# USECASE 3bis ANALYSE DE LOG

**Ticket 002**

**Titre:**

Analyse des activités suspectes sur le serveur mail

**Numéro :** 002

**Sévérité:** Critique

**Contexte :** L'analyse des logs du serveur mail révèle une activité répétée et structurée liée à l'envoi d'emails. Ces emails proviennent principalement d'un utilisateur identifié comme alexis.lebrun@cyber.com et sont adressés à divers destinataires externes. Les adresses IP observées incluent notamment 42.24.237.124, qui est particulièrement récurrente, ainsi que d'autres adresses proches dans la plage 42.24.237.xxx. Il est important de noter que certaines de ces IP pourraient correspondre à l'infrastructure SMTP interne de l'organisation. Les emails présentent des caractéristiques homogènes, avec des tailles similaires et des délais de traitement constants autour de 0.21 secondes, ce qui pourrait indiquer l'utilisation d'un script automatisé. Cette uniformité soulève des préoccupations quant à une possible exfiltration de données sensibles ou une activité malveillante ciblée.

**Analyse:** Les adresses IP identifiées dans les logs doivent être analysées en détail pour distinguer celles appartenant à l'infrastructure interne des connexions externes. L'utilisation fréquente de l'IP 42.24.237.124 mérite une attention particulière, car elle semble être à l'origine d'une grande partie des connexions. Les emails envoyés présentent des tailles de message proches les unes des autres, ce qui pourrait indiquer une tentative d'exfiltration de données structurées ou une répétition orchestrée. Les délais similaires pour chaque envoi, couplés à un volume important, laissent penser que ces opérations sont automatisées via un script. Enfin, le compte utilisateur alexis.lebrun@cyber.com semble être un point central de cette activité, ce qui soulève la possibilité d'une compromission.

**Recommandation:** Il est impératif de vérifier si les adresses IP identifiées appartiennent à l'infrastructure interne ou SMTP. Si oui, une analyse forensique des serveurs doit être menée pour détecter toute compromission. Le compte alexis.lebrun@cyber.com doit être immédiatement bloqué, et une analyse forensique de son poste de travail réalisée pour identifier d'éventuelles anomalies. L'utilisateur doit être interrogé pour fournir des explications.

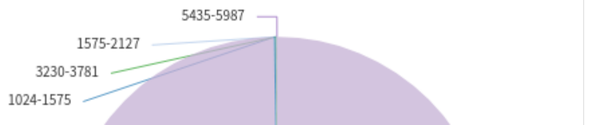
Le contenu des emails doit être inspecté pour vérifier s'il contient des données exfiltrées. Des alertes doivent être configurées pour détecter des comportements similaires à l'avenir. Cette activité rappelle les modes opératoires d'APT tels que APT28 (Fancy Bear) et APT32 (OceanLotus), connus pour leurs scripts automatisés et leurs campagnes d'exfiltration via des emails homogènes.

structured_email_logs table

| Date | Time | Server | ID | Client | IP | SASLMethod | Username | From | To | Size | Delay | Status |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 05:11:22 | mailserver038 | 18F8914006403 | unknown | 42.24.237.169 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | garage.chardon@wanadoo.fr | 6490 | 0.21 | sent |
| 7 | 05:11:21 | mailserver038 | 25FF114006403 | unknown | 42.24.237.169 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | garagejm@orange.fr | 6476 | 0.22 | sent |
| 7 | 05:11:20 | mailserver038 | 7389014006409 | unknown | 42.24.236.156 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | garageducoude@wanadoo.fr | 6488 | 0.21 | sent |
| 7 | 05:11:20 | mailserver038 | 6693D14006403 | unknown | 42.24.236.156 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | spatigj@wanadoo.fr | 6476 | 0.21 | sent |
| 7 | 05:11:19 | mailserver038 | 9D84514006403 | unknown | 42.24.236.120 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | christian.pourron@wanadoo.fr | 6496 | 0.21 | sent |
| 7 | 05:11:19 | mailserver038 | 44FB31400600C | unknown | 42.24.236.156 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | garage.pelot@wanadoo.fr | 6486 | 0.22 | sent |
| 7 | 05:11:18 | mailserver038 | 8C68614005809 | unknown | 42.24.237.64 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | garage.jeanvoine.renault@orange.fr | 6507 | 0.21 | sent |
| 7 | 05:11:17 | mailserver038 | E266514005809 | unknown | 42.24.237.3 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | deronchi@wanadoo.fr | 6476 | 0.22 | sent |
| 7 | 05:11:17 | mailserver038 | 8E64814005421 | unknown | 42.24.237.64 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | ghauto@wanadoo.fr | 6473 | 0.23 | sent |
| 7 | 05:11:16 | mailserver038 | DDD0614005421 | unknown | 42.24.237.64 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | garage.du.lion@wanadoo.fr | 6489 | 0.21 | sent |
| 7 | 05:11:16 | mailserver038 | 799F114005421 | unknown | 42.24.237.169 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | ghauto2@orange.fr | 6474 | 0.21 | sent |
| 7 | 05:11:16 | mailserver038 | 3E61B14005421 | unknown | 42.24.237.124 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | carrosserie.besnard@orange.fr | 6498 | 0.21 | sent |
| 7 | 05:11:15 | mailserver038 | DA8A714005421 | unknown | 42.24.236.171 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | maichepneus@orange.fr | 6482 | 0.21 | sent |
| 7 | 05:11:14 | mailserver038 | 4183A14005421 | unknown | 42.24.237.64 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | garage.gerdy@orange.fr | 6483 | 0.21 | sent |
| 7 | 05:11:14 | mailserver038 | 0C62C14005421 | unknown | 42.24.236.156 | XCLIENT | alexis.lebrun | alexis.lebrun@cyber.com | contact@garageauthier.fr | 6490 | 0.21 | sent |

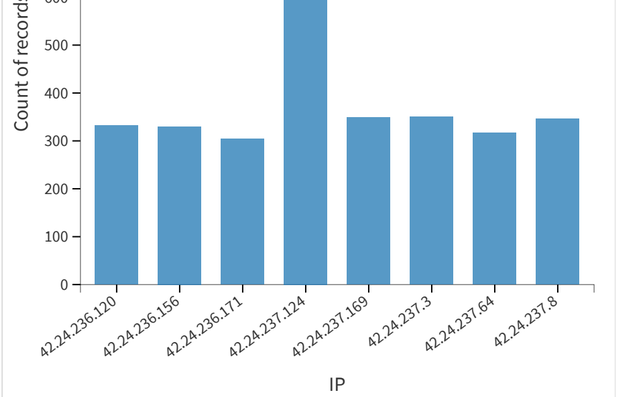
Count by IP on structured_email_logs

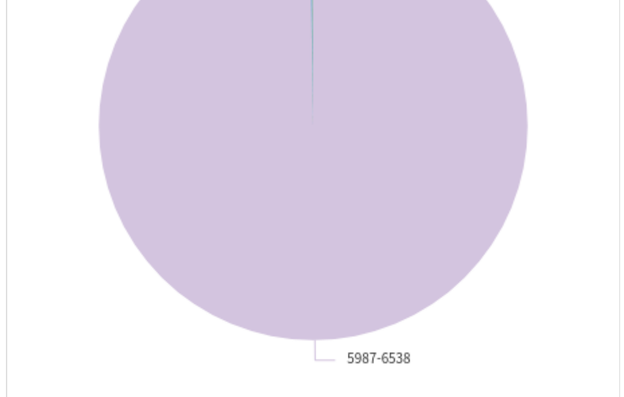

Taille des mails envoyés (presque tout le temps la meme taille) on stru…

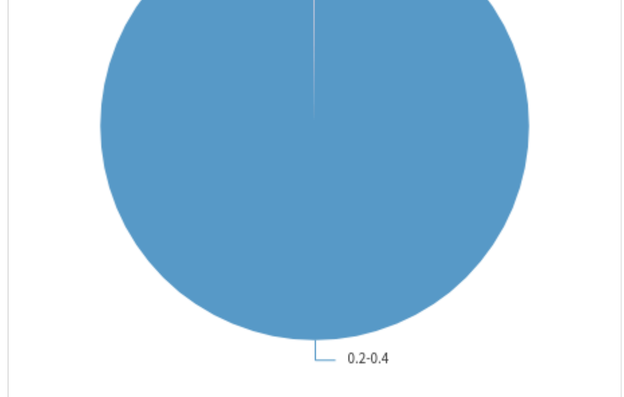


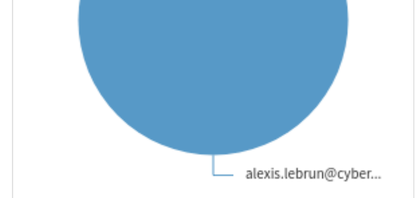

Les delays entre chaque mails sont tous de 0.2 sec on structured_emai…


Les mails viennent tous du mail alexis.leb…


Count of records
500
400
300
200
100
0
42.24.236.120
42.24.236.156
42.24.236.171
42.24.237.124
42.24.237.169
42.24.237.3
42.24.237.64
42.24.237.8
IP


5987-6538


0.2-0.4


alexis.lebrun@cyber...