Dear

Freedom of Information request reference K/20/106

Thank you for your Freedom of Information (FOI) request dated 11 February 2020, reference K/20/106.

Your request read:

“Question 1 – Name of Your Institution:
Question 2 - Who monitors your institution's IT estate for malware activity? Select one from:
  • In-house
  • 3rd Party or SIEM as a Service
  • Both
  • Neither
  • Other – please specify:
Question 3 - Does your institution monitor for malware activity through the use of endpoint agents? For example, deployed anti-virus / anti-malware software to workstations, phones, etc. Select one from:
  • Yes
  • No
  • Other – please specify:
Question 4 - Does your institution monitor for malware activity by inspecting / analysing network traffic, either as part of a system or service? For example, a SIEM product or service, Intrusion Detection solution, etc. Select one from:
  • Yes
  • No
  • Other – please specify:
Question 5 - To what extent does DNS analysis form a part of malware identification within your solutions? Solutions many include vendor software, firewalls, analysis performed by a person, or by a SIEM service. Please select all that apply.
  • DNS analysis does not form any part of our solutions
  • Our solutions look for DNS to/from known malware/malicious infrastructure (e.g. botnets, command-and-control servers)
  • Our solution identifies malware from looking at DNS features (e.g. TTL, query/prefix-length, domain-names, IP response diversity, geolocation)
  • Our solution identifies malware attempting to perform reconnaissance, weaponisation, delivery, exploitation or exfiltration by DNS
  • Other - please specify:
Question 6 - To what extent can your in-house cyber security professionals perform DNS analysis as part of malware analysis? Mark on a scale of 1 to 5 where:
  1. We have no in-house cyber security professionals / all cyber security work is outsourced.
  5. Our cyber security professionals are fully competent in DNS packet inspection (e.g. using tools such as Wireshark)
Question 7 - In the last 12 months, compared with the previous 12 months, have you seen malware infections:
• Increase
• Decrease
• Remain relatively constant

Question 8 - Are outgoing DNS requests blocked or filtered on your network? Select one from:
• No
• No - but DNS requests to malicious or inappropriate sites are monitored
• Yes - DNS requests to malicious or inappropriate sites are blocked / filtered (blacklisting)
• Yes - only approved DNS requests are permitted (whitelisting)
• Other – please specify:

Question 9 - Are internally-resolved DNS requests blocked or filtered on your network? Select one from:
• No
• No - but DNS requests are monitored
• Yes - certain DNS requests are blocked / filtered (blacklisting)
• Yes - only approved DNS requests are permitted (whitelisting)
• Other

Question 10 - Has funding allocated towards preventing malware infection changed due to the demographic dip?
"Demographic dip" refers to the number of 18-year-olds in the UK population falling significantly between now and 2022. Changes may be directly or indirectly caused by the dip. Select one from:
• Funding has increased
• Funding has decreased
• Funding has remained the same

Question 11 - How much did your institution spend on cyber-defence (including malware prevention) over the last 12 months?
Please do not include costs of any staff. Include any capital or revenue costs.

Question 12 - Have resources (including people) allocated towards preventing malware infection changed due to the demographic dip?
"Demographic dip" refers to the number of 18-year-olds in the UK population falling significantly between now and 2022. Changes may be directly or indirectly caused by the dip. Select one from:
• Resourcing has increased
• Resourcing has decreased
• Resourcing has remained the same

Question 13 - How many people (in FTEs) do you have working on cyber-defence of your institution's network?
Please don’t include research activities, or staff of third-parties."

The University of Leeds holds this information. For your convenience we have responded to each of your questions in turn below.

Name of Your Institution
University of Leeds
Who monitors your institution’s IT estate for malware activity?
In-house

Does your institution monitor for malware activity through the use of endpoint agents? For example, deployed anti-virus / anti-malware software to workstations, phones, etc.
Yes

Does your institution monitor for malware activity by inspecting / analysing network traffic, either as part of a system or service? For example, a SIEM product or service, Intrusion Detection solution, etc.
Yes

To what extent does DNS analysis form a part of malware identification within your solutions?
Our solutions look for DNS to/from known malware/malicious infrastructure

To what extent can your in-house cyber security professionals perform DNS analysis as part of malware analysis? Mark on a scale of 1 to 5 where 1. We have no in-house cyber security professionals / all cyber security work is outsourced. 5. Our cyber security professionals are fully competent in DNS packet inspection (e.g. using tools such as Wireshark)
4

In the last 12 months, compared with the previous 12 months, have you seen malware infections:
Increase

Are outgoing DNS requests blocked or filtered on your network?
Yes - DNS requests to malicious or inappropriate sites are blocked / filtered (blacklisting)

Are internally-resolved DNS requests blocked or filtered on your network?
Yes - certain DNS requests are blocked / filtered (blacklisting)

Has funding allocated towards preventing malware infection changed due to the demographic dip?
Funding has increased

How much did your institution spend on cyber-defence (including malware prevention) over the last 12 months?
We consider that this information is exempt from disclosure under section 31(1)(a) of the Freedom of Information Act.

Section 31(1)(a) sets out that information is exempt from disclosure if its release would or would be likely to prejudice the prevention or detection of crime.
To reveal the information regarding the expenditure and resources in place regarding our cyber-defence provision would go some way to demonstrating the methods used. For instance, a small team operating with a small budget is very unlikely to have sophisticated technologies in place, while a large team operating a large
budget is likely to have wider-reaching capabilities. We consider that to release this information, alongside information such as that requested at other parts of your request (e.g. regarding the nature of the cyber-defence systems and procedures in place) could be added together into a ‘mosaic effect’ to give a detailed picture of the security measures in place (and not in place) at the University. Motivated individuals could use the information in order to target the University, or to adapt behaviour in order to avoid detection.

Section 31(1)(a) is a qualified exemption. This means that the University of Leeds is required to consider whether the public interest in the information outweighs the public interest in maintaining the exemption.

There is clearly a very strong public interest in protecting public authorities from crime. To release information which increases the University’s vulnerability to cyber-crime would jeopardise our ability to provide services to our students (current, former and potential), and would put at risk personal, financial and commercial sensitive information. We therefore consider that there is a very strong public interest in maintaining the exemption. Conversely, we do not consider there to be any particular public interest in the disclosure of this information. While it is important for students and the public to understand that the University takes the threat of cyber-crime seriously, and are taking appropriate measures to tackle it, we do not consider that this interest would be furthered by the release of this information.

We therefore consider that the public interest is firmly in favour of withholding the information in this case.

Have resources (including people) allocated towards preventing malware infection changed due to the demographic dip?
Resourcing has remained the same

How many people (in FTEs) do you have working on cyber-defence of your institution's network?
We consider this information to be exempt under section 31(1)(a) as outlined above.

We hope this information is helpful. If you have any questions about this email, however, please do not hesitate to contact us on foi@leeds.ac.uk

If you are unhappy with the service you have received in relation to your request and wish to make a complaint or request a review of our decision, you can request an Internal Review. Requests for Internal Review should be made in writing using the following contact information:

Post: Mr D Wardle
Deputy Secretary
The University of Leeds
Leeds
LS2 9JT

Email: foi@leeds.ac.uk
Requests for Internal Review should be submitted within 40 working days of receiving the University’s response to your request. Further information about how the University manages Freedom of Information requests and about our complaints procedure is also available on our website (www.leeds.ac.uk).

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. Generally, the ICO cannot make a decision unless you have exhausted the review/complaints procedure provided by the University. The Information Commissioner can be contacted at: Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Kind regards

Chloe Wilkins

Freedom of Information Officer
Secretariat
University of Leeds