AYI NEDJIMI Consultants

Quand les défenseurs passent à l'attaque : leçons de l'affaire ALPHV

Catégorie : Cybersécurité Générale Lecture : 7 min Publié le : 02/04/2026 Auteur : Ayi NEDJIMI

Deux experts cyber condamnés pour des attaques ALPHV/BlackCat. Analyse des risques liés aux prestataires de confiance et recommandations pour renforcer vos contrôles.

Deux professionnels de la cybersécurité — un incident responder et un négociateur ransomware — viennent de plaider coupable pour avoir mené des attaques avec ALPHV/BlackCat. L'affaire pose une question dérangeante : et si la menace la plus difficile à détecter venait de l'intérieur même de l'écosystème de défense ?

Les faits qui dérangent

L'affaire est inédite par sa nature. Goldberg, 40 ans, était incident responder chez Sygnia — une des firmes les plus respectées du secteur. Martin, 36 ans, était négociateur ransomware chez DigitalMint, intervenant directement avec les victimes pour gérer le paiement des rançons. Entre avril et décembre 2023, les deux hommes et un complice ont mené des attaques ALPHV/BlackCat contre des organisations américaines, empochant au moins 1,2 million de dollars en Bitcoin sur une seule victime. Ils ont plaidé coupable de conspiration en vue d'extorsion et risquent jusqu'à 20 ans de prison.

Ce qui rend cette affaire unique, c'est le niveau d'accès et de connaissance dont disposaient ces individus. Un incident responder connaît les playbooks de détection, les outils EDR déployés, les faiblesses des architectures qu'il audite. Un négociateur connaît les seuils de paiement, les polices d'assurance cyber, les points de rupture psychologiques des victimes. Ces connaissances, normalement au service de la défense, deviennent des armes redoutables une fois retournées.

Le problème structurel du secteur

Cette affaire n'est pas un cas isolé — c'est un symptôme. Le marché de la cybersécurité repose sur une confiance implicite : on donne aux défenseurs un accès total à nos systèmes, nos données, nos vulnérabilités. Un pentester voit tout. Un incident responder accède aux logs, aux backups, aux credentials. Un négociateur connaît la capacité financière exacte de la victime. Cette confiance est rarement formalisée au-delà d'un NDA et d'une clause de confidentialité dans un contrat de prestation.

Le secteur manque cruellement de mécanismes de contrôle interne pour ses propres praticiens. Les certifications (CISSP, OSCP, GIAC) valident des compétences techniques, pas l'intégrité. Les background checks sont souvent superficiels. Et surtout, la rotation des prestataires est telle qu'un même individu peut intervenir chez des dizaines de clients en quelques mois, accumulant une connaissance exploitable considérable.

Ce que ça change pour les RSSI

Si vous êtes RSSI ou dirigeant, cette affaire devrait modifier votre approche de la gestion des tiers de confiance. Premièrement, le principe du moindre privilège ne s'applique pas qu'aux comptes techniques — il doit aussi encadrer l'accès des prestataires humains. Un incident responder n'a pas besoin d'un accès permanent à votre SIEM. Un pentester n'a pas besoin de conserver les rapports sur son laptop personnel.

Deuxièmement, la traçabilité des actions des prestataires doit être systématique et indépendante. Si votre incident responder désactive un log pour « faciliter l'investigation », qui le vérifie ? Les sessions PAM (Privileged Access Management) enregistrées, les comptes nominatifs temporaires et les revues post-intervention ne sont pas du luxe — ce sont des nécessités.

Troisièmement, diversifiez vos prestataires et cloisonnez les informations. Le même cabinet ne devrait pas gérer votre pentest, votre incident response et votre négociation ransomware. C'est du bon sens, mais la réalité du marché pousse à la concentration.

Mon avis d'expert
Je travaille dans ce secteur depuis suffisamment longtemps pour savoir que la grande majorité des professionnels de la cybersécurité sont intègres et passionnés. Mais l'affaire Goldberg-Martin révèle une faille systémique que notre industrie refuse de regarder en face : nous exigeons de nos clients une hygiène de sécurité irréprochable tout en fonctionnant nous-mêmes sur un modèle de confiance aveugle. Le jour où un incident responder véreux exfiltre les données d'un client français du CAC 40, on ne pourra pas dire qu'on ne savait pas. Il est temps d'appliquer à notre propre écosystème les principes que nous prêchons : zero trust, moindre privilège, traçabilité complète.

Conclusion

L'affaire ALPHV n'est pas qu'un fait divers judiciaire. C'est un signal d'alarme pour tout l'écosystème cyber. Les organisations doivent repenser la confiance accordée à leurs prestataires de sécurité avec la même rigueur qu'elles appliquent à leurs propres employés — voire davantage, compte tenu du niveau d'accès accordé. La cybersécurité ne peut pas se permettre d'être le cordonnier mal chaussé.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr