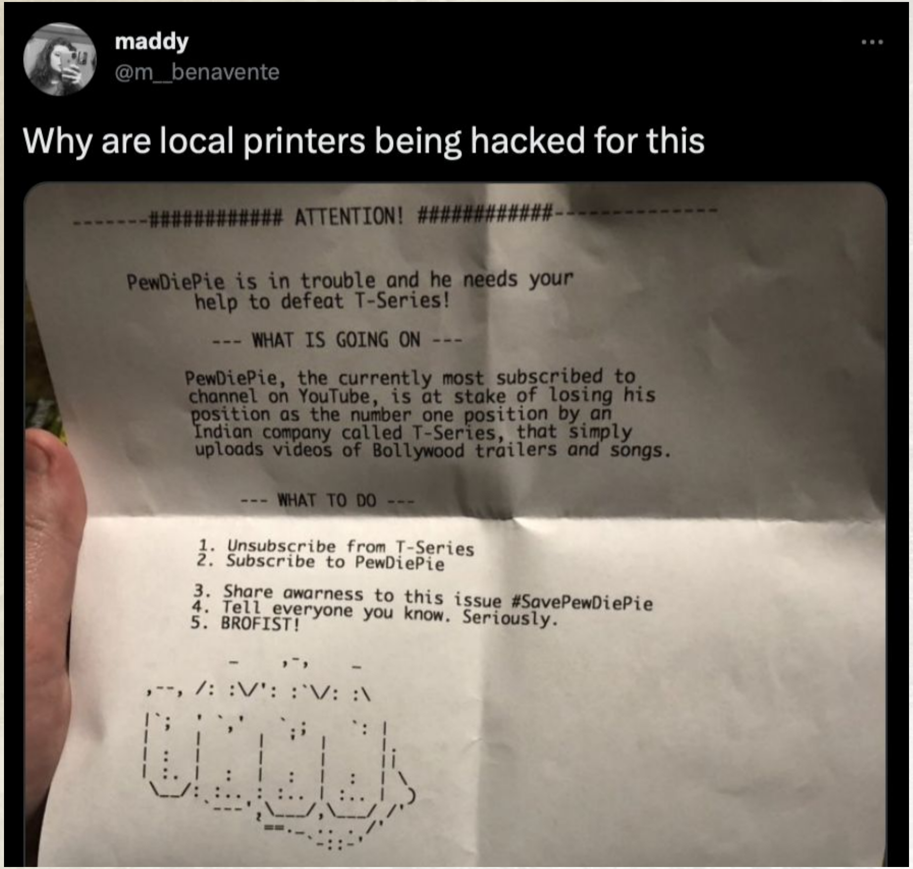
Censys :
A Search Engine Backed by Internet-Wide Scanning

Authors : Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, J. Alex Halderman

Presented by : Deepak Gouda

2nd Feb, 2023

Georgia Tech



maddy
@m__benavente

Why are local printers being hacked for this

-------############ ATTENTION! ############-------------

PewDiePie is in trouble and he needs your help to defeat T-Series!

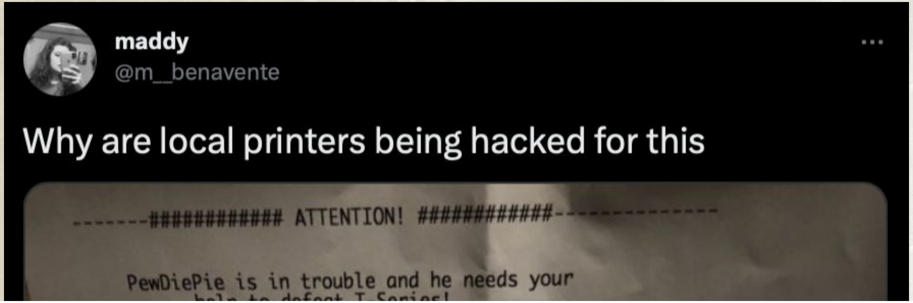
--- WHAT IS GOING ON ---

PewDiePie, the currently most subscribed to channel on YouTube, is at stake of losing his position as the number one position by an Indian company called T-Series, that simply uploads videos of Bollywood trailers and songs.

--- WHAT TO DO ---

1. Unsubscribe from T-Series
2. Subscribe to PewDiePie
3. Share awarness to this issue #SavePewDiePie
4. Tell everyone you know. Seriously.
5. BROFIST!

Source : Twitter

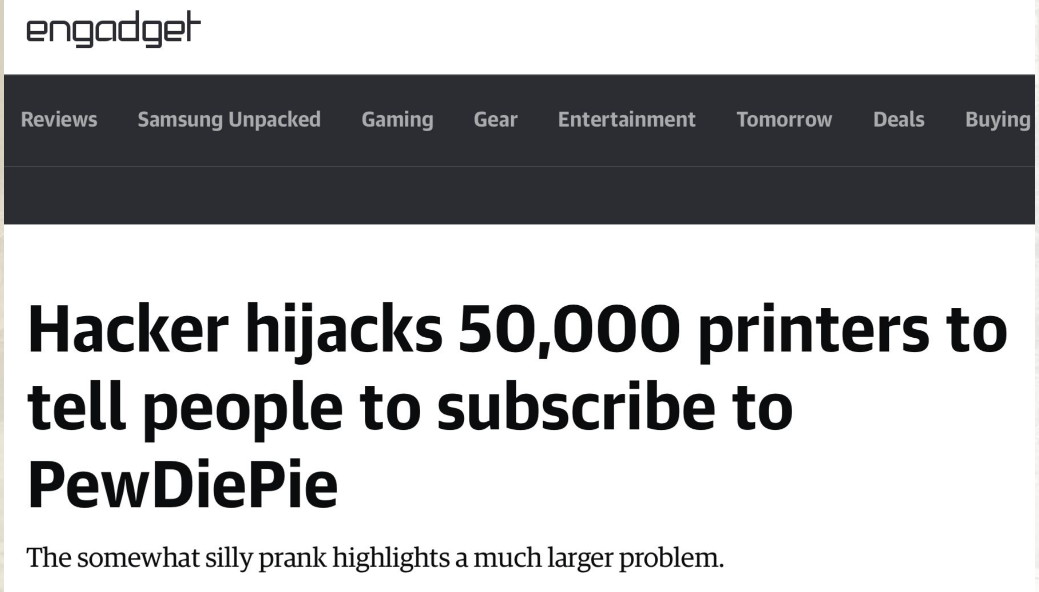


maddy
@m__benavente

Why are local printers being hacked for this

-------############ ATTENTION! ############-------------

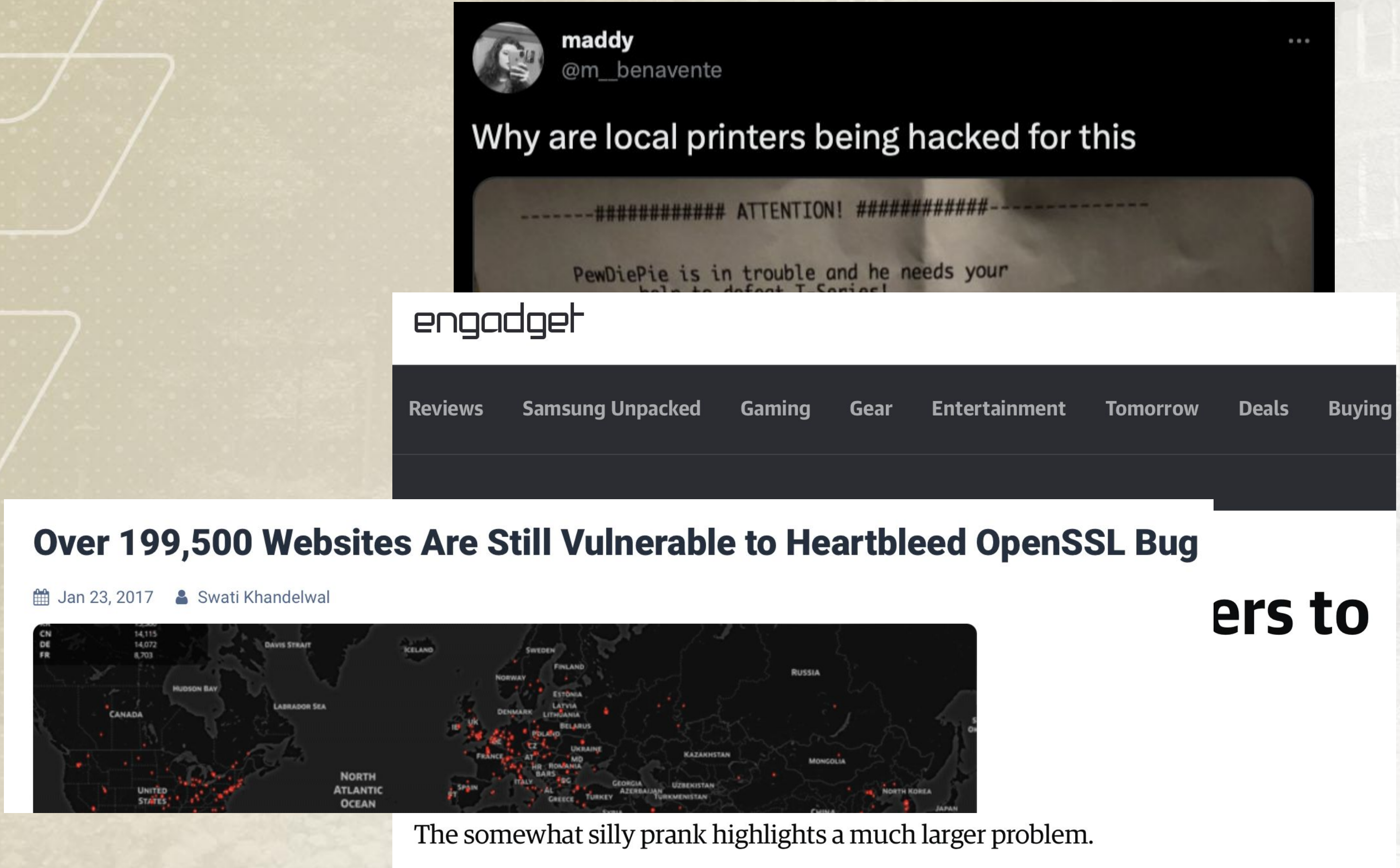
PewDiePie is in trouble and he needs your
help to defeat T-Series!



Hacker hijacks 50,000 printers to tell people to subscribe to PewDiePie

The somewhat silly prank highlights a much larger problem.

Source : Twitter
Source : Engadget



maddy
@m__benavente

Why are local printers being hacked for this

-------############ ATTENTION! ############-------------

PewDiePie is in trouble and he needs your help to defeat T-Series!

engadget

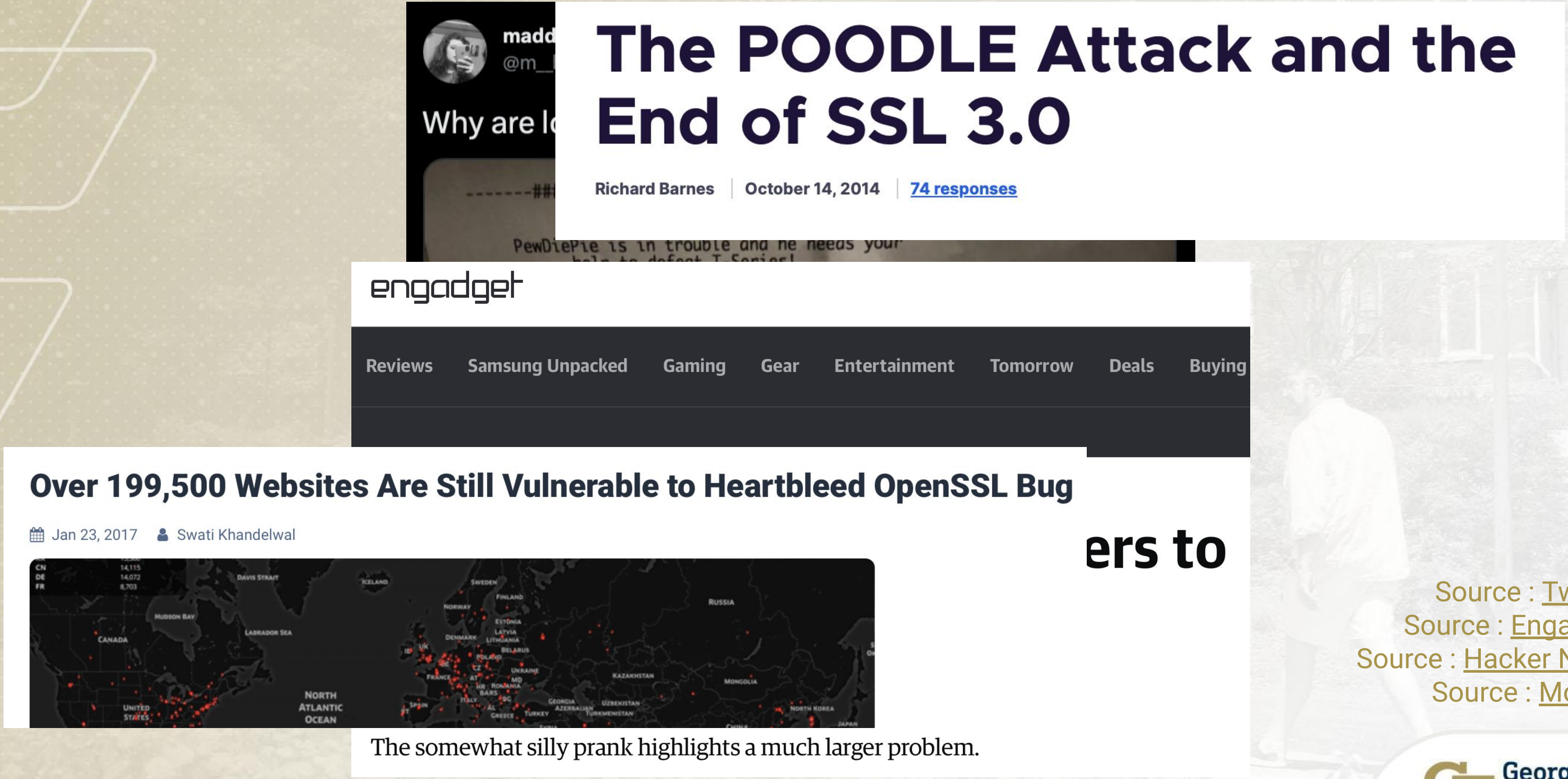
ers to

The somewhat silly prank highlights a much larger problem.

Over 199,500 Websites Are Still Vulnerable to Heartbleed OpenSSL Bug

Jan 23, 2017 Swati Khandelwal

Source : Twitter
Source : Engadget
Source : Hacker News



madd

@m_

Why are l

-------###

PewDiePie is in trouble and he needs your

help to defeat T-Series!

The POODLE Attack and the End of SSL 3.0

Richard Barnes | October 14, 2014 | 74 responses

engadget

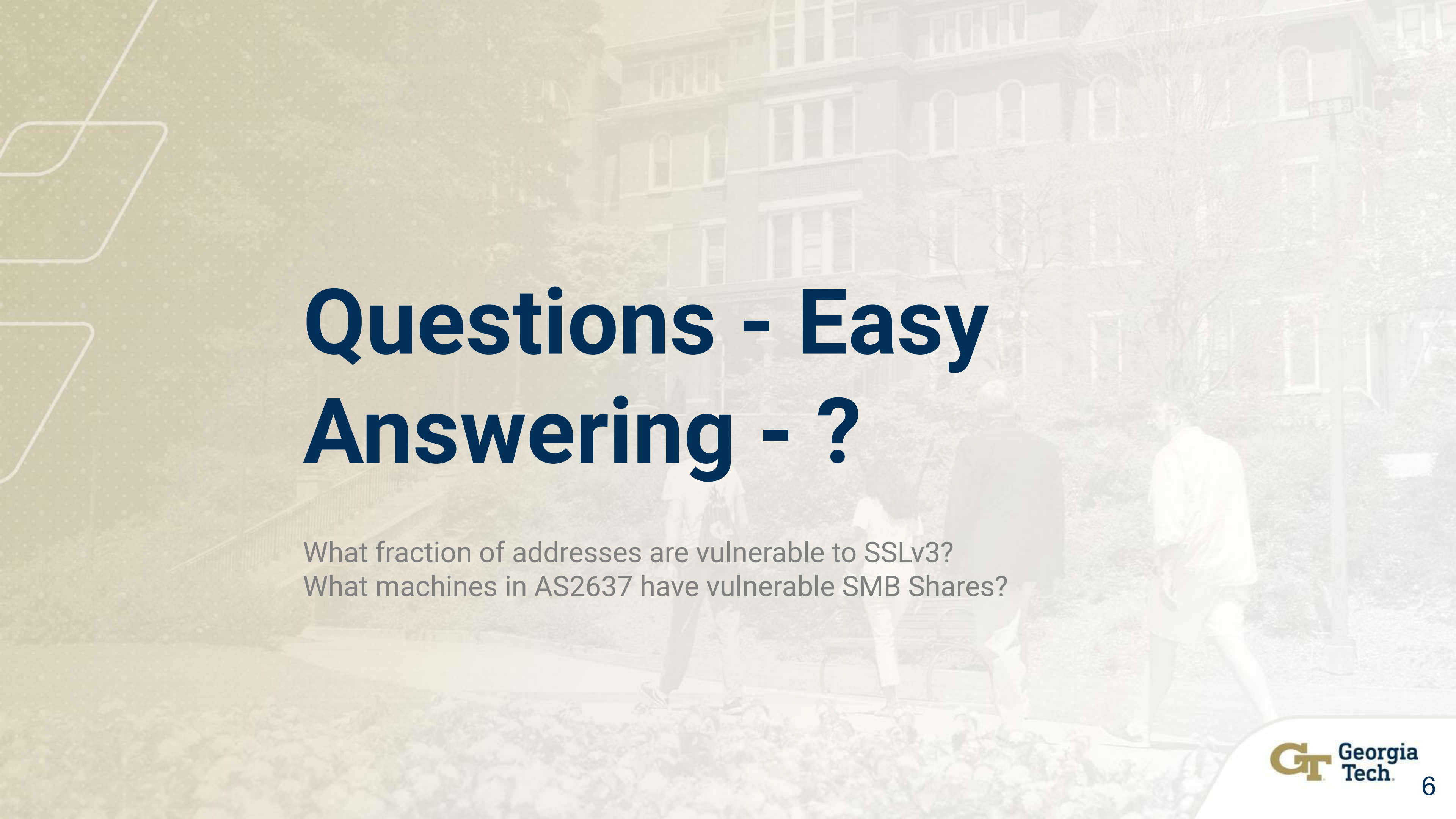
ers to

The somewhat silly prank highlights a much larger problem.

Over 199,500 Websites Are Still Vulnerable to Heartbleed OpenSSL Bug

Jan 23, 2017 Swati Khandelwal

Source : Twitter
Source : Engadget
Source : Hacker News
Source : Mozilla



Questions - Easy
Answering - ?

What fraction of addresses are vulnerable to SSLv3?
What machines in AS2637 have vulnerable SMB Shares?

How to scan the internet ?

1. Develop a scanner - We got zmap (yay!)
2. Take permits for scanning
3. Scan systems
4. Process data
5. Liable to complaints
6. Generate reports

Internet wide scanning is tough!

We have port scanners…

Censys

censys.io

Contents :

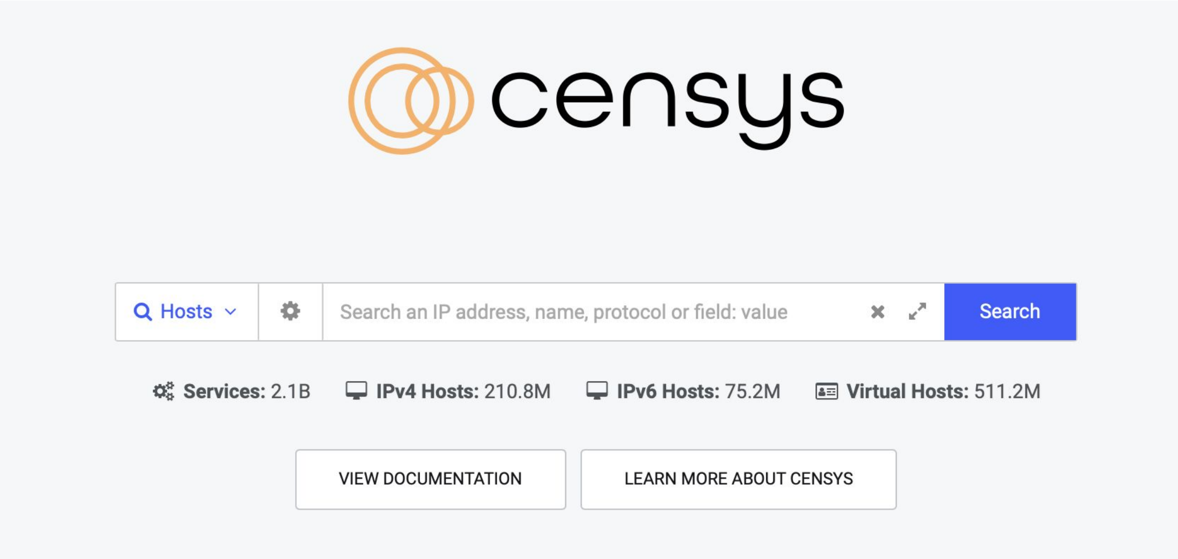
Motivation

Architecture

Application

Censys

- Cloud based
- Up-to-date
- Internet-wide
- Text based filters
- Search engine and API
- No abuse complaints
- Raw application data
- Daily snapshots



Services: 2.1B **IPv4 Hosts:** 210.8M **IPv6 Hosts:** 75.2M **Virtual Hosts:** 511.2M

Search Expressions

- Full-text searches
- Regular expressions
- Numeric ranges
- Boolean logic

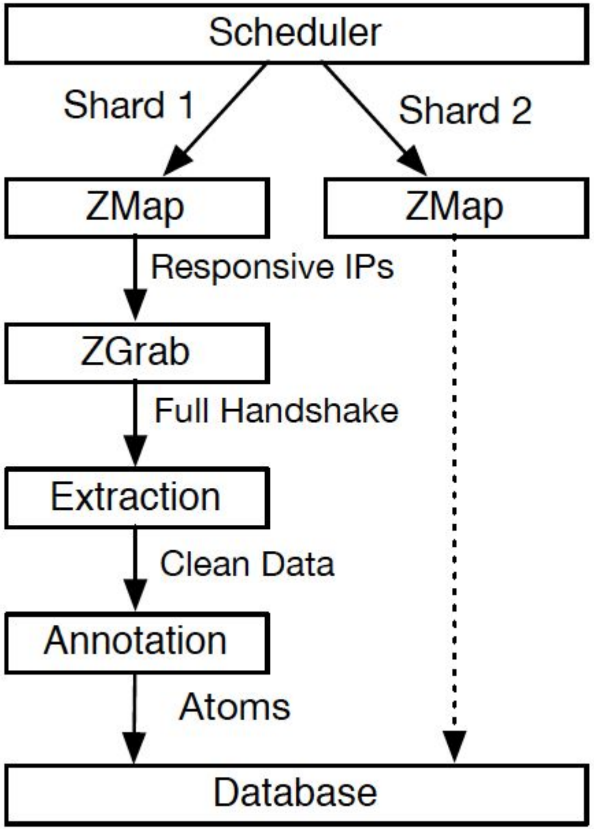
same_service(services.service_name: "ELASTICSEARCH" and services.port: 443)

*services.tls.certificates.leaf_data.issuer.organization : GoDaddy**

Architecture

Data Collection

- **ZMap** - Identify listening hosts
- **ZGrab** - Application layer data
- **ZTag** - Annotate additional metadata (user-defined)
- **ZDb** - Aggregate the horizontal scan results



Source : Zakir Durumeric et. al

ZMap

- **1200x** performance improvement over Nmap (2013)
- Scan the Internet in **under 5 minutes** (2014)
- Built-in sharding for rate-limiting network bandwidth
- Detects variance in response rates

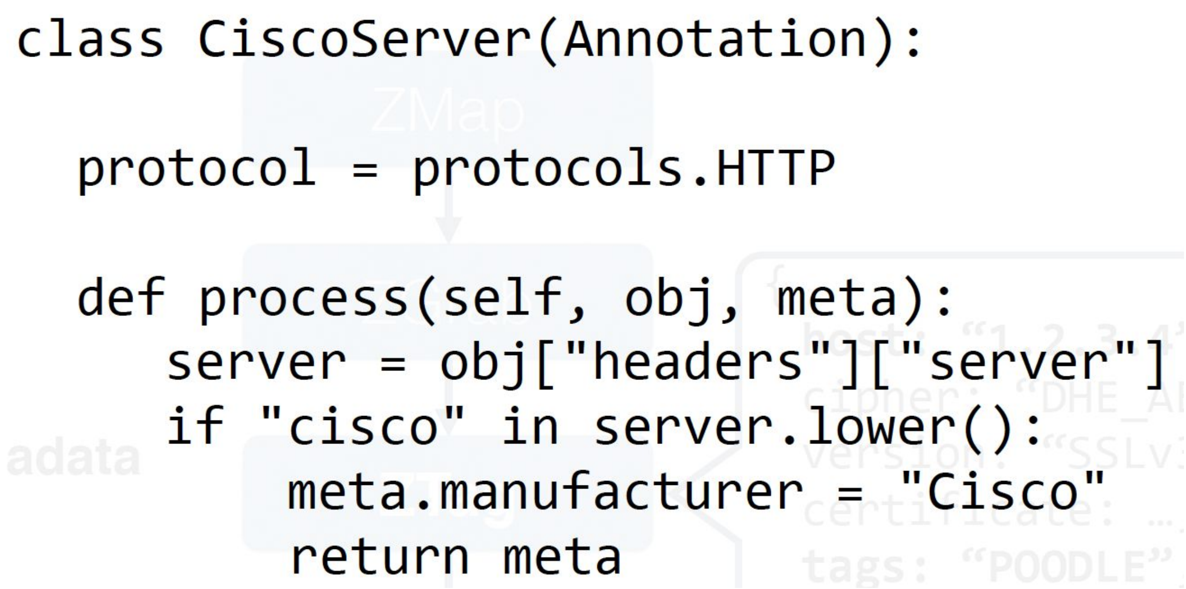
Source Code : https://github.com/zmap/zmap

ZGrab

- Supports various application handshakes
- Complete HTTPS handshakes with full IPv4 address space in **6h 20m**
- Handles concurrent connections, logging and generating JSON documents

Source Code : https://github.com/zmap/zgrab2

Custom annotations



```
class CiscoServer(Annotation):

  protocol = protocols.HTTP

  def process(self, obj, meta):
      server = obj["headers"]["server"]
      if "cisco" in server.lower():
          meta.manufacturer = "Cisco"
          return meta
```

Source : David Adrian

ZDb

- Aggregate all responses by horizontal workers
- Aggregation of scan top 5 protocol scans requires **330M records/day**
- Apache Cassandra (**37 Hrs**) & MongoDB (**13 Hrs**)
- **90%** of data is unchanged

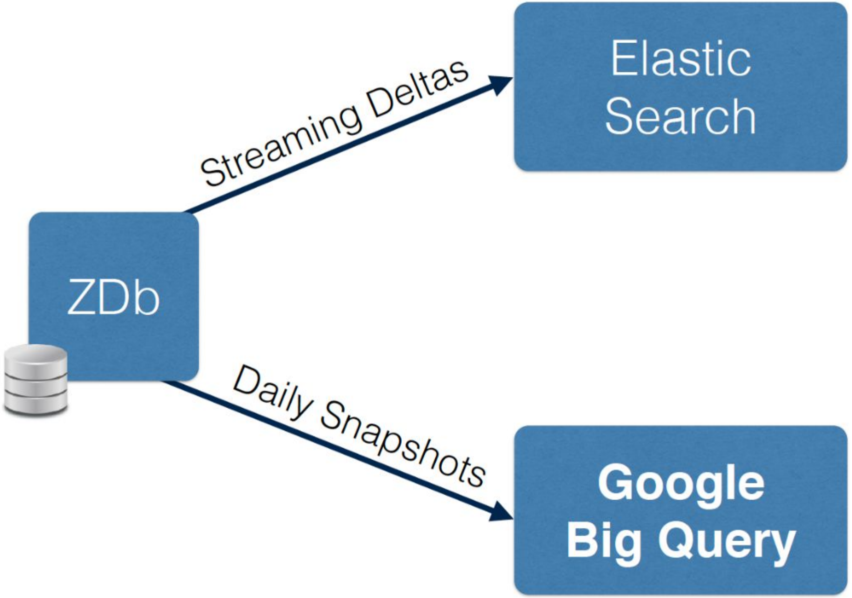
ZDb

- Aggregate all responses by horizontal workers
- Aggregation of scan top 5 protocol scans requires **330M records/day**
- Apache Cassandra (**37 Hrs**) & MongoDB (**13 Hrs**)
- **90%** of data is unchanged

10 minutes!

Exposing Data

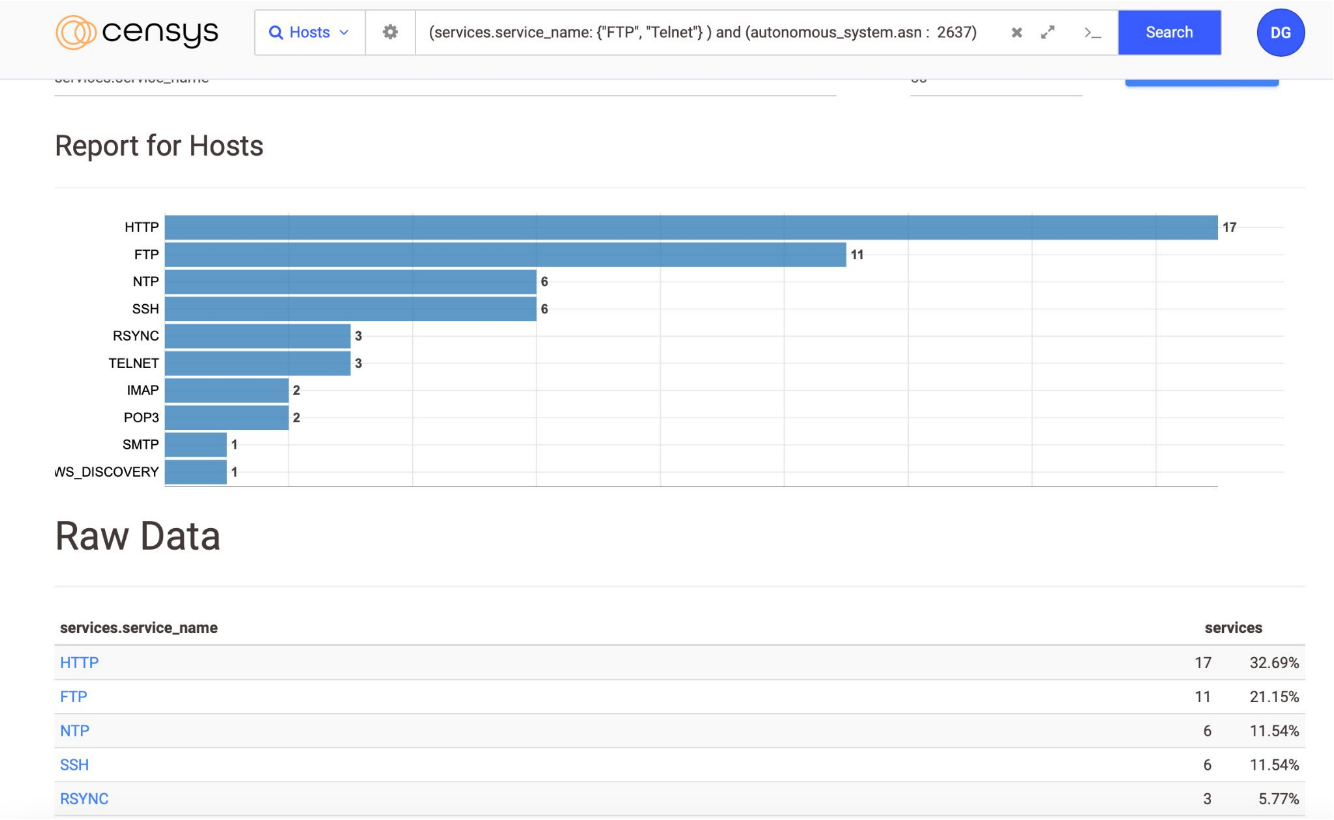
- ElasticSearch
  - Full text search
  - Queries over current data
- Google Big Query
  - SQL queries
  - Queries over historical data



Source : David Adrian

Applications

List of FTP and Telnet ports in Georgia Tech



(services.service_name: {"FTP", "Telnet"}) and (autonomous_system.asn : 2637)

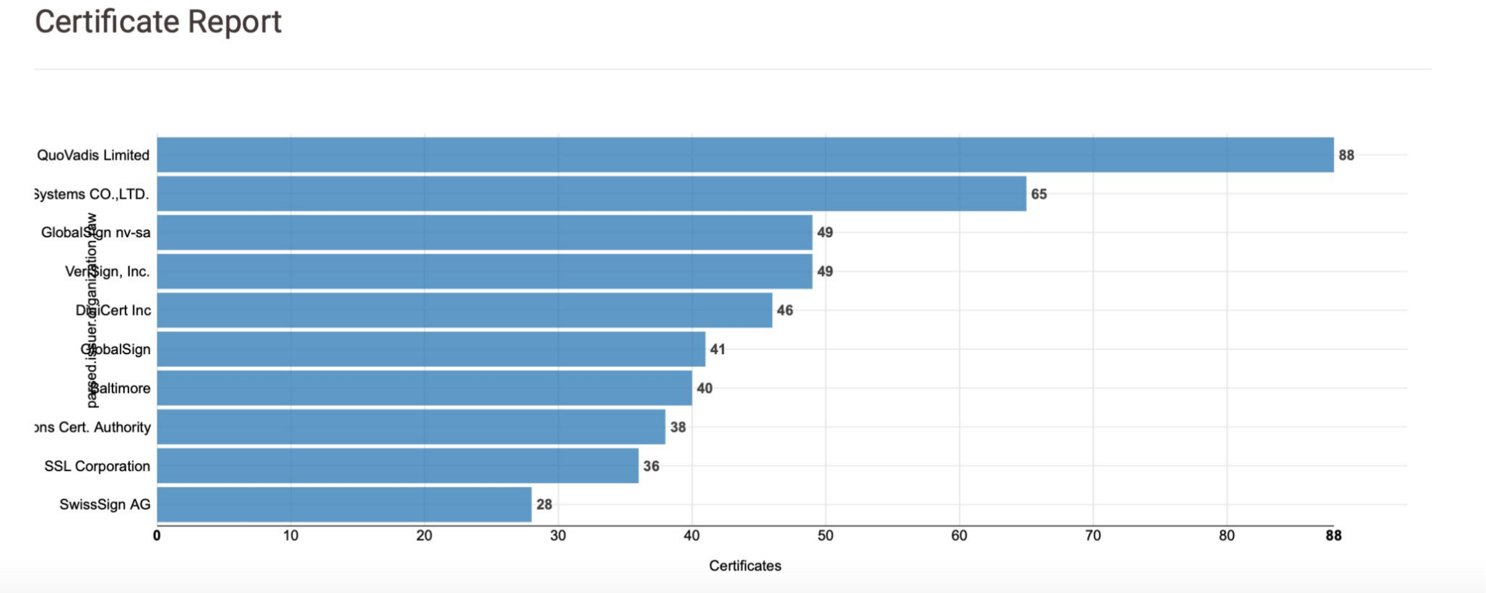
Report for Hosts

Raw Data

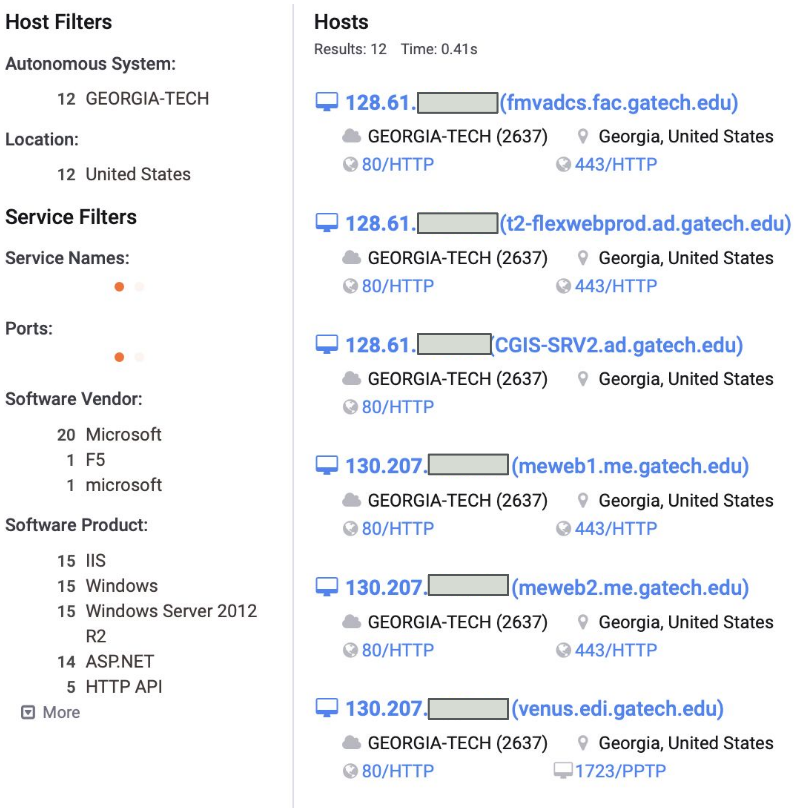
services.service_name	services	
HTTP	17	32.69%
FTP	11	21.15%
NTP	6	11.54%
SSH	6	11.54%
RSYNC	3	5.77%

Certificates whose trust has been revoked

Query : *validation.google_ct_primary.in_revocation_set: true*



Windows 2008 and 2012 R2 servers at Georgia Tech



Host Filters

Autonomous System:

12	GEORGIA-TECH

Location:

12	United States

Service Filters

Service Names:

Ports:

Software Vendor:

20	Microsoft
1	F5
1	microsoft

Software Product:

15	IIS
15	Windows
15	Windows Server 2012 R2
14	ASP.NET
5	HTTP API

More

Hosts

Results: 12 Time: 0.41s

128.61.[redacted](fmvadcs.fac.gatech.edu)
GEORGIA-TECH (2637) Georgia, United States
80/HTTP 443/HTTP

128.61.[redacted](t2-flexwebprod.ad.gatech.edu)
GEORGIA-TECH (2637) Georgia, United States
80/HTTP 443/HTTP

128.61.[redacted](CGIS-SRV2.ad.gatech.edu)
GEORGIA-TECH (2637) Georgia, United States
80/HTTP

130.207.[redacted](meweb1.me.gatech.edu)
GEORGIA-TECH (2637) Georgia, United States
80/HTTP 443/HTTP

130.207.[redacted](meweb2.me.gatech.edu)
GEORGIA-TECH (2637) Georgia, United States
80/HTTP 443/HTTP

130.207.[redacted](venus.edi.gatech.edu)
GEORGIA-TECH (2637) Georgia, United States
80/HTTP 1723/PPTP

Censys vs Shodan

Ethical Considerations

- Exposes information about vulnerable systems in public

Ethical Considerations

- Exposes information about vulnerable systems in public
- Opt-out facility

Ethical Considerations

- Exposes information about vulnerable systems in public
- Opt-out facility
- Concurrent scans on low-bandwidth devices

Thank You!