Malware

Dickerson JAJOUTE

IPSSI - MCS4 27.4

Qu’est-ce qu’un malware ?

Un malware est l’abréviation de malicious software , c’est un programme conçu pour nuire ou agir sans accord sur un appareil ou un réseau.

Exemples de ce qu’un malware peut faire :

- voler des données (mots de passe, fichiers, infos bancaires),
- espionner (keylogger, micro/caméra, messages),
- bloquer/chiffrer des fichiers (ransomware),
- détruire ou modifier des données,
- prendre le contrôle de la machine à distance,
- utiliser ton appareil pour attaquer d’autres (botnet).

Pegasus

Pegasus est un logiciel espion (spyware) attribué à la société israélienne NSO Group, conçu pour infiltrer des smartphones et permettre une surveillance très intrusive d’une cible. Une fois installé, il peut donner accès à une grande partie de la vie numérique de la personne : messages, appels, contacts, photos, localisation, et dans certains cas activer le micro ou la caméra. Pegasus est particulièrement connu parce qu’il a été associé à des infections discrètes, parfois sans action visible de l’utilisateur ce qui rend la détection difficile.

Le nom Pegasus est devenu célèbre à partir de révélations et d’enquêtes journalistiques qui ont mis en avant son utilisation présumée contre des journalistes, militants, opposants politiques ou avocats dans plusieurs pays. Ces affaires ont déclenché un débat important sur l’encadrement des outils de surveillance : d’un côté, certains gouvernements expliquent qu’ils servent à lutter contre le crime organisé et le terrorisme ; de l’autre, des ONG et chercheurs en cybersécurité alertent sur les risques d’abus, le manque de transparence et l’atteinte aux droits fondamentaux (vie privée, liberté de la presse, droit à un procès équitable).

Sur le plan de la cybersécurité, Pegasus illustre la puissance des chaînes d’exploitation de failles logicielles sur mobile, ainsi que l’importance des mises à jour régulières et des mécanismes de défense des systèmes (durcissement, sandboxing, protections mémoire). Il rappelle aussi que la sécurité des appareils dépend autant des correctifs techniques que du

contrôle démocratique et juridique de l’usage de technologies capables de transformer un téléphone en outil de surveillance permanente.

Comment s’en protéger ?

Pour réduire le risque d’attaque liée à Pegasus, la mesure la plus importante est de maintenir son smartphone à jour, car ce type de logiciel espion exploite souvent des failles corrigées par les mises à jour de sécurité. Il est aussi recommandé de limiter au maximum la surface d’attaque en évitant d’installer des applications inutiles ou provenant de sources non fiables, et en contrôlant les autorisations accordées aux applications, notamment l’accès au micro, à la caméra et à la localisation. Dans un contexte professionnel ou pour des personnes exposées, l’utilisation de solutions de gestion et de sécurité mobile, ainsi que des audits réguliers, permettent de mieux détecter des comportements anormaux et de réagir plus vite. Globalement, Pegasus rappelle que la meilleure protection repose sur une hygiène numérique stricte et une mise à jour constante du système.

LockBit

LockBit est un ransomware qui s'est imposé à partir de 2019 comme l'une des opérations de ransomware les plus actives au monde. Son modèle repose sur le "Ransomware as a Service." Un groupe principal développe le logiciel malveillant, gère l'infrastructure et les paiements, et des affiliés réalisent les intrusions chez les victimes puis partagent les gains.

Une attaque suit souvent une chaîne en plusieurs étapes. Les attaquants obtiennent un accès initial, se déplacent dans le réseau, volent des données, puis chiffrent les systèmes pour perturber l'activité. LockBit est connu pour la double extorsion. Même si une organisation restaure ses fichiers, les attaquants menacent de publier les données dérobées si la rançon n'est pas payée. L'objectif est de maximiser la pression en combinant arrêt de production et risque juridique ou réputationnel.

LockBit a marqué le paysage de la cybersécurité par sa professionnalisation, avec un programme d'affiliation, un support aux affiliés, des versions successives et une communication agressive. Cette industrialisation illustre la transformation du ransomware en une économie structurée, où la technique, l'infrastructure et la négociation sont réparties entre acteurs spécialisés.

En février 2024, une opération internationale coordonnée a perturbé l'infrastructure de LockBit, avec des actions menées dans plusieurs pays. D'autres actions publiques et procédures judiciaires ont ensuite visé des membres ou rôles clés présumés.

Pour réduire le risque de ransomware, les mesures essentielles sont la mise à jour régulière des systèmes, l'activation de l'authentification multifacteur sur les accès distants, la segmentation du réseau, des sauvegardes hors ligne testées et une supervision permettant de détecter l'exfiltration de données et le chiffrement massif.

Comment s'en protéger ?

Pour se protéger contre LockBit et les ransomwares en général, l'objectif principal est d'empêcher l'intrusion et de limiter l'impact si une infection survient. La première ligne de défense consiste à mettre à jour les systèmes et logiciels afin de réduire les failles exploitables et à sécuriser les accès, notamment en activant l'authentification multifacteur sur les comptes sensibles et les connexions à distance. Ensuite, il est essentiel de disposer de sauvegardes hors ligne ou isolées, régulièrement testées, car elles permettent de restaurer l'activité sans dépendre d'une rançon. La segmentation du réseau et la limitation des droits des utilisateurs réduisent aussi la propagation du malware. Enfin, une supervision des journaux et des alertes de sécurité aide à repérer rapidement des signes comme une exfiltration de données ou un chiffrement massif, ce qui permet d'isoler les machines à temps et de déclencher un plan de réponse à incident.

Conclusion

En conclusion, les malwares représentent une menace majeure car ils peuvent viser aussi bien des individus que des organisations, avec des objectifs très différents. Pegasus montre une forme d'attaque discrète et ciblée, centrée sur l'espionnage et l'atteinte à la vie privée, tandis que LockBit illustre une cybercriminalité organisée cherchant surtout un gain financier en paralysant des systèmes et en menaçant de divulguer des données. Ces deux exemples prouvent que les attaques ne reposent pas seulement sur la technologie, mais aussi sur les failles humaines, l'organisation des réseaux et le manque de mises à jour. Face à cela, la meilleure défense repose sur une hygiène numérique constante, des protections adaptées et une bonne préparation, afin de réduire les risques et de réagir efficacement en cas d'incident