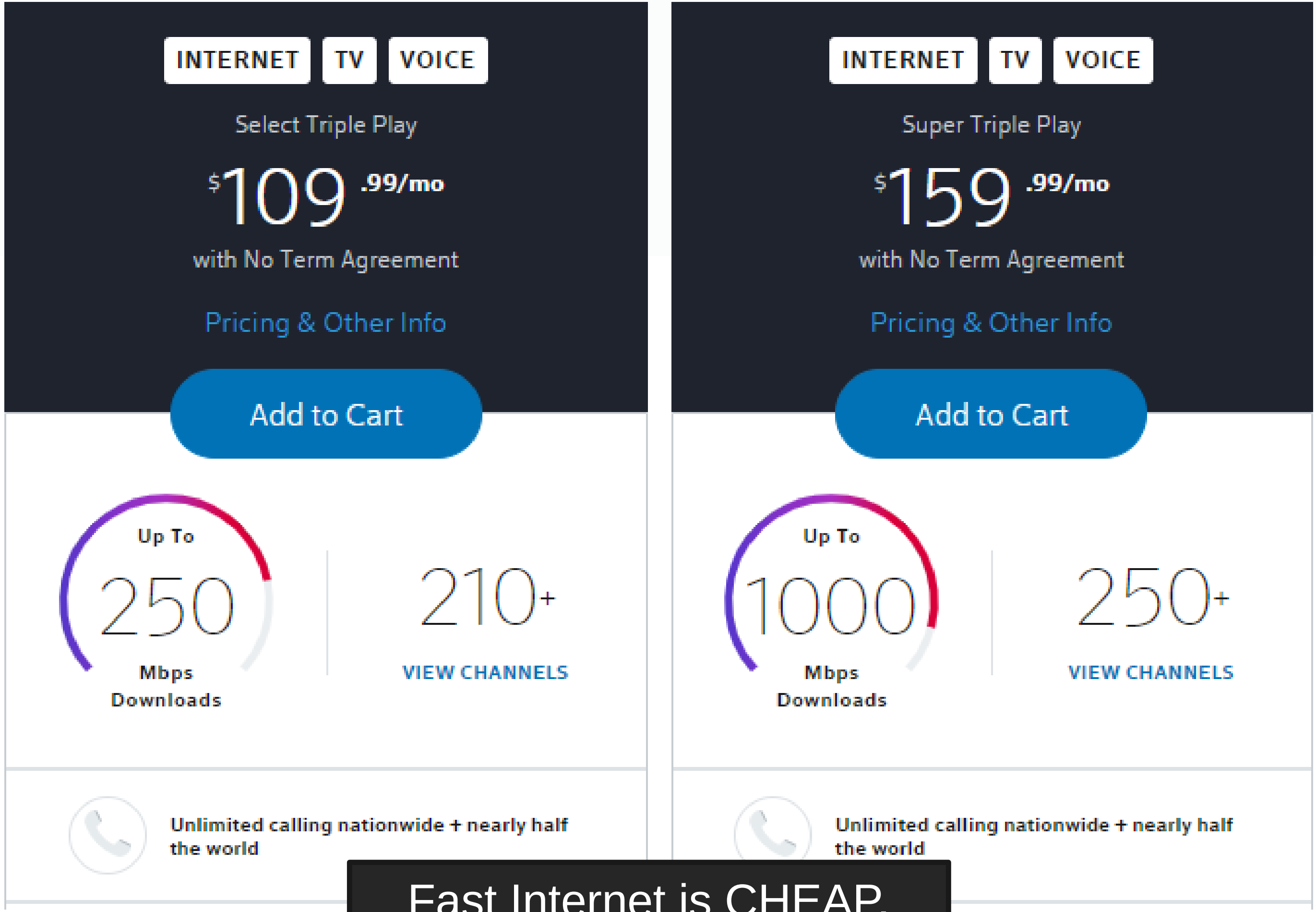
4 days

Why is this important?

- Four days was the amount of time that the IT team tried to fix it on their own.
  - before the CEO told the board
  - before the CEO even KNEW that his systems were being held for ransom.
- At a cost of approximately $25 mil per day in losses, $700K in bitcoin, $4 mil in remediation

Is this your IT?

Things to consider...



INTERNET TV VOICE

Select Triple Play

$109.99/mo

with No Term Agreement

Pricing & Other Info

Add to Cart

Up To 250 Mbps Downloads

210+ VIEW CHANNELS

☎ Unlimited calling nationwide + nearly half the world

INTERNET TV VOICE

Super Triple Play

$159.99/mo

with No Term Agreement

Pricing & Other Info

Add to Cart

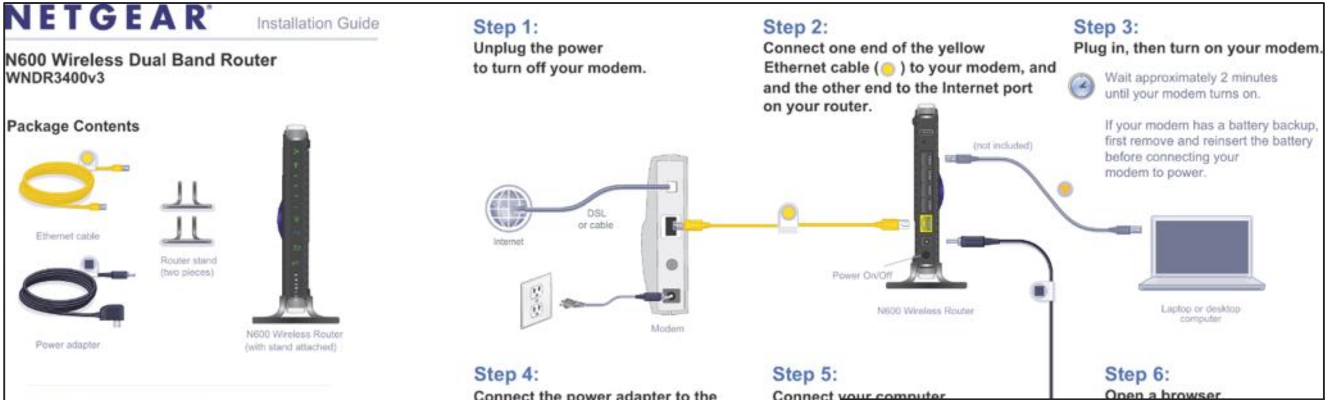
Up To 1000 Mbps Downloads

250+ VIEW CHANNELS

☎ Unlimited calling nationwide + nearly half the world

Fast Internet is CHEAP.

The instructions don't mention firewalls (or any security for that matter)



NETGEAR Installation Guide

N600 Wireless Dual Band Router
WNDR3400v3

Package Contents

Ethernet cable
Router stand (two pieces)
Power adapter
N600 Wireless Router (with stand attached)

Attach the stand to the router:

1. Position the router so that the Power button is at the bottom and the USB

Step 1:
Unplug the power to turn off your modem.

Step 2:
Connect one end of the yellow Ethernet cable (●) to your modem, and and the other end to the Internet port on your router.

Step 3:
Plug in, then turn on your modem.

Wait approximately 2 minutes until your modem turns on.

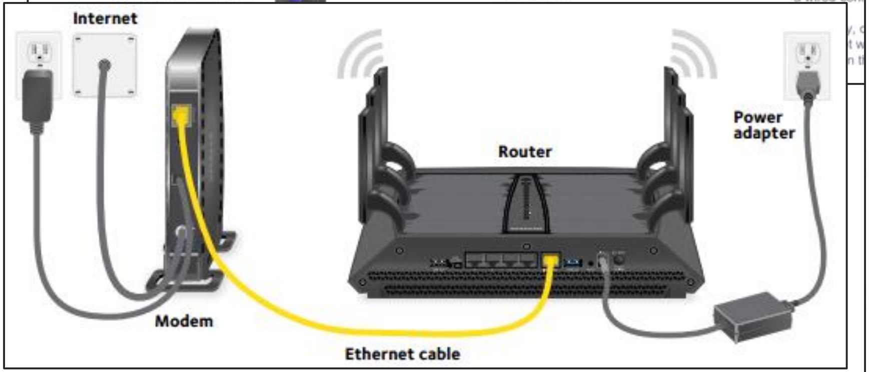
If your modem has a battery backup, first remove and reinsert the battery before connecting your modem to power.

Step 4:
Connect the power adapter to the router, then plug it into an outlet. Wait for the 2.4 GHz LED (2.4) to turn on.

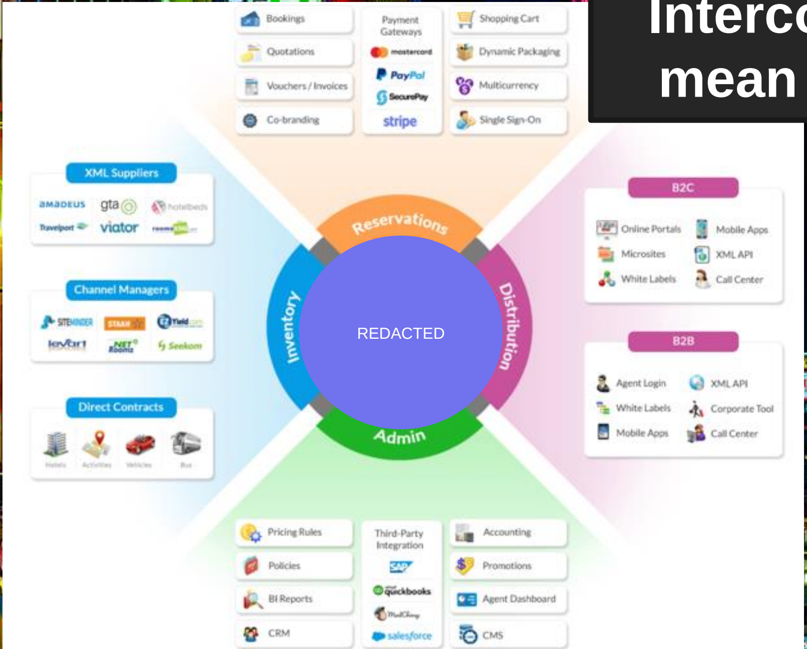
Step 5:
Connect your computer to the rou

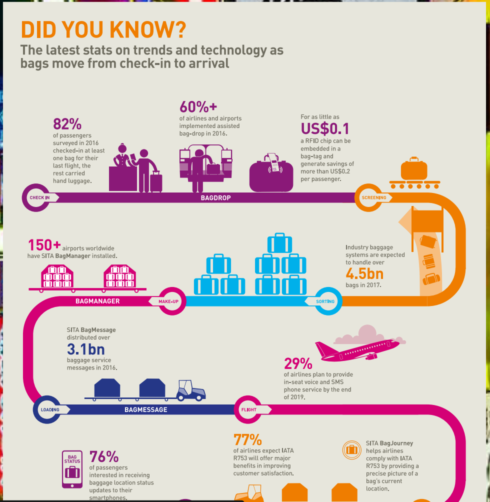
Use another
a wired conn

Step 6:
Open a browser



Interconnectedness could mean massive insecurity.





DID YOU KNOW?

The latest stats on trends and technology as bags move from check-in to arrival

82% of passengers surveyed in 2016 checked-in at least one bag for their last flight, the rest carried hand luggage.

60%+ of airlines and airports implemented assisted bag-drop in 2016.

For as little as **US$0.1** a RFID chip can be embedded in a bag-tag and generate savings of more than US$0.2 per passenger.

150+ airports worldwide have SITA **BagManager** installed.

Industry baggage systems are expected to handle over **4.5bn** bags in 2017.

SITA **BagMessage** distributed over **3.1bn** baggage service messages in 2016.

29% of airlines plan to provide in-seat voice and SMS phone service by the end of 2019.

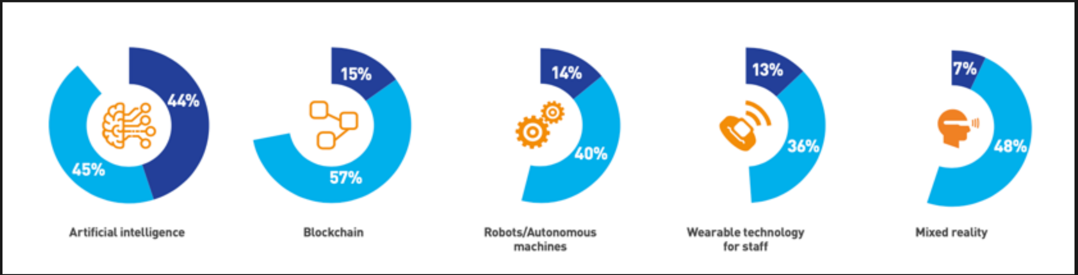
76% of passengers interested in receiving baggage location status updates to their smartphones.

77% of airlines expect IATA R753 will offer major benefits in improving customer satisfaction.

SITA **BagJourney** helps airlines comply with IATA R753 by providing a precise picture of a bag's current location.

47% of mishandled bags occurred during transfer in 2016.

RFID can potentially save the industry more than **US$3bn** over the next seven years by helping to reduce mishandling during transfers.

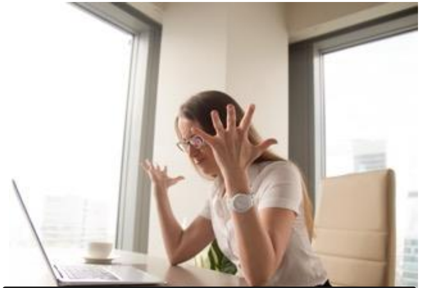


Artificial intelligence (AI) continues to be a focal point for airline investment. AI has become the most common technology that airlines are currently investing in: 44% have a major program (up from 32%) and a further 45% are running a pilot. (SOURCE: SITA)

Targets?

Things you may not have considered…

Mobiles



Executives

The unsuspecting

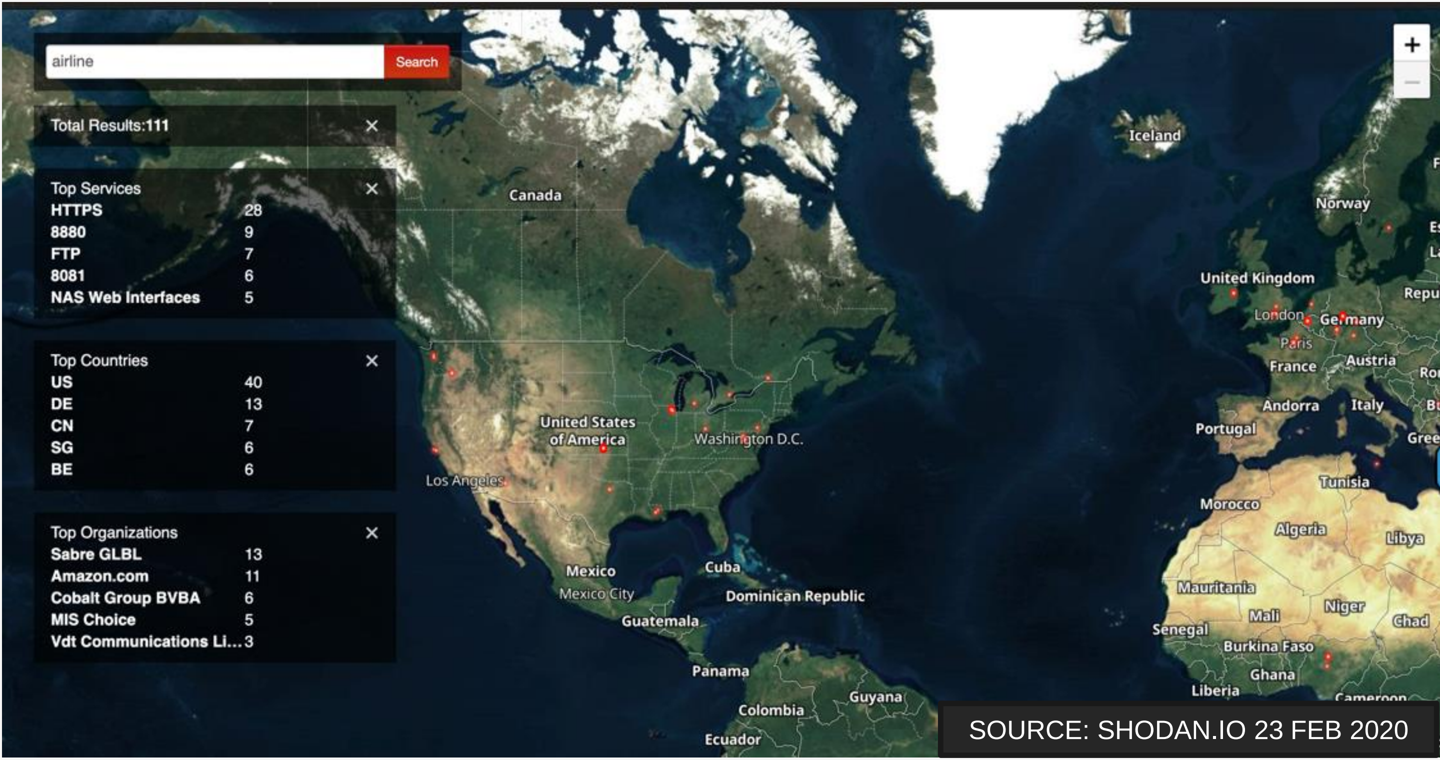
OWASP TOP 10
VULNERABILITIES
INJECTION
SECURITY MISCONFIGURATION
BROKEN AUTHENTICATION
CROSS-SITE SCRIPTING (XSS)
SENSITIVE DATA EXPOSURE
INSECURE DESERIALIZATION
XML EXTERNAL ENTITIES (XXE)
USING COMPONENTS WITH KNOWN VULNERABILITIES

Cloud and SaaS

Physical Security Systems

Everything leaks

No matter how good you are, or how hard you try…



Total Results:111

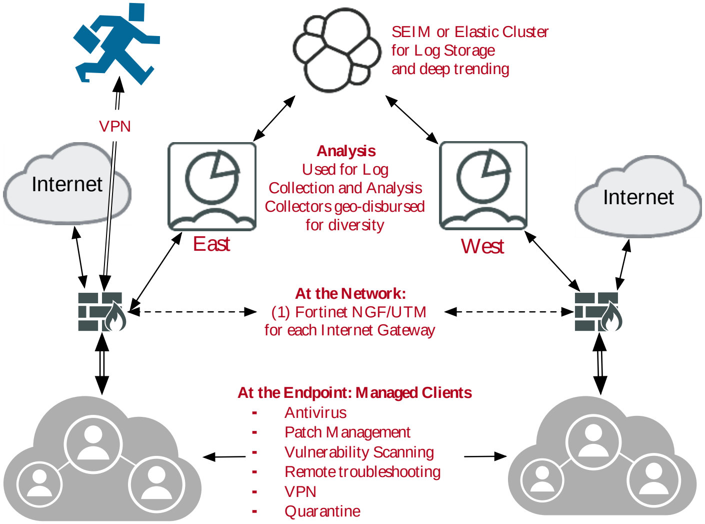
Top Services	
HTTPS	28
8880	9
FTP	7
8081	6
NAS Web Interfaces	5

Top Countries	
US	40
DE	13
CN	7
SG	6
BE	6

Top Organizations	
Sabre GLBL	13
Amazon.com	11
Cobalt Group BVBA	6
MIS Choice	5
Vdt Communications Li…	3

SOURCE: SHODAN.IO 23 FEB 2020

This is what good networking should look like.
(It’s not as hard as it looks)



SEIM or Elastic Cluster
for Log Storage
and deep trending

Analysis
Used for Log
Collection and Analysis
Collectors geo-disbursed
for diversity

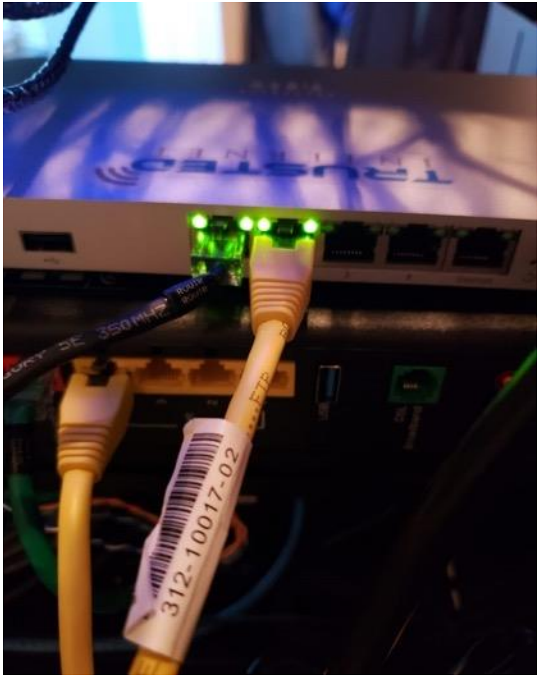
At the Network:
(1) Fortinet NGF/UTM
for each Internet Gateway

At the Endpoint: Managed Clients
- Antivirus
- Patch Management
- Vulnerability Scanning
- Remote troubleshooting
- VPN
- Quarantine

- Common sense architecture
- Easily implemented, easily monitored.
- Low cost high payoff security infrastructure.
- Gets you compliant quickly with many of your government technical compliance requirements.

Here’s what we use:

- Sophos or FortiNet Anti-virus
- Cisco Meraki Firewall (homes, execs, small business)
- FortiGate Firewall (business)



THANK YOU

Jeff Stutzman, CISSP

Founder & Chief Information Security Officer