LOLBins réseau : quand vos équipements deviennent vos pires ennemis

> FortiBleed a exposé une vérité inconfortable : les attaquants n'ont plus besoin d'exploits complexes quand ils abusent des outils natifs de vos pare-feux....

FortiBleed n'aurait pas dû être possible. L'outil utilisé pour voler 105 millions de credentials sur 430 000 pare-feux ne contient aucun exploit, aucune shellcode, aucun malware détectable. Il exécute une seule commande : `diagnose sniffer packet` — une commande que vos administrateurs réseau tapent chaque semaine pour déboguer des problèmes de connectivité. C'est ça, le Living off the Land appliqué aux équipements réseau. Et vos défenses sont probablement aveugles à cette catégorie d'attaque.

Points clés à retenir

- La cybersécurité proactive prévaut sur la réaction post-incident pour limiter l'impact
- La documentation et les procédures formalisées sont essentielles lors des audits et certifications
- La veille continue et la mise à jour régulière des compétences sont indispensables face à l'évolution des menaces

Le concept de Living off the Land (LotL) a émergé dans la communauté sécurité autour de 2012-2014, popularisé par l'analyse de campagnes d'espionnage attribuées à des groupes APT étatiques, notamment dans les leaks du Shadow Brokers révélant les outils de la NSA TAO. L'idée fondamentale est d'une simplicité désarmante : pourquoi apporter vos propres outils quand l'environnement cible en fournit de bien meilleurs, déjà présents, déjà signés, déjà autorisés par toutes vos politiques de sécurité ?

⚡ **Retour terrain**

Dans mes missions d'audit, je rencontre régulièrement la même configuration à risque : des règles de firewall héritées depuis 5 à 10 ans, que personne n'ose supprimer par crainte de casser quelque chose. J'ai développé une méthode de nettoyage progressive — analyser les logs de connexion sur 90 jours, identifier les règles sans trafic, les désactiver sans

supprimer pendant 30 jours, puis valider avec les équipes métier. Sur un parc de 340 règles dans un groupe logistique, nous en avons supprimé 218 sans incident.

Sur les systèmes Windows, le Living off the Land — souvent abrégé LOLBins pour Living off the Land Binaries — s'est d'abord matérialisé autour d'un ensemble d'outils système légitimes détournés à des fins malveillantes. PowerShell en premier lieu : capable d'exécuter du code arbitraire, de télécharger des charges depuis Internet, de se connecter à des services C2, d'accéder au registre et aux certificats, tout en étant signé Microsoft et donc généralement whitelisté dans les politiques de sécurité. WMI (Windows Management Instrumentation) permet la persistance, l'exécution à distance et l'exfiltration de données de configuration. Certutil.exe permet le téléchargement de fichiers depuis Internet déguisé en opération de gestion de certificats. BITSAdmin réalise des transferts de fichiers en arrière-plan sans alerte réseau. Regsvr32 exécute du code arbitraire via l'enregistrement de COM. La liste des LOLBAS (Living Off The Land Binaries And Scripts) documentés dans le projet communautaire du même nom compte aujourd'hui plus de 200 entrées, chacune correspondant à un outil légitime Windows qui peut être détourné à des fins offensives.

L'efficacité de cette approche est documentée par chaque grand rapport de threat intelligence des cinq dernières années. Selon le rapport M-Trends 2025 de Mandiant, 73 % des intrusions avancées investiguées en 2024 comprenaient au moins une phase utilisant des LOLBins. Le rapport CrowdStrike 2026 Global Threat Report indique que le "malware-free activity" — les attaques sans dépose de fichier malveillant traditionnel — représente désormais 79 % des détections d'intrusion initiale. La raison est structurelle : les LOLBins contournent les défenses basées sur les signatures antivirales et les règles de whitelisting applicatif, car les binaires sont légitimes par définition. Détecter un usage malveillant de PowerShell nécessite une analyse comportementale — ce que seul un EDR moderne peut faire — et non une détection sur signature.

La progression naturelle a conduit les attaquants à étendre cette logique au-delà des LOLBins Windows classiques : aux macros Microsoft Office (VBA, XLSM), aux scripts bash et Python sur Linux, aux outils de monitoring et de déploiement légitimes (PSExec, Atera, AnyDesk), et aux outils de sécurité eux-mêmes (la vulnérabilité BlueHammer, qui ciblait Microsoft Defender pour en faire un vecteur de déploiement ransomware, en est l'illustration parfaite). Mais la

dernière évolution — et la plus préoccupante — est l'extension de la logique LotL aux équipements réseau eux-mêmes : pare-feux, routeurs, switches, sondes de monitoring. FortiBleed en est la démonstration la plus visible à ce jour. Ce n'est pas la première. Ce ne sera pas la dernière.

Pourquoi les équipements réseau sont le terrain LOL idéal

Les équipements réseau réunissent une convergence de caractéristiques qui les rendent particulièrement attractifs pour la stratégie Living off the Land étendue à l'infrastructure. Comprendre précisément pourquoi est indispensable pour construire une défense adaptée — et pour convaincre les équipes dirigeantes que ces équipements méritent le même niveau d'attention sécurité que les serveurs Windows.

L'absence d'agents de sécurité endpoint. Les pare-feux Fortinet, les routeurs Cisco, les appliances Palo Alto et Juniper fonctionnent sur des systèmes d'exploitation propriétaires — FortiOS, IOS-XE, PAN-OS, Junos — qui ne supportent pas l'installation d'agents EDR tiers. Pas de CrowdStrike Falcon sur votre FortiGate. Pas de Microsoft Defender sur votre Cisco ASA. Pas de SentinelOne sur votre Palo Alto. Cette contrainte architecturale est fondamentale : elle signifie que l'ensemble des couches de détection comportementale qui fonctionnent sur vos serveurs et postes de travail sont simplement absentes sur vos équipements réseau. Un attaquant qui opère depuis un FortiGate compromis est invisible pour votre EDR.

Des privilèges natifs d'une puissance exceptionnelle. Un compte administrateur sur un FortiGate ou un routeur Cisco de périmètre offre quelque chose qu'aucun compte domain admin Windows n'offre directement : le contrôle de l'ensemble du trafic réseau entrant et sortant de l'organisation, la capacité de modifier les règles de routage et de filtrage en temps réel, la possibilité de créer des tunnels VPN arbitraires vers des destinations externes, et l'accès CLI à des outils de capture et d'analyse de trafic. C'est le point de contrôle ultime de l'infrastructure réseau — et il est accessible à un nombre restreint d'administrateurs dont les pratiques de sécurité des comptes sont rarement soumises au même niveau de rigueur que les comptes domain admin.

Des outils natifs d'une richesse fonctionnelle considérable. FortiOS dispose de `diagnose sniffer packet`. Cisco IOS dispose de `debug ip packet` et d'embedded packet captures accessibles via ASDM. Junos dispose de `monitor traffic`. MikroTik RouterOS — massivement déployé dans les PME françaises — dispose de `/tool sniffer` qui peut capturer le trafic sur toutes les interfaces et l'exporter automatiquement vers un serveur distant en temps réel. Ces outils existent pour des raisons légitimes et indispensables : le diagnostic réseau en production requiert la capacité d'inspecter le trafic. Mais ils constituent également des armes d'exfiltration massives entre les mains d'un attaquant ayant obtenu un accès admin. Et leur usage ne génère pas d'alerte par défaut — car il est légitime.

La position architecturale centrale. Le pare-feu de périmètre et le routeur de sortie Internet sont par définition les équipements par lesquels transite l'ensemble du trafic entrant et sortant. Déployez un sniffer sur un serveur Windows compromis, et vous capturez le trafic de ce serveur. Déployez-le sur le FortiGate, et vous capturez potentiellement l'intégralité du trafic de l'organisation — VPN SSL, authentifications Active Directory, sessions de gestion des systèmes critiques, communications avec les fournisseurs et partenaires. La valeur stratégique d'un équipement réseau compromis est structurellement supérieure à celle d'un serveur compromis.

Une cinétique d'attaque invisible aux défenses traditionnelles. FortigateSniffer n'a déposé aucun fichier malveillant sur les systèmes compromis, n'a exécuté aucun code détectable par un antivirus, et n'a généré aucune alerte SIEM classique — parce que chaque action qu'il a réalisée correspondait à une commande légitime et documentée dans le manuel FortiOS. La détection nécessite de savoir à l'avance ce qui est "anormal" dans l'usage de ces commandes, et d'avoir mis en place le monitoring granulaire qui permet de l'observer. La grande majorité des organisations n'ont fait ni l'un ni l'autre.

FortiBleed : anatomie détaillée d'une attaque LOL-réseau industrialisée

Déconstruire FortiBleed phase par phase permet de comprendre concrètement comment la logique Living off the Land s'applique à l'infrastructure réseau — et d'identifier où se situent les points de détection possibles que les équipes sécurité auraient pu activer.

Phase 1 — Accès initial par credential stuffing. Les attaquants n'ont exploité aucune vulnérabilité technique sur FortiGate pour obtenir leur accès initial. Ils ont utilisé trois vecteurs : credential stuffing à partir de bases de données d'identifiants issues des fuites de configuration FortiGate de 2024 et 2025 (plusieurs dizaines de milliers de configurations incluant des identifiants administrateurs avaient été publiées sur des forums cybercriminels), force brute sur des comptes sans politique de complexité de mot de passe, et réutilisation de credentials volés dans d'autres incidents. La porte d'entrée était simplement une hygiène insuffisante des credentials — le problème de sécurité le plus vieux du monde, et toujours le plus répandu. Point de détection potentiel : logs d'authentification FortiGate avec alertes sur les tentatives répétées depuis des IP inhabituelles. Combien d'organisations avaient activé cette surveillance ? Les données de l'incident suggèrent : très peu.

Phase 2 — Déploiement du sniffer via commandes natives. Une fois l'accès admin FortiGate obtenu, FortigateSniffer exécute via SSH la commande `diagnose sniffer packet any 'port 88 or port 389 or port 636 or port 1812 or port 3389 or port 1433' 6` — capturant les ports des principaux protocoles d'authentification d'entreprise avec verbosité maximale (payloads complets). L'outil orchestrait cette capture sur 659 instances FortiGate en parallèle, agrégait les résultats dans une base de données centralisée, et en extrayait automatiquement les credentials. Point de détection potentiel : un SIEM recevant les logs CLI FortiOS et disposant d'une règle alertant sur les exécutions longue durée de `diagnose sniffer packet` sur des ports d'authentification. Nombre d'organisations disposant de cette règle : quasi-zéro selon mon expérience terrain.

Phase 3 — Exploitation des credentials et déploiement ransomware. Les 105 millions de credentials capturés ont été organisés par organisation, par protocole et par niveau de privilège apparent. Pour les 409 organisations où des credentials Domain Admin ont été identifiés, les attaquants ont utilisé le VPN FortiGate compromis comme tunnel d'accès vers le réseau interne, puis déployé INC Ransom ou Lynx sur l'infrastructure interne. Le délai entre la capture des credentials et le déploiement du ransomware était typiquement de 48 à 96 heures — largement dans la fenêtre d'opacité d'un SOC qui ne surveille pas ses équipements réseau en temps réel.

Ce qui rend FortiBleed particulièrement instructif pour les équipes sécurité est l'industrialisation de la phase 2. Déployer un sniffer sur un FortiGate est une action manuelle banale réalisée régulièrement par les équipes réseau. FortigateSniffer l'a automatisée et parallélisée sur des

centaines d'instances simultanément. L'attaque est scalable, silencieuse, et utilise exclusivement des outils légitimes. C'est la définition parfaite d'un LOLBin appliqué à l'infrastructure réseau.

Les autres équipements réseau exposés à la même logique

FortiBleed serait une anomalie si les fonctionnalités qu'il exploite étaient propres à Fortinet. Elles ne le sont pas. L'ensemble des équipements réseau professionnels disposent de capacités similaires — c'est une nécessité fonctionnelle pour le diagnostic réseau — et tous peuvent être détournés selon la même logique d'un attaquant suffisamment habile.

Cisco IOS et IOS-XE sont les systèmes d'exploitation réseau les plus déployés au monde, largement présents dans les grandes entreprises et les administrations françaises. La commande `debug ip packet detail` sur un routeur Cisco capture l'intégralité du trafic IP en transit avec les payloads. L'interface ASDM des Cisco ASA offre une interface graphique de capture de paquets exportable en format PCAP vers un serveur FTP ou TFTP intégré via `copy capture: ftp://`. Un attaquant avec un accès enable (niveau 15) peut capturer et exfiltrer silencieusement le trafic transitant par l'équipement, sans déposer le moindre fichier externe.

Palo Alto Networks PAN-OS, utilisé dans de nombreux environnements enterprise français, intègre une fonctionnalité de packet capture accessible via la GUI (Monitor > Packet Capture) et via la CLI via `tcpdump` dans le shell Linux sous-jacent accessible en mode debug. Un accès administrateur PAN-OS permet de démarrer une capture sur toutes les interfaces simultanément et de l'exporter vers un serveur FTP ou SCP externe. Même fonctionnalité, même risque.

MikroTik RouterOS mérite une attention particulière dans le contexte français : c'est le système d'exploitation réseau dominant dans les TPE/PME, une large partie des installations WISP et de nombreux hébergeurs. L'outil `/tool sniffer` de RouterOS permet de capturer le trafic sur toutes les interfaces et de le streamer automatiquement vers un serveur TZSP (TaZmen Sniffer Protocol) distant en temps réel, de manière totalement silencieuse du point de vue des systèmes surveillés. La campagne Cyclops Blink de 2022, attribuée au groupe russe Sandworm, avait précisément ciblé les MikroTik comme infrastructure de C2 — FortiBleed représente l'évolution logique : les équipements réseau comme outils d'exfiltration de credentials à grande échelle.

Les switches de niveau 3 (Cisco Catalyst, Juniper EX, Aruba) disposent de fonctionnalités SPAN (Switched Port Analyzer) et RSPAN (Remote SPAN) qui permettent de dupliquer le trafic d'un ou plusieurs ports vers un port de surveillance. Un attaquant ayant accès à la gestion d'un switch peut configurer un RSPAN pour envoyer une copie de l'ensemble du trafic d'un VLAN vers une interface contrôlée par l'attaquant, installée sur un serveur externe. Fonctionnalité légitime de diagnostic, arme redoutable entre de mauvaises mains, et invisible pour les outils de sécurité traditionnels.

L'angle mort structurel de vos défenses actuelles

La plupart des architectures de sécurité défensives ont été conçues pour protéger les serveurs et les postes de travail. Elles présentent des angles morts structurels vis-à-vis des attaques LOL-réseau, et ces angles morts ne se résolvent pas avec des outils supplémentaires si la télémétrie de base n'est pas en place.

Absence de télémétrie CLI réseau dans les SIEM. La grande majorité des déploiements SIEM ingèrent des logs syslog réseau (connexions, règles firewall matchées, alertes IDS/IPS) mais pas le détail des commandes CLI exécutées sur les équipements. Pour que les commandes FortiOS soient visibles dans un SIEM, il faut avoir préalablement configuré une journalisation granulaire des sessions CLI sur FortiGate via `config log syslogd setting` avec les options de log CLI, et avoir créé des règles de corrélation SIEM spécifiques. Dans mon expérience terrain d'audit, moins de 10 % des organisations que j'examine ont mis en place cette surveillance.

Absence de baseline comportemental sur les équipements réseau. Pour détecter que `diagnose sniffer packet` est exécuté de manière anormale — longue durée, capture sur des protocoles d'authentification, à des horaires inhabituels — il faut d'abord avoir défini ce qu'est une utilisation normale de cette commande dans votre environnement spécifique. Combien d'organisations ont réalisé ce travail de baselining comportemental sur leurs FortiGate ou leurs routeurs Cisco ? Dans ma pratique, quasi-aucune.

Ségrégation insuffisante des rôles sur les équipements réseau. Dans la majorité des organisations françaises de taille PME à ETI, les mêmes comptes administrateurs sont utilisés

pour configurer les règles de pare-feu, gérer les certificats VPN, et effectuer le diagnostic réseau. Il n'existe pas de principe de moindre privilège appliqué au niveau CLI réseau : soit vous avez un accès admin complet, soit vous n'avez aucun accès. Cette absence de granularité signifie qu'un credential administrateur compromis donne accès à toutes les fonctionnalités de l'équipement, y compris les plus dangereuses comme la capture de trafic.

La fausse sécurité liée au monitoring réseau traditionnel. Les outils de monitoring réseau (PRTG, Nagios, LibreNMS, Zabbix) surveillent la disponibilité, les performances et les volumes de trafic — mais pas le comportement CLI des équipements. Un FortiGate 100 % disponible avec des performances nominales peut très bien exfiltrer des credentials en arrière-plan depuis des semaines sans que votre NMS déclenche la moindre alerte. La disponibilité et les performances ne sont pas des indicateurs de sécurité.

Détecter et se défendre : le guide opérationnel

La bonne nouvelle est que les LOLBins réseau sont détectables et défendables. Cela nécessite des actions spécifiques qui ne font généralement pas partie des programmes de sécurité standard — mais toutes réalisables avec des ressources raisonnables, y compris dans un contexte PME ou ETI.

Journalisation CLI centralisée — la priorité absolue. Activer la journalisation granulaire des sessions CLI sur tous les équipements réseau critiques et centraliser ces logs dans le SIEM. Sur FortiGate : `config log syslogd setting` avec `set status enable` et configuration des filtres pour inclure les événements de type `cli-cmd`. Sur Cisco IOS : `archive log config` avec envoi vers un serveur syslog centralisé. Sur MikroTik : configuration du logging vers un serveur Syslog distant avec niveau "debug". L'objectif est que chaque commande exécutée en CLI sur vos équipements critiques soit visible dans votre SIEM dans les secondes qui suivent. Sans cette télémétrie, toute autre mesure de détection est construite sur du vide.

Règles de détection SIEM spécifiques aux commandes réseau sensibles. Une fois la télémétrie CLI disponible, créer des règles de détection adaptées. Pour FortiGate : alerte sur toute exécution de `diagnose sniffer packet` durant plus de 60 secondes (un usage légitime de debug

ponctuel dure rarement plus), ou capturant les ports d'authentification (88, 389, 636, 1812, 3268, 3389, 1433). Pour Cisco IOS : alerte sur `debug ip packet` activé en dehors des fenêtres de maintenance documentées. Pour MikroTik : alerte sur toute configuration de `/tool sniffer` avec une destination de streaming externe. Ces règles utilisent votre SIEM existant avec une nouvelle source de données — elles n'exigent pas d'outil supplémentaire.

MFA sur toutes les interfaces d'administration réseau — non négociable. Le vecteur d'accès initial de FortiBleed était des credentials faibles ou réutilisés. L'authentification multifacteur sur les interfaces d'administration FortiGate, les accès SSH aux équipements Cisco, et les portails de gestion réseau est la mesure la plus impactante par rapport à l'effort requis pour l'implémenter. Les solutions RADIUS avec MFA (Cisco ISE, FreeRADIUS combiné à un OTP, ou les services MFA cloud comme Microsoft Entra) s'intègrent avec tout équipement réseau supportant RADIUS — ce qui inclut tous les équipements cités dans cet article. Si vous ne devez retenir qu'une action de cet article, c'est celle-ci.

Séparation des rôles et moindre privilège sur les équipements réseau. Créer des profils administrateurs distincts sur vos équipements : un profil "configuration" (gestion des règles, des VPN, des interfaces) sans accès aux outils de diagnostic CLI avancés, et un profil "debug" avec accès aux outils de capture uniquement dans le cadre de procédures de diagnostic formalisées, avec logging renforcé. FortiGate supporte les profils d'administrateur avec restriction de commandes via `config system accprofile`. Cisco IOS supporte les niveaux de privilège (1-15) avec des commandes assignées à chaque niveau par configuration.

NDR sur le trafic des interfaces de gestion. Un outil NDR (Network Detection and Response) placé en dérivation (TAP) sur les liens de gestion out-of-band de vos équipements réseau peut détecter des connexions sortantes anormales : transferts de fichiers PCAP vers des IP externes inconnues, sessions SFTP/FTP non documentées, trafic TZSP vers des destinations non répertoriées. Cette couche de détection est complémentaire à la journalisation CLI et peut détecter des exfiltrations même en l'absence de logs CLI disponibles.

ZTNA pour remplacer progressivement les VPN exposés. La migration vers une architecture Zero Trust Network Access (ZTNA) — où l'accès aux ressources internes est conditionné à l'identité de l'utilisateur, à l'état de santé du terminal, et au contexte de la requête plutôt qu'à l'appartenance au réseau VPN — réduit structurellement l'exposition liée aux credentials VPN compromis. Si votre VPN SSL FortiGate est remplacé par un accès ZTNA, les credentials volés par une campagne de type FortiBleed ne permettent plus d'accéder directement à votre réseau

interne. Cette migration est structurelle et prend du temps, mais elle élimine la classe d'attaque entière plutôt que d'en mitiger les symptômes.

AVIS DrXPERT

Mon avis d'expert

FortiBleed est révélateur d'un problème de gouvernance sécurité que je constate systématiquement dans les audits que je réalise : les équipements réseau sont les enfants pauvres de la sécurité défensive. On déploie des EDR sur chaque poste, des agents de sécurité sur chaque serveur, des règles SIEM sur chaque application — et on laisse les FortiGate et les Cisco tourner sans surveillance granulaire, avec des mots de passe recyclés et sans MFA, parce que "ce sont des équipements réseau, pas des serveurs". Cette distinction n'a plus de sens en 2026. Un FortiGate compromis est plus dangereux qu'un serveur compromis : il voit tout le trafic, il ouvre le réseau interne, et il ne génère aucune alerte dans vos outils de sécurité habituels. Si vous n'avez pas de MFA sur votre interface d'admin FortiGate aujourd'hui, c'est votre priorité numéro un — avant le prochain audit de conformité, avant la prochaine mise à jour de politique, avant tout.

Ce que FortiBleed change dans votre programme de sécurité

FortiBleed n'est pas un incident isolé — c'est le signal d'une maturation dans les stratégies d'attaque que vous reverrez, sous d'autres noms, sur d'autres équipements, dans les mois qui viennent. Les groupes qui opèrent FortiBleed, INC Ransom et Lynx ne sont pas des acteurs d'État avec des ressources illimitées. Ce sont des organisations cybercriminelles professionnelles qui ont industrialisé une approche d'une efficacité redoutable : compromettre les équipements réseau via des credentials faibles, utiliser les outils natifs pour voler massivement des credentials d'authentification, et déployer des ransomwares dans les organisations les plus lucratives identifiées dans le dataset volé. Cette chaîne est réplicable à grande échelle par des groupes de taille modeste — ce qui signifie que vous pouvez vous attendre à en voir d'autres variantes.

Concrètement, FortiBleed impose trois évolutions dans votre programme de sécurité : premièrement, inclure les équipements réseau dans votre périmètre de supervision sécurité au même titre que les serveurs (SIEM, logs CLI, revues de comptes) ; deuxièmement, appliquer aux équipements réseau les mêmes standards d'hygiène des comptes qu'aux serveurs critiques (MFA, rotation des mots de passe, moindre privilège) ; troisièmement, intégrer dans vos exercices de réponse à incident le scénario "notre équipement réseau est compromis et sert d'outil d'attaque depuis plusieurs semaines". Ce dernier point est souvent absent des playbooks de réponse à incident que j'examine — il doit maintenant y figurer.

La sécurité du périmètre réseau des années 2010 consistait à sécuriser l'infrastructure avec un bon pare-feu bien configuré. La sécurité réseau de 2026 inclut de sécuriser le pare-feu lui-même — en partant du principe qu'il est une cible aussi attractive que n'importe quel serveur critique de votre infrastructure.

À RETENIR

Points clés à retenir

Living off the Land : origines et évolution d'une technique qui a tout changé

Pourquoi les équipements réseau sont le terrain LOL idéal

FortiBleed : anatomie détaillée d'une attaque LOL-réseau industrialisée

Les autres équipements réseau exposés à la même logique

L'angle mort structurel de vos défenses actuelles

Sources et références

ANSSI — Bonnes pratiques de sécurité

CISA — Ressources cybersécurité

ENISA — Threat Landscape 2024