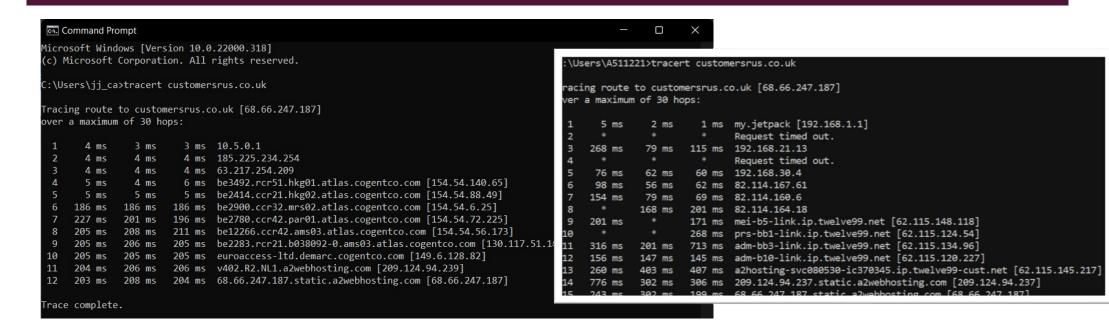
UNIVERSITY OF ESSEX PRACTICAL ACTIVITY - SCANNING EXERCISE

NETWORK AND INFORMATION SECURITY MANAGEMENT NOVEMBER 2021 A GROUP 3



[CUSTOMERSRUS.CO.UK] TRACERT



Findings in tracert:

After the local ISP, other country hop in atlas.cogentco.com domain (ISP: Cogentco) caused the biggest delay, the average duration is 121.41ms.

[CUSTOMERSRUS.CO.UK] NAMESERVERS AND REGISTERED CONTACT

A2 Hosting web hosting nameservers (nslookup)

Name servers: ns1.a2hosting.com ns2.a2hosting.com ns3.a2hosting.com ns4.a2hosting.com :\Users\A511221>nslookup -type=ns customersrus.co.uk
erver: my.jetpack
ddress: 192.168.1.1

on-authoritative answer:
ustomersrus.co.uk nameserver = ns3.a2hosting.com
ustomersrus.co.uk nameserver = ns4.a2hosting.com
ustomersrus.co.uk nameserver = ns2.a2hosting.com
ustomersrus.co.uk nameserver = ns1.a2hosting.com

MX record (nslookup)

customersrus.co.uk. 5 IN MX 0 mail.customersrus.co.uk.

:\Users\A511221>nslookup -q=MX customersrus.co.uk erver: my.jetpack ddress: 192.168.1.1 on-authoritative answer: ustomersrus.co.uk MX preference = 0, mail exchanger = mail.customersrus.co.uk

Based the IP ping result, showed that the mail server hosting in A2 Hosting

Ping mail.customersrus.co.uk [68.66.247.187]

Registered contact (whois)



City: Ann Arbor StateProv: MI

PostalCode: 48106

Country: US

RegDate: 2004-03-16 Updated: 2021-10-13

Comment: http://www.a2hosting.com

Ref: https://rdap.arin.net/registry/entity/A2HOS



[CUSTOMERSRUS.CO.UK] WEBSITE HOSTED

- A2 Hosting, Inc.
 - United States of America (Ann Arbor)
 - Netherlands (Amsterdam)
- Ref: https://www.iplocation.net/ip-lookup

Geolocation data from IP2Location (Product: DB6, updated on 2021-11-1)

IP Address	Country	Region	City
68.66.247.187	United States of America	Michigan	Ann Arbor
ISP	Organization	Latitude	Longitude
A2 Hosting Inc.	Not Available	42.2288	-83.7359

Geolocation data from ipinfo.io (Product: API, real-time)

IP Address	Country	Region	City
68.66.247.187	Netherlands 🔤	North Holland	Amsterdam
ISP	Organization	Latitude	Longitude
A2 Hosting, Inc.	A2 Hosting, Inc. (a2hosting.com)	52.3740	4.8897

TEAM ACTIVITY

- A2 Hosting, Inc. provided solutions to prevent attack and abuse:
 - Google reCAPTCHA bot detection
 - Affect: Testing the website with lower level
 - Temporarily banned IP addresses
 - Affect: Unable to send too much request and require to change IP address if blocked
 - SSL
 - Affect: Packet or traffic capture may not able to get information
- References:
 - https://www.a2hosting.com/kb/security/temporarily-banned-ip-addresses
 - https://www.a2hosting.com/kb/security

DISCUSS THE RESULTS

Did you have any issues or challenges with the scans?

There were discrepancies between results produced from the traceroute such as number of hobs to the target website and the delay on the route and average delay.

Two IP location (United States – Netherlands/Amsterdam)

Limited information on the domain registration and the registered contact

DISCUSS THE RESULTS

How did you overcome them?

Using online tools such as ICANN LOOKUP https://lookup.icann.org/lookup (to find registered contact) and WHOIS https://who.is/whois/customersrus.co.uk (to find registrar and Name servers) and https://www.findip-address.com/ (to find Hosting name and location)

How will they affect your final report?

Depending on one scan tool would be not enough to get the complete information about the target, which will be needed to conduct a proper website vulnerability assessment.