Rapport d’investigation

Remplissez ce document avec les informations demandées. N’oubliez pas d’inclure des captures d’écran dans toutes les instances indiquées.

Alerte 1 : ***Un email avec une pièce jointe suspicieuse*** *"facture_edf_1.docm", a été reçu. Ce document Word contient une macro VBA malveillante qui exécute un script PowerShell à la fermeture du document.*

Risque : élevé

Détails d’investigation

Reportez ici la chronologie de l’attaque et les détails techniques. Ajoutez ou enlevez des points au besoin.

Plus d'informations en consultant le rapport associé à cette alerte.

- Analyse Oletools : Le fichier facture_edf_1.docm contient une macro VBA malveillante qui s'exécute à la fermeture du document via la commande AutoClose
La macro lance un script PowerShell encodé en Base64, conçu pour télécharger des charges supplémentaires à partir d'un serveur externe via l'IP 107.189.8.58.

- Analyse des logs Elastic : Les logs Elastic montrent que l'utilisateur "RolandBlanc" sur la machine "DESKTOP-UUNV01D" a exécuté PowerShell pour établir une connexion avec l'adresse IP 107.189.8.58.

Indicateurs de compromission

Détaillez ici les éléments qui permettent d’identifier cette menace dans l'avenir. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

Indicateurs de compromission (IOCs)

IP malveillante : 107.189.8.58
URL malveillante : http://107.189.8.58:8088/admin/get.php
Processus suspect : powershell.exe

Hash des fichiers malveillants :
SHA256 : 1c10ddc82fc2799acd9a3ee2d9ca6f9733efe005866bdaf2a7ab6105f42d61ec
SHA1 : 32748377a75aa7faba3b556fa11bcfd86758fa54
MD5 : 4ecfb5cec0dc5455f038c5539e2949de

[*Insérez des captures d'écran démontrant la recherche d'IOCs*]

Actifs impactés

Détaillez ici les machines, applications et utilisateurs impactés par cette alerte. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

Machine impactée : DESKTOP-UUNV01D
Utilisateur : RolandBlanc
IP locale : 192.168.1.100

Informations supplémentaires

Remplissez le tableau avec les informations indiquées.

Source de l'alerte	Qualification de l'alerte *(faux positif ou incident vérifié)*	Justification de la qualification
Incident identifié suite à une pièce jointe suspecte dans un email.	*Incident vérifié*	*La pièce jointe contient une macro malveillante exécutant un script PowerShell et établissant une connexion à une IP malveillante.*

Alerte 2 : ***Un nombre élevé de requêtes HTTP bloquées par le Web Application Firewall (WAF)*** *suggèrent des tentatives d'exploitation de la vulnérabilité Log4Shell via des injections JNDI. Requêtes avec les chaînes ${jndi:ldap://...} et ${jndi:dns://...} identifiées. Sur 100 requêtes trouvées dans les logs, 39 ont été bloquées par le WAF (status 503).*

Risque : Elevé

Détails d'investigation

Reportez ici la chronologie de l'attaque et les détails techniques. Ajoutez ou enlevez des points au besoin.

Plus d'informations en consultant le rapport associé à cette alerte.

IP 78.34.3.1 : Utilisée dans des requêtes LDAP. Signalé non malveillante sur Virustotal.
graffa.basics-shelter.corp : Tentatives de contact via DNS.
grecofood.com : Associé à l'IP 74.208.236.236 (hébergée par IONOS SE), non signalée comme malveillante par VirusTotal. Impliquée dans les tentatives d'exploitation de Log4Shell via JNDI, détectées dans les logs analysés.
Résolution des domaines : L'IP 74.208.236.236 a résolu plusieurs domaines.
Analyse de ce domaine (Virustotal) : Non malveillant.mais ses résolutions DNS passées incluent des adresses IP malveillantes (99.83.154.118, 198.54.117.199, 198.54.117.198, 198.54.117.197, 198.54.117.200, 162.255.119.68, et 203.170.82.73.)

Détaillez ici les éléments qui permettent d'identifier cette menace dans l'avenir. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

Chaînes malveillantes : ${jndi:ldap://...} et ${jndi:dns://...}.
IP suspectes : 78.34.3.1 (LDAP) et 74.208.236.236 (associé à des domaines passés liés à des tentatives de reconnaissance ou d'attaque).
Domaines suspects : graffa.basics-shelter.corp et grecofood.com.
Ips non bloquées par le wad : 89.12.180.216 - 86.246.66.199 - 54.71.99.184 - 212.6.39.132 - 108.177.18.197 - 91.65.34.195 - 93.66.84.155 - 13.37.213.116 - 5.20.12.48 - 92.177.225.197 - 156.200.122.222 - 34.242.179.93 - 79.146.134.209 - 34.201.141.138 - 83.159.94.173 - 52.18.55.16 - 185.73.204.8 - 79.112.20.12 - 37.223.37.88 - 51.255.49.229 - 82.163.203.42 - 185.73.204.8

Actifs impactés

Détaillez ici les machines, applications et utilisateurs impactés par cette alerte. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

Ces domaines sont associés aux tentatives de contact avec des serveurs externes, ce qui pourrait être lié à des tentatives d'exploitation de vulnérabilité, comme dans le cas de la vulnérabilité Log4Shell :

app.crackot.co
product.crackot.co
faq.crackot.co
partners.crackot.co
gateway.crackot.co
hello.crackot.co
a.crackot.co
api.crackot.co

Informations supplémentaires

Remplissez le tableau avec les informations indiquées.

Source de l’alerte	Qualification de l’alerte *(faux positif ou incident vérifié)*	Justification de la qualification
Logs des requêtes HTTP analysées dans Elastic.	*Incident vérifié*	*Le nombre élevé de tentatives d'exploitation bloquées (avec certaines réussies) indique qu'il s'agit d'une attaque active ciblant la vulnérabilité Log4j.*

Alerte 3 : ***Un employé de la division recrutement a signalé des activités anormales sur son poste de travail*** *, tels que l'activation inopinée de la caméra et des fenêtres de commande qui apparaissent et disparaissent. L'analyse du fichier PCAP et des logs a permis d'identifier des connexions sortantes suspectes.*

Risque : Elevé

Détails d'investigation

Reportez ici la chronologie de l'attaque et les détails techniques. Ajoutez ou enlevez des points au besoin.

Plus d'informations en consultant le rapport associé à cette alerte.

Machines impliquées :

- DESKTOP-O6CSQRA (IP locale 192.168.1.35) : -> 101.43.190.181 - Malveillante
  -> 209.197.3.8 - Associée à des fichiers malveillants

- DESKTOP-UUNV01D (IP locale 192.168.1.100) : -> 107.189.8.58 - Malveillante

Indicateurs de compromission

Détaillez ici les éléments qui permettent d'identifier cette menace dans l'avenir. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

- **IP malveillantes :**
  101.43.190.181 (Chine)
  107.189.8.58 (Luxembourg)
  209.197.3.8 (USA, StackPath)
- **Fichier malveillant :** facture_edf_1.docm
- **Hash (lié à mshta.exe, potentiel PowerShell) :**
  SHA-256 : 7762a4766bc394b4cb2d658144b207183ff23b3139181cd74e615db63e6e57d6
- **URL :** http://107.189.8.58:8088/admin/get.php
- **User-Agent :** Mozilla/5.0

Actifs impactés

Détaillez ici les machines, applications et utilisateurs impactés par cette alerte. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

Machines impactées :

- DESKTOP-O6CSQRA - (IP: 192.168.1.35 - Utilisateur : PrinGbedjinou)
- DESKTOP-UUNV01D - (IP: 192.168.1.100 - Utilisateur : RolandBlanc)

.

Informations supplémentaires

Remplissez le tableau avec les informations indiquées.

Source de l’alerte	Qualification de l’alerte *(faux positif ou incident vérifié)*	Justification de la qualification
Un employé de la division recrutement a signalé des activités anormales sur son poste de travail ,	*Incident vérifié*	*Les connexions sortantes suspectes, identifiées dans les logs et via le fichier PCAP, ont permis de déterminer que les machines DESKTOP-O6CSQRA et DESKTOP-UUNV01D ont été compromises via des malwares contrôlés à distance.*