Email Security Solutions Analysis Questions

By: Ryan Stewart

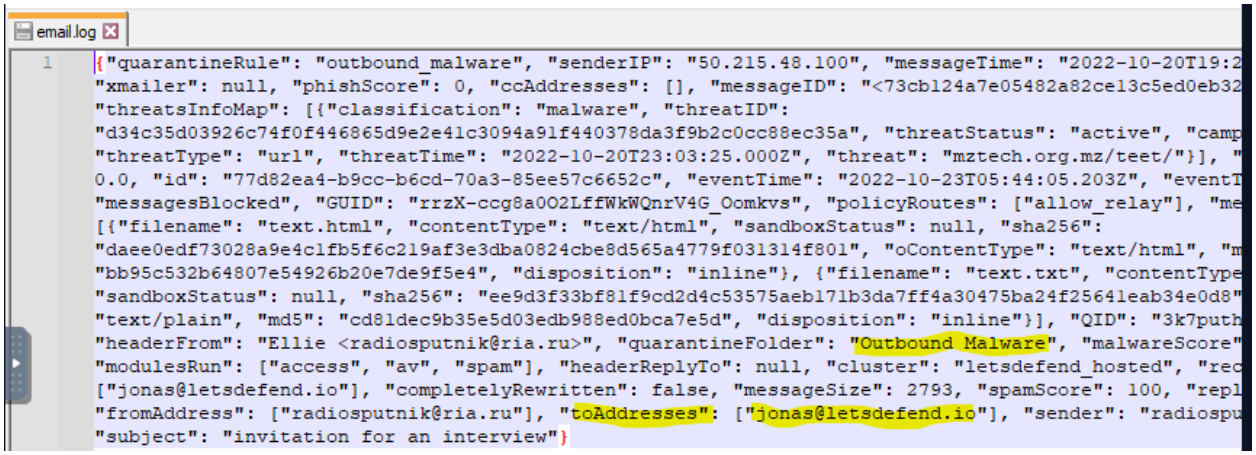
(Image Source: https://www.proofpoint.com/au/threat-reference/email-security)

Question: According to the email security solution log, what is the email address of the recipient of the email? (Check the "recipient" field)

email.log


```
{"quarantineRule": "outbound_malware", "senderIP": "50.215.48.100", "messageTime": "2022-10-20T19:2
"xmailer": null, "phishScore": 0, "ccAddresses": [], "messageID": "<73cb124a7e05482a82ce13c5ed0eb32
"threatsInfoMap": [{"classification": "malware", "threatID":
"d34c35d03926c74f0f446865d9e2e41c3094a91f440378da3f9b2c0cc88ec35a", "threatStatus": "active", "camp
"threatType": "url", "threatTime": "2022-10-20T23:03:25.000Z", "threat": "mztech.org.mz/teet/"}], "
0.0, "id": "77d82ea4-b9cc-b6cd-70a3-85ee57c6652c", "eventTime": "2022-10-23T05:44:05.203Z", "eventT
"messagesBlocked", "GUID": "rrzX-ccg8a0O2LffWkWQnrV4G_Oomkvs", "policyRoutes": ["allow_relay"], "me
[{"filename": "text.html", "contentType": "text/html", "sandboxStatus": null, "sha256":
"daee0edf73028a9e4c1fb5f6c219af3e3dba0824cbe8d565a4779f031314f801", "oContentType": "text/html", "m
"bb95c532b64807e54926b20e7de9f5e4", "disposition": "inline"}, {"filename": "text.txt", "contentType
"sandboxStatus": null, "sha256": "ee9d3f33bf81f9cd2d4c53575aeb171b3da7ff4a30475ba24f2564leab34e0d8"
"text/plain", "md5": "cd81dec9b35e5d03edb988ed0bca7e5d", "disposition": "inline"}], "QID": "3k7puth
"headerFrom": "Ellie <radiosputnik@ria.ru>", "quarantineFolder": "Outbound Malware", "malwareScore"
"modulesRun": ["access", "av", "spam"], "headerReplyTo": null, "cluster": "letsdefend_hosted", "rec
["jonas@letsdefend.io"], "completelyRewritten": false, "messageSize": 2793, "spamScore": 100, "repl
"fromAddress": ["radiosputnik@ria.ru"], "toAddresses": ["jonas@letsdefend.io"], "sender": "radiospu
"subject": "invitation for an interview"}
```

What is the type of threat according to the email security solution log provided? (Check the "classification" field)


email.log


```
{"quarantineRule": "outbound_malware", "senderIP": "50.215.48.100", "messageTime": "2022-10-20T19:2
"xmailer": null, "phishScore": 0, "ccAddresses": [], "messageID": "<73cb124a7e05482a82ce13c5ed0eb32
"threatsInfoMap": [{"classification": "malware", "threatID":
"d34c35d03926c74f0f446865d9e2e41c3094a91f440378da3f9b2c0cc88ec35a", "threatStatus": "active", "camp
"threatType": "url", "threatTime": "2022-10-20T23:03:25.000Z", "threat": "mztech.org.mz/teet/"}], "
0.0, "id": "77d82ea4-b9cc-b6cd-70a3-85ee57c6652c", "eventTime": "2022-10-23T05:44:05.203Z", "eventT
"messagesBlocked", "GUID": "rrzX-ccg8a0O2LffWkWQnrV4G_Oomkvs", "policyRoutes": ["allow_relay"], "me
[{"filename": "text.html", "contentType": "text/html", "sandboxStatus": null, "sha256":
"daee0edf73028a9e4c1fb5f6c219af3e3dba0824cbe8d565a4779f031314f801", "oContentType": "text/html", "m
"bb95c532b64807e54926b20e7de9f5e4", "disposition": "inline"}, {"filename": "text.txt", "contentType
"sandboxStatus": null, "sha256": "ee9d3f33bf81f9cd2d4c53575aeb171b3da7ff4a30475ba24f2564leab34e0d8"
"text/plain", "md5": "cd81dec9b35e5d03edb988ed0bca7e5d", "disposition": "inline"}], "QID": "3k7puth
"headerFrom": "Ellie <radiosputnik@ria.ru>", "quarantineFolder": "Outbound Malware", "malwareScore"
"modulesRun": ["access", "av", "spam"], "headerReplyTo": null, "cluster": "letsdefend_hosted", "rec
["jonas@letsdefend.io"], "completelyRewritten": false, "messageSize": 2793, "spamScore": 100, "repl
"fromAddress": ["radiosputnik@ria.ru"], "toAddresses": ["jonas@letsdefend.io"], "sender": "radiospu
"subject": "invitation for an interview"}
```