EternalBlue

Quand la NSA a armé internet

Stéphane FOSSE
fosse.fr

04 avril 2026

Résumé

EternalBlue est un exploit développé par la NSA américaine qui cible une vulnérabilité du protocole SMBv1 de Windows, référencée CVE-2017-0144. Conservé secret pendant cinq ans par l'agence, il a été volé puis publié sur internet par le groupe Shadow Brokers le 14 avril 2017. Trente jours plus tard, le ransomware WannaCry s'en emparait pour infecter 230 000 machines dans 150 pays. Six semaines après, NotPetya l'utilisait pour dévaster des pans entiers de l'économie mondiale, causant des dommages estimés à plus de 10 milliards de dollars.

Comment fonctionne la vulnérabilité SMBv1 qu'exploite EternalBlue ?

Le protocole SMB (Server Message Block) est le mécanisme standard de partage de fichiers et d'imprimantes sur les réseaux Windows. Sa première version, SMBv1, date de 1984 et n'a jamais été conçue pour résister à des attaques sophistiquées — elle était encore active par défaut dans Windows 7, Windows Server 2008 et même Windows 10 au moment des faits.

La vulnérabilité exploitée par EternalBlue se situe dans la fonction `srv!SrvOs2FeaListSizeToNt`, chargée de convertir les attributs étendus de fichiers (FEA, File Extended Attributes) du format OS/2 vers le format NT. Cette conversion souffre d'un bug de transtypage : lorsque la taille de la liste OS2FeaList dépasse la capacité d'un mot 16 bits, la fonction tronque incorrectement le calcul de taille. Le résultat : le tampon alloué pour la liste NtFeaList est bien plus petit que la quantité de données effectivement copiée dedans. C'est un débordement de tas classique dans le pool noyau non paginé de Windows.

Un second bug, qualifié d'erreur d'analyse (*wrong parsing function bug*), permet à l'attaquant de forcer ce chemin d'exécution en combinant un paquet SMB_COM_NT_TRANSACT suivi d'une séquence SMB_COM_TRANSACTION2_SECONDARY. Le serveur interprète alors la transaction finale comme un Trans2, perdant la trace du type initial et déclenchant la mauvaise fonction de conversion. La NSA, via son unité Tailored Access Operations (TAO), a réussi à transformer ce bug en exploit fiable en combinant trois vulnérabilités distinctes et une technique de *heap grooming* — le conditionnement préalable du tas noyau pour garantir que l'overflow écrase précisément la bonne structure mémoire.

Qu'est-ce que DoublePulsar, le backdoor qui accompagne EternalBlue ?

EternalBlue ouvre la porte ; DoublePulsar l'habite. Ces deux outils, développés conjointement par la NSA au sein du framework FuzzBunch, fonctionnent en tandem : EternalBlue livre l'exécution de code arbitraire en ring-0 (le niveau le plus privilégié du noyau), et son shellcode embarqué installe immédiatement DoublePulsar comme backdoor persistant.

DoublePulsar est un implant noyau d'une sophistication remarquable. Son shellcode, d'environ 3 600 octets, supporte nativement les architectures x86 et x64 via une astuce d'encodage assembleur : les mêmes premiers octets sont interprétés différemment selon l'architecture, permettant d'emprunter la bonne branche d'exécution sans détection. Une fois exécuté, le shellcode localise l'adresse de base de `ntoskrnl.exe` en remontant la table des descripteurs d'interruptions (IDT) depuis le registre KPCR, puis résout par hachage les adresses de `ExAllocatePool`, `ExFreePool` et `ZwQuerySystemInformation`. Il localise ensuite le pilote SMB `Srv.sys` en énumérant les modules chargés via `ZwQuerySystemInformation`.

La dernière étape est la plus élégante : DoublePulsar remplace silencieusement le pointeur de fonction `SrvTransactionNotImplemented` dans le tableau `SrvTransaction2DispatchTable` (à l'index 14) par un hook

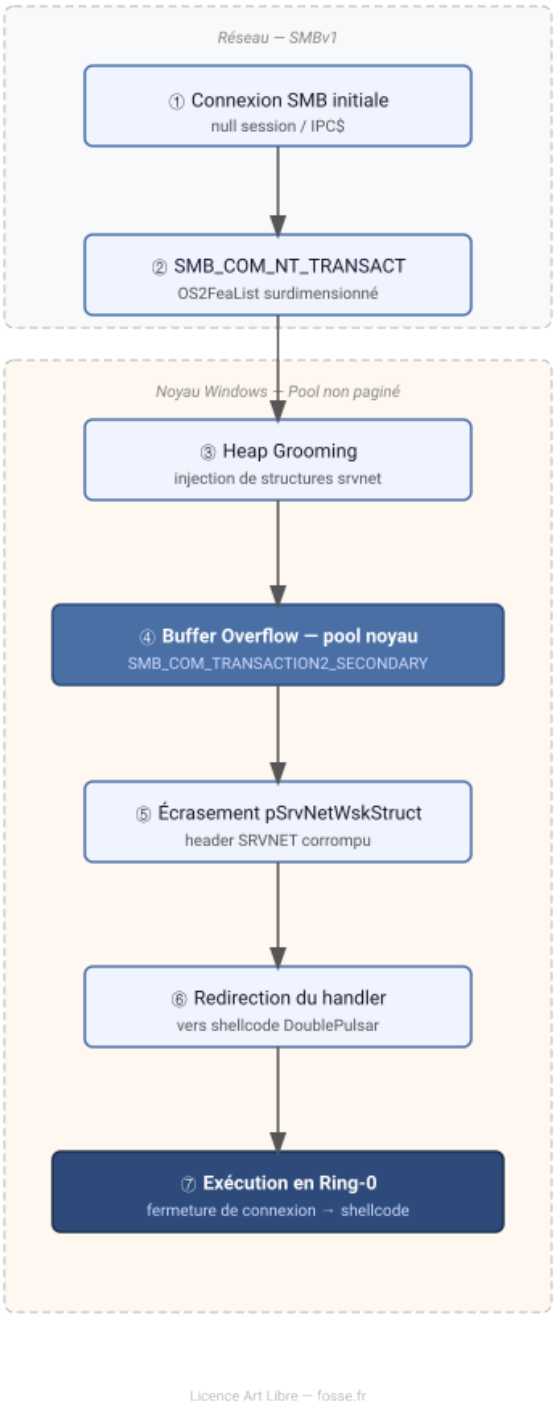

FIGURE 1 – Schéma du mécanisme d'exploitation EternalBlue dans le noyau Windows

personnalisé. Dès lors, tout paquet SMB Trans2 bien formé envoyé par l'attaquant active ce hook, qui déchiffre et exécute le shellcode secondaire transmis dans les données du paquet. Le backdoor utilise un mécanisme de *knocking* stéganographique : les opcodes de commande (ping 0x23, exec 0xC8, kill 0x77) sont encodés dans le champ Timeout des paquets SMB, invisible aux analyseurs réseau ordinaires. Cette conception lui permettait de rester dormant indéfiniment, utilisable à la demande, sans ouvrir de port supplémentaire.

Comment les Shadow Brokers ont-ils volé les outils de la NSA ?

Le 13 août 2016, un compte Twitter inconnu, *@shadowbrokerss*, poste un lien vers un dépôt GitHub contenant des fichiers chiffrés prétendant être des outils volés à l'Equation Group — le nom de code donné dans la communauté de la sécurité à l'unité TAO de la NSA. L'authenticité des outils est rapidement confirmée par des chercheurs indépendants : les exploits correspondent aux descriptions de programmes NSA mentionnés dans les documents divulgués par Edward Snowden en 2013.

Les Shadow Brokers publient leurs fuites en cinq vagues entre août 2016 et avril 2017. La dernière, intitulée « Lost in Translation » et diffusée le 14 avril 2017, est la plus dévastatrice : elle contient EternalBlue, EternalRomance, EternalSynergy, EternalChampion, DoublePulsar, DanderSpritz et le framework FuzzBunch, soit la totalité de l'arsenal SMB de la NSA.

L'identité des Shadow Brokers n'a jamais été établie avec certitude. Deux pistes ont dominé les enquêtes. La première pointe vers un initié de la NSA : en août 2016, le FBI arrêtait Harold T. Martin III, ancien sous-traitant de Booz Allen Hamilton ayant travaillé avec l'unité TAO entre 2012 et 2015, en possession de plus de 50 téraoctets de données classifiées. Il a plaidé coupable en 2019 pour rétention de documents de défense nationale, mais aucun lien direct avec les fuites n'a été établi. La seconde piste, défendue par la communauté du renseignement américain et par Edward Snowden lui-même, pointe vers une opération d'influence russe exploitant possiblement un initié comme source. La question reste ouverte. Ce qui est certain, c'est que la NSA a été informée du vol probable d'EternalBlue avant la publication des Shadow Brokers et a immédiatement alerté Microsoft, qui a publié le correctif MS17-010 le 14 mars 2017 — exactement un mois avant la fuite publique.

Quel a été l'impact de WannaCry et NotPetya sur les infrastructures critiques ?

Le 12 mai 2017, un vendredi matin, WannaCry se répand à une vitesse sans précédent : 10 000 machines par heure, 230 000 systèmes infectés dans 150 pays en l'espace d'une journée. Le ransomware, attribué par les agences de renseignement américaine, britannique et australienne au groupe Lazarus de la Corée du Nord, chiffre les fichiers et exige une rançon en Bitcoin. Il embarque EternalBlue pour sa propagation en réseau et vérifie l'absence de DoublePulsar avant d'installer sa propre charge utile.

L'impact sur le National Health Service britannique illustre crûment ce que représente une attaque contre des systèmes de santé mal entretenus. Sur 236 *NHS trusts* en Angleterre, 81 ont été affectés directement ou indirectement : 34 ont été infectés et verrouillés hors de leurs systèmes, dont 27 établissements de soins aigus. Au total, 603 organisations de soins primaires — dont 595 cabinets médicaux — ont été touchées. Les chiffres publiés par le National Audit Office britannique en octobre 2017 font état de 19 000 rendez-vous annulés sur la semaine de l'attaque, dont au moins 139 concernaient des patients avec suspicion de cancer. Une analyse publiée en 2019 dans *NPJ Digital Medicine* par des chercheurs d'Imperial College London évalue le coût direct sur les hôpitaux infectés à 5,9 millions de livres sterling, avec une réduction de 6 % des admissions par jour dans les établissements touchés. L'ensemble de l'attaque n'a été stoppé que par la découverte fortuite d'un *kill-switch* : un chercheur en sécurité, Marcus Hutchins, a enregistré un domaine présent dans le code du ransomware, bloquant ainsi sa propagation mondiale.

NotPetya, déployé le 27 juin 2017, est d'une autre nature. Attribué par la CISA américaine, l'OTAN et le gouvernement britannique au groupe Sandworm de la Direction générale du renseignement de l'état-major russe (GRU), il n'est pas un ransomware au sens propre — c'est un wiper. Son vecteur initial est une mise à jour empoisonnée du logiciel de comptabilité ukrainien M.E.Doc, préparée dès le 14 avril 2017. Une fois installé, NotPetya combine EternalBlue pour la propagation latérale avec Mimikatz, un outil de vol d'identifiants Windows créé en 2011 par le chercheur français Benjamin Delpy, pour se diffuser même sur des machines correctement patchées en usurpant des comptes administrateurs légitimes. La rançon affichée à l'écran est une décoration : l'identifiant présenté à la victime est généré aléatoirement, rendant tout déchiffrement impossible.

Les dommages de NotPetya dépassent l'entendement. Maersk, premier armateur mondial avec 76 ports et 800 navires, voit l'intégralité de son réseau s'effondrer en quelques minutes : la compagnie devra réinstaller 45 000 PC, 4 000 serveurs et 2 500 applications. Les pertes sont estimées entre 200 et 300 millions de dollars. Merck, le groupe pharmaceutique américain, perd 870 millions de dollars. FedEx, via sa filiale européenne TNT, 400 millions. L'évaluation de la Maison-Blanche fixe le bilan global à plus de 10 milliards de dollars, faisant de NotPetya la cyberattaque la plus coûteuse de l'histoire. Plusieurs assureurs refuseront d'indemniser leurs clients en invoquant la clause « acte de guerre », ouvrant un contentieux juridique inédit sur la nature des cyberarmes d'État.

Le Vulnerabilities Equities Process : cinq ans de secret au détriment de la sécurité publique

L'histoire d'EternalBlue ne commence pas avec les Shadow Brokers. Elle commence entre 2011 et 2012, quand la NSA découvre la vulnérabilité SMBv1 et choisit de la conserver. Ce choix relève d'un processus interagences américain créé en 2010 sous George W. Bush et formalisé sous Barack Obama : le Vulnerabilities Equities Process (VEP). Ce mécanisme est censé arbitrer, pour chaque vulnérabilité découverte, entre deux impératifs contradictoires — la divulguer à l'éditeur pour qu'il la corrige, ou la garder secrète pour l'exploiter à des fins de renseignement ou d'opérations offensives.

Dans le cas d'EternalBlue, la balance a penché du côté offensif pendant cinq années consécutives. Ce n'est qu'en apprenant le vol probable par les Shadow Brokers que l'agence a décidé d'en informer Microsoft. La question posée par le VEP n'était pas binaire — divulguer ou conserver — mais temporelle : quand divulguer. Et la réponse a été cinq ans.

La réaction de Microsoft a été cinglante. Brad Smith, alors président de Microsoft, a publié le 14 mai 2017 un billet de blog dans lequel il comparait la situation à celle d'un fabricant d'armes dont des missiles Tomahawk auraient été dérobés. Microsoft a réclamé une Convention de Genève numérique imposant aux États de cesser de constituer des arsenaux de vulnérabilités logicielles. Le VEP lui-même a été sévèrement critiqué : son secrétariat exécutif était logé à la NSA, créant un conflit d'intérêts structurel entre les missions offensives de l'agence et la sécurité défensive des systèmes civils. Une analyse publiée par la Columbia University Journal of International Affairs pointait également les failles du processus : des agences comme le FBI contournaient le VEP en achetant des vulnérabilités via des contrats stipulant expressément qu'elles ne recevraient pas les détails techniques, évitant ainsi l'obligation de divulgation.

Vu d'un poste d'architecte IT, le mécanisme révèle une tension fondamentale que les responsables politiques peinent à formuler clairement : les infrastructures que les agences de renseignement cherchent à attaquer chez leurs adversaires sont, dans leur très grande majorité, identiques à celles qui font fonctionner les hôpitaux, les réseaux électriques et les systèmes financiers de leurs propres citoyens. EternalBlue ciblait SMBv1 — un protocole Microsoft déployé uniformément dans les entreprises américaines, européennes et russes. L'arme ne discrimine pas.

EternalBlue est-il encore une menace en 2025 ?

Le correctif MS17-010 existe depuis le 14 mars 2017. Sur le papier, le problème est réglé depuis presque une décennie. Dans les faits, EternalBlue reste un vecteur actif en 2025, particulièrement dans les environnements industriels, les systèmes de santé et les administrations publiques d'Asie du Sud-Est et d'Europe de l'Est qui maintiennent des parcs de machines Windows non patchées pour des raisons de compatibilité opérationnelle.

La persistance de l'exploit ne tient pas à sa sophistication — elle tient à l'inertie des organisations. En février 2018, Sean Dillon, le chercheur de RiskSense qui avait analysé DoublePulsar, a porté EternalBlue sur l'ensemble des versions Windows depuis Windows 2000, y compris Windows 8 et Windows 10, démontrant que la surface d'attaque était encore plus large qu'initialement supposé. Les modules Metasploit correspondants sont librement accessibles depuis 2018. EternalRocks, un ver exploitant simultanément sept des outils fuités par les Shadow Brokers, a été observé dès mai 2017.

Les recommandations restent simples à énoncer, difficiles à appliquer dans des environnements contraints : désactiver SMBv1 sur tous les systèmes où il n'est pas fonctionnellement nécessaire, appliquer MS17-010 ou migrer vers des versions de Windows maintenues, segmenter les réseaux pour limiter les mouvements latéraux, et détecter les traces de DoublePulsar via des outils d'analyse mémoire comme Volatility ou Rekall. La vraie difficulté n'est pas technique — elle est organisationnelle. Les systèmes qui restent vulnérables en 2025 sont rarement vulnérables par ignorance : ils le sont parce que personne n'a assumé la responsabilité de leur mise à niveau, parce que le coût perçu du patch dépasse le risque perçu d'une attaque, et parce que la direction ne comprend pas encore qu'une machine non patchée connectée à un réseau n'est pas une machine protégée par une politique de sécurité — c'est une porte ouverte.

Conclusion

L'affaire EternalBlue concentre à elle seule les pathologies structurelles de la cybersécurité de notre époque : un État qui stocke des cyberarmes en espérant ne jamais les perdre, un processus de gestion des vulnérabilités structurellement biaisé vers l'offensif, un éditeur qui maintient une décennie après sa publication un protocole réseau des années 1980, et des organisations qui différent les patchs de sécurité jusqu'à ce que l'inévitable se produise. Les dommages directs de WannaCry et NotPetya dépassent les 14 milliards de dollars. Ils auraient pu être évités si la NSA avait signalé la faille à Microsoft en 2012 plutôt qu'en 2017.

Ce qui rend l'histoire d'EternalBlue particulièrement inconfortable, c'est qu'elle ne met pas en scène des cybercriminels isolés mais les États eux-mêmes comme producteurs de risque systémique. Les citoyens des pays membres de l'OTAN ont payé — en rendez-vous médicaux annulés, en données chiffrées, en systèmes

industriels détruits — le coût d'un secret que leur propre agence de renseignement avait décidé de conserver. Cette réalité devrait peser dans tout débat sur la gouvernance des capacités cyber offensives des démocraties.

Références

[1] Auteurs anonymisés. Working mechanism of EternalBlue and its application in ransomworm. Anglais. In : *ResearchGate preprint* (2021). Analyse académique des paquets NT Trans et Trans2 craftés, grooming du pool noyau, implémentation dans WannaCry, règles Snort de détection.

[2] Check Point Research. EternalBlue: Everything There Is To Know. Anglais. Analyse technique complète par reverse engineering, débogage noyau et capture réseau : les trois bugs SMBv1, heap grooming, installation de DoublePulsar. 2017.

[3] Sean Dillon. DoublePulsar Initial SMB Backdoor Ring 0 Shellcode Analysis. Anglais. Analyse ring-0 du shellcode DoublePulsar : localisation ntoskrnl.exe, hook SrvTransaction2DispatchTable, protocole de communication stéganographique. Avr. 2017.

[4] Jason Healey et Hannah Pitts. The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers. Anglais. In : *Columbia Journal of International Affairs* (2017). Analyse du Vulnerabilities Equities Process : historique, critiques structurelles, conflits d'intérêts et propositions de réforme.

[5] Kelly Rudder. An Analysis of NotPetya and EternalBlue: Past Damage and Future Risk. Anglais. Rapport de cours CPSC 610. Analyse technico-juridique de WannaCry et NotPetya : responsabilités comparées NSA/Microsoft, scénarios hypothétiques, persistance de la menace. Yale University, Department of Computer Science, 2021.

[6] Lucas Tran. EternalBlue Exploit. Anglais. Rapport pédagogique CSC 427. Synthèse pédagogique du mécanisme d'exploit : bugs FEA, heap spray, propagation wormable et contre-mesures. University of Toronto, Department of Computer Science, 2018.

[7] Virus Bulletin Research. EternalBlue: a prominent threat actor of 2017-2018. Anglais. In : *Virus Bulletin* (juin 2018). Revue académique spécialisée : structures OS2FeaList, buffer overflow dans srv!SrvOs2FeaToNt, comparaison avec les autres exploits Eternal.