tenable | RESEARCH

LA LONGUEUR D'AVANCE DES ATTAQUANTS : UN AVANTAGE QUANTIFIÉ

SOMMAIRE

Résumé 3
Résultats 3
Recommandations 3
Introduction 4
La longueur d'avance des attaquants : un avantage quantifié 4
Jeu de données de vulnérabilité 6
Delta médian 6
Delta négatif 7
Deltas notables 8
Conclusion 9
Répartition générale des données 11
Méthodologie 12
Limites 12
Analyse étendue 13
Normes et conventions 14
À propos de Tenable 14

I. RÉSUMÉ

Le présent rapport mesure l'écart, en nombre de jours, entre le moment où un code malveillant permettant d'exploiter une vulnérabilité devient publiquement disponible (délai de disponibilité de l'exploit) et le moment où cette vulnérabilité est évaluée pour la première fois (délai d'évaluation).

Un delta négatif indique que l'attaquant a la possibilité d'exploiter une vulnérabilité avant même que le défenseur ne prenne connaissance du risque.

L'échantillon utilisé pour cette analyse est basé sur les 50 vulnérabilités les plus courantes parmi près de 200 000 scans de vulnérabilité uniques.

Résultats :

7 jours

Les attaquants disposent en moyenne d'une fenêtre d'opportunité de sept jours pour exploiter une vulnérabilité avant même que le défenseur ne se soit rendu compte qu'il est vulnérable.

76 %

des vulnérabilités analysées présentent un delta négatif, ce qui indique que l'attaquant a pris l'avantage de l'offensive.

34 %

Pour 34 % des vulnérabilités analysées, un exploit a été mis à disposition le jour même de la divulgation de la vulnérabilité.

24 %

Autre sujet d'inquiétude, 24 % des vulnérabilités analysées sont activement exploitées par des programmes malveillants, des ransomwares ou des kits d'exploit à disposition.

75 %

Une amélioration du délai d'évaluation de 75 % générerait un delta positif pour 66 % des vulnérabilités analysées. Car le délai de disponibilité d'un exploit et sa dangerosité potentielle sont tels que les défenseurs sont le plus souvent désavantagés dès le départ et ont bien du mal à reprendre le dessus.

Recommandations :

- Réalisez des évaluations des vulnérabilités continues afin de réduire le délai d'évaluation. Cependant, cette mesure ne suffit pas à elle seule à refermer totalement la fenêtre d'exposition.
- De nouvelles vulnérabilités ou nouveaux exploits sont constamment découverts et publiés. Les attaques et menaces évoluent rapidement et peuvent frapper à tout moment. Un programme efficace de gestion des vulnérabilités doit avoir pour objectif de s'adapter et de réagir rapidement face à ces situations changeantes. Un modèle de type marche-arrêt ou cyclique n'est pas à la hauteur d'un tel objectif, nécessitant plutôt une approche de gestion de vulnérabilité de type intégration et distribution continues (CI/CD).
- Alignez les processus opérationnels de façon à favoriser une réponse rapide, des demandes de remédiation et de limitation de risque ad hoc, en dehors des fenêtres habituelles de maintenance et de patch.
- Concentrez vos efforts de correction et de priorisation sur les vulnérabilités pour lesquelles des exploits sont publiquement disponibles, ainsi que sur celles activement visées par des programmes malveillants, des kits d'exploit et des ransomwares. Cela nécessite de comprendre la situation et le contexte des menaces en se basant sur des données à jour.

II. INTRODUCTION

Le présent rapport de recherche examine le temps écoulé entre la publication d'un code malveillant exploitant une vulnérabilité et le moment où les utilisateurs évaluent activement cette vulnérabilité. Ces deux événements correspondent à la première action respective de l'attaquant et du défenseur.

Le présent rapport part du principe que ce delta est un indicateur significatif de la Cyber Exposure. L'échantillon utilisé est basé sur l'analyse de données réelles résultant de près de 200 000 scans de vulnérabilités uniques. Pour les besoins du présent rapport, nous avons sélectionné les 50 vulnérabilités de gravité et de sévérité les plus courantes.

Nous supposons que le lecteur possède des connaissances basiques sur la manière dont les vulnérabilités sont recherchées, évaluées et exploitées.

III. LA LONGUEUR D'AVANCE DES ATTAQUANTS : UN AVANTAGE QUANTIFIÉ

Les professionnels de la sécurité sont engagés dans une course contre la montre avec les instigateurs des menaces. Dans le domaine des vulnérabilités, cette course consiste, pour les attaquants, à accéder aux exploits et, pour les défenseurs, à être capables d'évaluer les vulnérabilités, d'y remédier et de les réduire. Les attaquants obtiennent et conservent l'avantage s'ils peuvent avoir au moins un coup d'avance sur les défenseurs, ouvrant ainsi une fenêtre d'exposition. Cette course sans fin recommence à chaque fois qu'une nouvelle vulnérabilité est découverte. La ligne d'arrivée est mouvante et c'est l'attaquant qui impose son rythme.

La figure 1 décrit les premières actions des attaquants et des défenseurs suite à la divulgation d'une vulnérabilité.

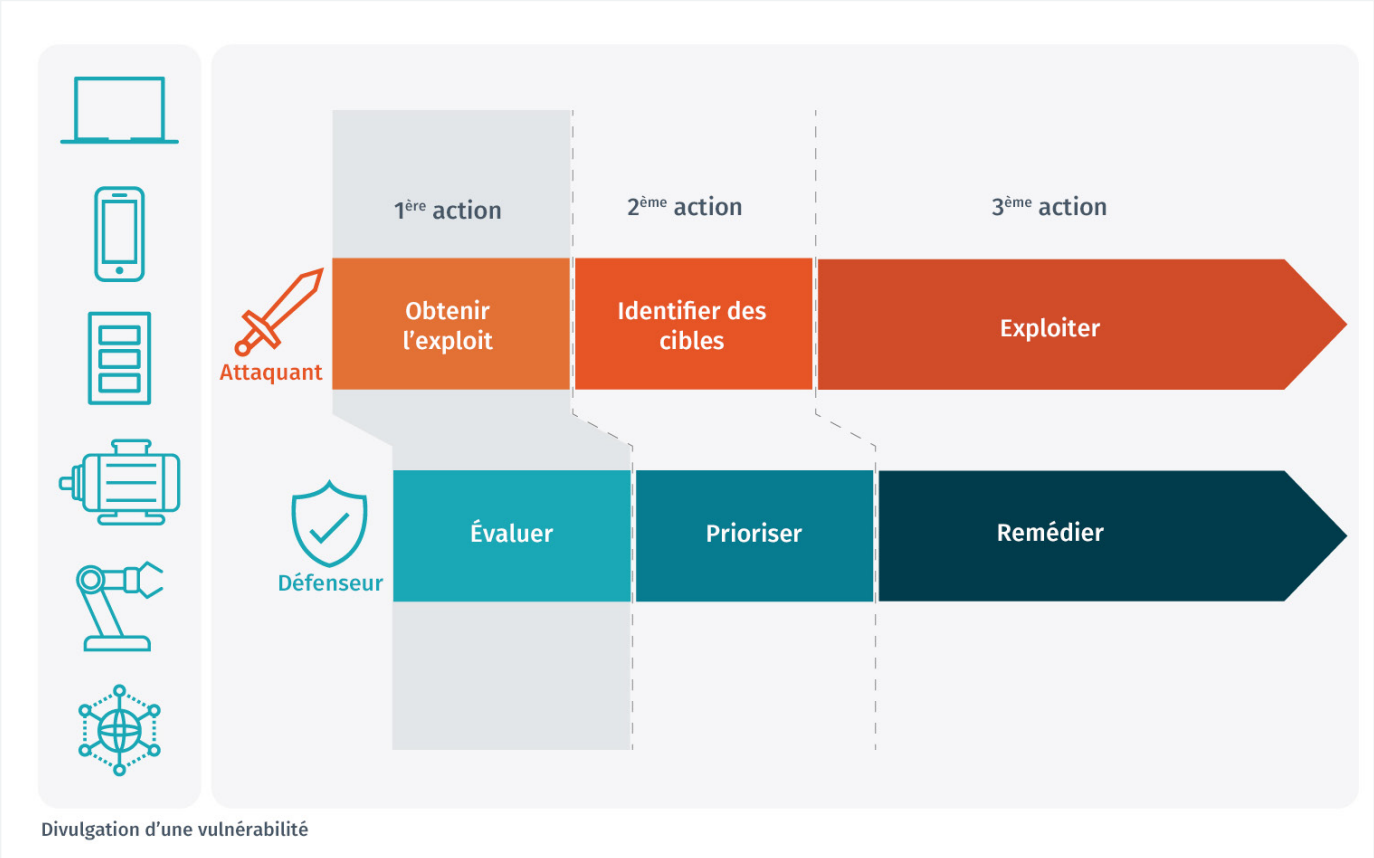


Figure 1. Premières actions des attaquants et des défenseurs suite à l'apparition d'une vulnérabilité

Lorsqu'une nouvelle vulnérabilité est divulguée, la première action de l'attaquant consiste à se procurer un exploit qui fonctionne. La première action du défenseur consiste à évaluer l'impact de cette vulnérabilité dans son entreprise et le risque qu'elle représente. Pour ce faire, il procède à une scan de vulnérabilités. Si nous comparons le délai de disponibilité de l'exploit (Time to Exploit) au délai d'évaluation initiale (Time to Assess), nous obtiendrons un chiffre négatif ou positif exprimant le delta entre ces deux valeurs :

- Un delta négatif indique que l'attaquant a pris l'avantage de l'offensive.
- Un delta positif indique que le défenseur a évalué la vulnérabilité avant que l'exploit correspondant ne devienne disponible, et qu'il bénéficie d'une marge de manœuvre pour lancer les étapes de remédiation et de limitation de risque.

Tant que l'attaquant conserve une longueur d'avance, le défenseur est vulnérable. L'attaquant dispose alors d'une fenêtre d'opportunité pour frapper en toute impunité.

En théorie, le défenseur a le temps de remédier à une vulnérabilité tant qu'aucun attaquant ne l'a effectivement exploitée. Dans la plupart des cas, nous ne disposons pas de données suffisantes pour déterminer à quel moment une vulnérabilité est activement exploitée dans la nature. Notre visibilité sur les actions des attaquants est limitée ; nous devons donc nous concentrer sur les informations fiables que nous sommes en mesure d'obtenir, pour ensuite les extrapoler. Lorsqu'un exploit est disponible, nous devons supposer qu'il peut être et sera utilisé. Contrairement à d'autres études exclusivement consacrées au délai de disponibilité de l'exploit, le présent rapport établit une corrélation entre celui-ci et le délai d'évaluation.

Notre analyse part du principe que le type de course est un sprint et non un marathon. En mesurant les premières actions des attaquants et des défenseurs, nous comprenons comment la course a commencé, ce qui nous permet d'en prévoir l'issue. En d'autres termes, le concurrent qui prend la tête dès le départ conserve généralement l'avantage. Mises à part les vulnérabilités zero-day, les vulnérabilités passent de risque hypothétique à réel dès qu'un exploit public est disponible.

Cette analyse calcule le delta entre le délai de disponibilité de l'exploit (DD) et le délai d'évaluation (DE) pour les 50 vulnérabilités les plus courantes, d'après le nombre d'actifs affectés dans le jeu de données. La taille de l'échantillon ne permet pas de tirer de conclusions plus générales au sujet des vulnérabilités. Le delta varie en fonction des vulnérabilités qui prédominent à un moment donné. Pour connaître le delta calculé pour un ensemble plus étendu de vulnérabilités, reportez-vous à l'annexe.

Nous mesurons le temps écoulé entre le moment où un exploit est mis à la disposition du public et le moment où la vulnérabilité est évaluée pour la première fois.

$$\Delta = DD - DE$$

DD = délai de disponibilité de l'exploit
DE = délai d'évaluation

IV. ANALYSE

Jeu de données de vulnérabilité

Pour mener notre analyse et calculer le delta médian, nous avons généré un jeu de données de vulnérabilité sur la base des critères suivants :

- Sévérité Élevée (CVSSv2 de 7 à 8,9) et Critique (CVSSv2 de 9 à 10) ;
- Disponibilité d'un exploit public
- Publication d'un plug-in Tenable en 2017.

Ensuite, nous avons sélectionné les 50 vulnérabilités les plus courantes, c'est-à-dire celles ayant affecté le plus grand nombre d'actifs sur une période de trois mois à la fin de l'année 2017. Nous avons choisi ces critères de sélection pour fonder notre analyse sur une activité réelle.

Delta médian	
Délai de disponibilité de l'exploit (DD) médian	5,5 jours
Délai d'évaluation (DE) médian	12,8 jours
Delta médian	**-7,3**

V. DELTA MÉDIAN

Tableau 1. Delta médian pour les 50 vulnérabilités les plus courantes

Les résultats de l'analyse des vulnérabilités les plus courantes indiquent que le délai de disponibilité médian de notre échantillon est de 5,5 jours. Le délai d'évaluation médian, quant à lui, est de 12,8 jours. Le delta médian s'élève donc à -7,3. **Cela signifie que, pour cet échantillon, les attaquants disposent en moyenne d'une fenêtre d'opportunité de sept jours pour exploiter une vulnérabilité avant même que le défenseur ne l'ait repérée.**

Profil des 50 vulnérabilités les plus courantes

Sévérité Critique

54 % des 50 vulnérabilités les plus courantes sont de sévérité critique, avec un CVSS version 2 Base Score de 9-10.

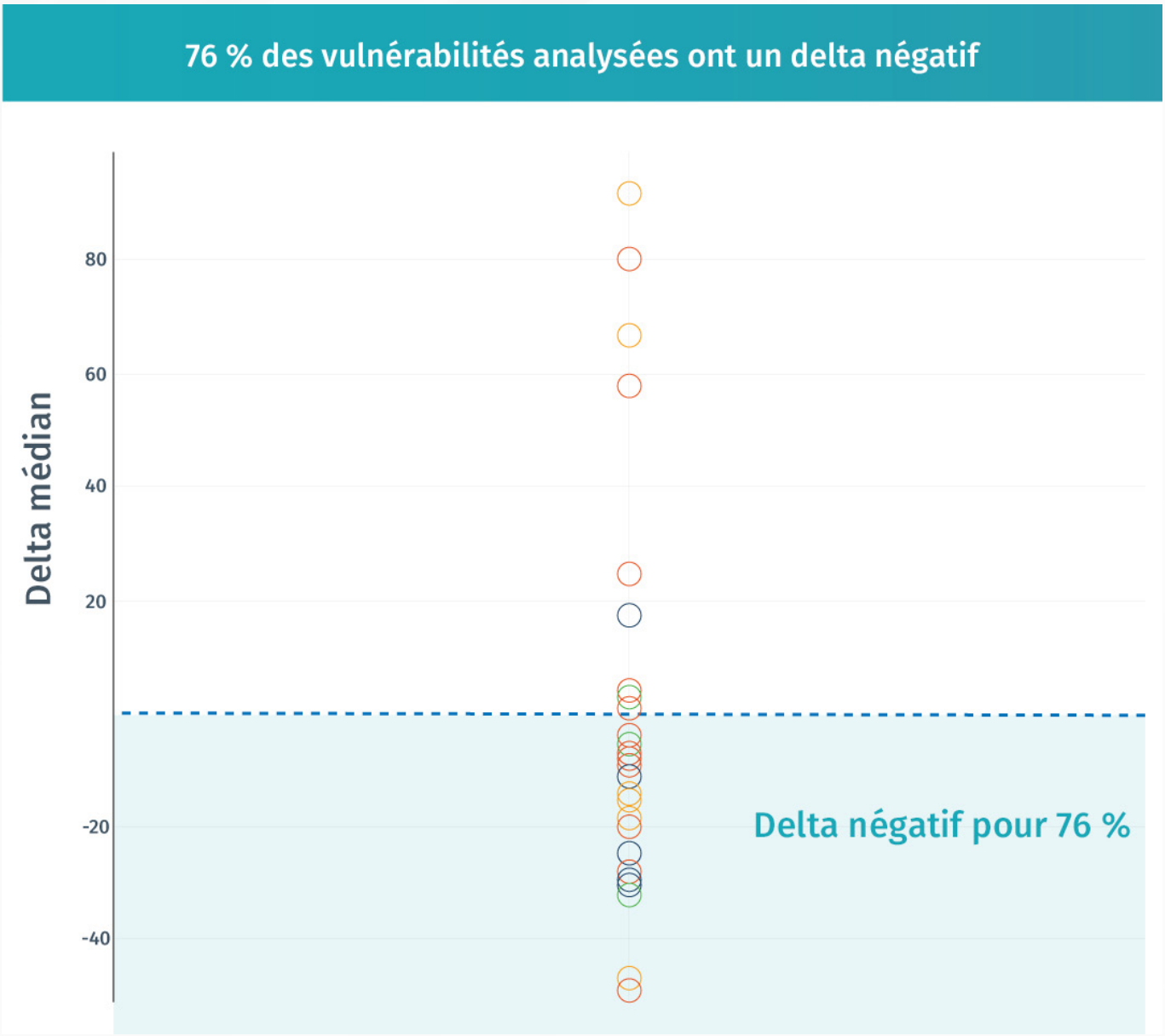
Exploitées par des programmes malveillants

24 % (12 sur 50) des vulnérabilités analysées sont effectivement visées par des programmes malveillants.

Relayées dans les médias

14 % (7 sur 50) des vulnérabilités analysées sont considérées comme étant de premier plan par Tenable en raison de la couverture médiatique dont elles font l'objet.

Δ médian = -7,3



Delta négatif

Pour 76 % des vulnérabilités, le delta est négatif, ce qui signifie que les attaquants ont pris l'avantage de l'offensive. Dans 34 % des cas, un exploit était publiquement disponible le jour même de la révélation de la vulnérabilité.

Fait inquiétant, 24 % des vulnérabilités incluses dans le jeu de données étaient activement visées par des programmes malveillants, avec un delta médian de -6,7. Quatorze pour cent des vulnérabilités analysées sont considérées comme étant de premier plan en raison de l'attention médiatique qu'elles ont suscitée. Ces vulnérabilités de premier plan ont un delta médian de -12,0.

Vulnérabilités exploitées par des programmes malveillants : delta médian de -6,7

Vulnérabilités relayées dans les médias : delta médian de -12,0

Deltas notables

CVE	Nom	Pourquoi est-elle notable ?	DD médian (en jours pleins)	DE médian (en jours pleins)	Delta médian (en jours pleins)
CVE-2017-5638*	Vulnérabilité dans Apache Struts permettant l'exécution de code à distance	De premier plan : cause première de la fuite de données chez Equifax.	1	4	-3
CVE-2017-7494	Vulnérabilité dans Samba permettant l'exécution de code à distance	De premier plan et incluse dans des programmes malveillants : SambaCry ou Eternal Red. Vulnérabilité apparentée à WannaCry, mais affectant Samba. Visée par le ransomware StorageCrypt.	0	9	-9
CVE-2017-8759	Vulnérabilité dans Microsoft Windows .NET Framework permettant l'exécution de code à distance	De premier plan et incluse dans des programmes malveillants : utilisée par des groupes APT agissant pour le compte d'un État afin de déployer l'outil de surveillance FinSpy.	1	7	-6
CVE-2017-5753** CVE-2017-5715	Vulnérabilité affectant plusieurs processeurs permettant la divulgation d'informations	De premier plan : vulnérabilité Spectre affectant les processeurs.	0	15	-15

* La CVE-2017-5638, indiquée ici à titre indicatif, ne figurait pas parmi les 50 vulnérabilités les plus courantes, mais figurait dans un jeu de données d'échantillon plus étendu. Pour en savoir plus, reportez-vous à l'annexe.

** La vulnérabilité Spectre a été divulguée début 2018, mais nous l'avons incluse à des fins de référence et de comparaison.

VI. CONCLUSION

La transformation digitale a entraîné une augmentation et une diversification considérables des nouvelles technologies et plateformes informatiques, du cloud à l'IoT et aux Technologies Opérationnelles. Résultat : la surface d'attaque s'est elle aussi nettement étendue. Inévitablement, cette situation donne naissance à un flot ininterrompu de vulnérabilités. Pourtant, de nombreuses entreprises gèrent encore leurs programmes d'opérations selon des cycles fixes (par ex. toutes les six semaines) qui ne sont pas adaptés à l'environnement informatique dynamique de notre époque.

Par conséquent, la latence fait partie intégrante du processus de cybersécurité, donnant l'avantage à l'attaquant dès le départ et créant un déficit de connaissances. De nombreux RSSI ont bien des difficultés à y voir clair dans un paysage de menaces en constante évolution. Ce manque de visibilité empêche la gestion proactive des cyber-risques en fonction de leur importance critique pour l'entreprise.

Les défenseurs avancent au rythme de facteurs internes au lieu de s'adapter à celui des événements externes.

7 jours

Les attaquants disposent d'une fenêtre d'opportunité de sept jours pour exploiter une vulnérabilité avant même que le défenseur ne se soit rendu compte qu'il est vulnérable.

76 %

des vulnérabilités analysées présentent un delta négatif, ce qui indique que l'attaquant a pris l'avantage de l'offensive.

Lorsque les défenseurs parviennent à prendre l'avantage, cela s'explique généralement par le fait qu'un exploit n'est devenu publiquement disponible que longtemps après la divulgation de la vulnérabilité, et non par un délai d'évaluation plus court. Autrement dit, ce n'est pas grâce à leurs propres actions que les défenseurs prennent l'avantage. L'attaquant amorce déjà son premier virage alors que le défenseur n'a pas encore quitté les starting-blocks. Ce dernier agit comme s'il courait en solitaire, oubliant qu'il a un adversaire.

Le moyen le plus efficace de conserver un delta positif pour la majorité des vulnérabilités consiste à procéder à des évaluations en continu.

34 %

Pour 34 % des vulnérabilités analysées, un exploit a été mis à disposition le jour même de la divulgation de la vulnérabilité.

75 %

Une amélioration du délai d'évaluation de 75 % générerait un delta positif pour 66 % des vulnérabilités analysées.

Les évaluations continues des vulnérabilités représentent la meilleure solution, parce que le délai d'évaluation dépend de la disponibilité d'un plug-in ou d'une signature et qu'il est impacté par les frais associés aux évaluations à grande échelle.

D'après le temps moyen qui s'écoule entre la divulgation d'une vulnérabilité et la disponibilité d'un exploit, une amélioration du délai d'évaluation de 60 % ne générerait un delta positif que pour 50 % des vulnérabilités analysées. Une amélioration de 75 % générerait un delta positif pour 66 % des vulnérabilités analysées.

Notre étude des habitudes d'analyse indique qu'à peine plus de 25 % des entreprises procèdent à des évaluations des vulnérabilités au moins tous les deux jours. Même si cet objectif est tout à fait réalisable et permet de réduire l'avance qu'ont les attaquants pour la plupart des vulnérabilités, pour certaines d'entre elles, le delta peut malgré tout rester négatif et donc poser des risques. Or cette exposition peut jouer un rôle décisif selon les vulnérabilités concernées.

Puisque ce sont les instigateurs des menaces qui imposent le rythme, les brèches existantes de Cyber Exposure ne peuvent pas être comblées par de petits ajustements ni par le département sécurité à lui seul.

24 %

des vulnérabilités incluses dans le jeu de données sont activement visées par des programmes malveillants.

14 %

des vulnérabilités analysées sont considérées comme étant de premier plan en raison de l'attention médiatique qu'elles ont suscitée.

Sachant que la plupart des vulnérabilités présentent un delta négatif et que leur évaluation survient généralement après la mise à disposition d'un exploit, les défenseurs doivent compenser ce désavantage dans les étapes suivantes, en améliorant leur approche de la gestion des vulnérabilités.

Un programme efficace de gestion des vulnérabilités garantit une adaptation et une réaction rapides face à un paysage de menaces en constante évolution. Les modèles de type marche-arrêt ou cycliques ne sont pas à la hauteur. L'approche de la gestion des vulnérabilités doit plutôt suivre un modèle d'intégration et de distribution en continu.

Il ne serait pas réaliste de croire que le département sécurité peut, à lui seul, atteindre cet objectif. Un meilleur alignement sur les divisions opérationnelles et le reste de l'entreprise est indispensable. Dans cette optique, les processus opérationnels doivent favoriser une réponse rapide et des étapes de remédiation et de limitation de risque ad hoc, en dehors des fenêtres habituelles de maintenance et de patchs.

Les efforts de remédiation et de priorisation doivent se concentrer sur les vulnérabilités pour lesquelles des exploits sont publiquement disponibles, ainsi que sur celles activement visées par des programmes malveillants, des kits d'exploit et des ransomwares. Cela nécessite de comprendre la situation et le contexte des menaces en se basant sur des données à jour, pour évaluer l'exposition et les risques réels, mais aussi prendre des décisions éclairées.

Recommandations

- Réalisez des évaluations continues des vulnérabilités afin de réduire le délai d'évaluation. Cependant, cette mesure ne suffit pas à elle seule à refermer totalement la fenêtre d'exposition.
- Sans cesse, de nouvelles vulnérabilités sont découvertes et de nouveaux exploits sont publiés. Les attaques et les menaces évoluent rapidement et peuvent frapper à tout moment. Un programme efficace de gestion des vulnérabilités doit avoir pour objectif de garantir une adaptation et une réaction rapides face à ces situations nouvelles. Un modèle de type marche-arrêt ou cyclique n'est pas à la hauteur d'un tel objectif. Une approche de gestion des vulnérabilités basée sur un modèle d'intégration et de distribution en continue est préférable.
- Alignez les processus opérationnels de façon à favoriser une réponse rapide et des étapes de remédiation et de limitation de risque ad hoc, en dehors des fenêtres habituelles de maintenance et d'application des patchs.
- Concentrez vos efforts de remédiation et de priorisation sur les vulnérabilités pour lesquelles des exploits sont publiquement disponibles, ainsi que sur celles activement visées par des programmes malveillants, des kits d'exploit et des ransomwares. Cela nécessite de comprendre la situation et le contexte des menaces en se basant sur des données à jour.

VII. ANNEXE

Répartition générale des données

Les tableaux qui suivent présentent la répartition des données de vulnérabilité analysées. L'échantillon ne permet pas de tirer de conclusions plus générales et il n'est pas destiné à être représentatif.

Le tableau ci-dessous répertorie, sans ordre particulier, les CPEs[1] des vulnérabilités analysées.

Systèmes d'exploitation	Applications
Microsoft Windows	Adobe Flash Player
Red Hat Enterprise	Apache Struts
Apple MacOS	Apple MacOS
Canonical Ubuntu Linux	Cisco WebEx
Novell SuSE Linux	Microsoft Internet Explorer
Oracle Linux	Microsoft .NET Framework
CentOS Linux	Microsoft Malware Protection Engine
Oracle VM Server	Microsoft SharePoint
Debian Linux	Oracle VirtualBox

Tableau 3. CPEs des vulnérabilités analysées

1. Common Platform Enumeration, voir www.nvd.nist.gov/products/cpe

Le tableau ci-dessous présente la répartition générale des valeurs mesurées. Il apparaît clairement que certaines

Analyse des valeurs aberrantes du jeu de données	DD	DE	Delta
Valeur la plus élevée du jeu de données	145,0	50,2	116,6
Valeur la plus basse du jeu de données	0	5,9	**-50,2**
Moyenne	15,0	17,1	**-2,0**
Médiane	5,5	12,8	**-7,3**

valeurs aberrantes ont faussé la moyenne.

Tableau 4. Analyse des valeurs aberrantes du jeu de données

Méthodologie

Notre analyse porte sur les vulnérabilités remplissant les critères suivants :

- Sévérité de niveau Élevé (CVSS2 de 7 à 8,9) et Critique (CVSS2 de 9 à 10)
- Disponibilité d'un exploit public
- Publication d'un plug-in Tenable en 2017
- Prévalence en termes de nombre d'actifs affectés d'après les évaluations Tenable.io sur une période de trois mois à la fin de l'année 2017

Pour identifier les vulnérabilités les plus courantes, nous nous sommes basés sur leur prévalence en termes de nombre total d'actifs affectés sur la période spécifiée. Nous avons également tenu compte du jour ayant le pic d'actifs affectés.

Le DD mesuré correspond à l'écart, en nombre de jours, entre la date de divulgation publique d'une vulnérabilité fournie par la base de données VulnDB[2] et la date de disponibilité d'un exploit fournie par la base de données Exploit-DB[3]. Dans certains cas, il est possible qu'un exploit ait été mis à disposition avant cette date via un autre canal, mais pour les besoins de la présente analyse, nous avons choisi VulnDB et Exploit-DB comme sources de référence.

Le DE mesuré correspond à l'écart entre la date de divulgation de la vulnérabilité selon VulnDB et la date à laquelle le plug-in correspondant a été inclus pour la première fois dans une analyse de vulnérabilité.

Limites

- Les dates de divulgation de la vulnérabilité utilisées sont basées sur celles de VulnDB. Dans certains cas exceptionnels, il se peut qu'une vulnérabilité ait été divulguée à une date antérieure (par ex. sur le darknet).
- La date de disponibilité de l'exploit est basée sur celle d'Exploit-DB. Dans certains cas, il est possible qu'un exploit ait été mis à la disposition du public à une date antérieure, par exemple dans le cadre d'une exploitation zero-day.
- La disponibilité d'un exploit n'est pas nécessairement synonyme d'exploitation active. En général, seul un sous-ensemble de vulnérabilités exploitables sont, par exemple, utilisées en tant que cyber-armes et automatisées sous forme de programmes malveillants, ransomwares et kits d'exploit. Un instigateur humain, toutefois, a accès à tout exploit publié.
- L'échantillon ne contenant que 50 vulnérabilités, il n'est pas représentatif et ne suffit pas à tirer des conclusions détaillées ou plus larges au sujet des vulnérabilités en général.

2. VulnDB est une base de données de vulnérabilités propriétaire appartenant à Risk Based Security. 3. Exploit-DB est une base de données gérée par Offensive Security.

Analyse étendue

Tenable Research a mené une précédente analyse de delta sur la base d'un échantillon contenant 430 CVE uniques.

Les critères d'échantillonnage étaient les suivants :

- publication de la vulnérabilité en 2017 ;
- disponibilité d'un exploit public ;
- prévalence suffisante pour permettre un calcul de DE représentatif.

Si l'on compare les vulnérabilités exploitables les plus courantes, le delta est variable, mais la tendance générale est toujours négative. Le tableau ci-dessous présente les valeurs mesurées pour les deux jeux de données :

	Vulnérabilités exploitables en 2017	50 vulnérabilités les plus courantes
DD médian (en jours)	7,1	5,5
DE médian (en jours)	11,8	12,8
Delta = DD - DE	**-4,7**	**-7,3**

Tableau 5. Comparaison des deltas médians des deux jeux de données

Normes et conventions

Le présent rapport utilise certains termes qui sont définis ci-après :

Terme	Définition
Disponibilité de l'exploit	Date à laquelle un code malveillant permettant d'exploiter la vulnérabilité devient publiquement disponible dans Exploit-DB.
Date d'évaluation	Date de la première exécution d'une analyse incluant un plug-in permettant d'évaluer la vulnérabilité.
Délai d'évaluation (DE)	Délai, en nombre de jours, qui s'écoule entre le moment où une vulnérabilité est divulguée au public et le moment où le plug-in correspondant est inclus dans une analyse des vulnérabilités. La date de publication du plug-in correspond au moment à partir duquel il devient possible de détecter une vulnérabilité spécifique.
Délai de disponibilité de l'exploit (DD)	Délai, en nombre de jours, qui s'écoule entre le moment où une vulnérabilité est divulguée au public et le moment où l'exploit correspondant est publié.
Asset affecté	Délai, en nombre de jours, qui s'écoule entre le moment où une vulnérabilité est divulguée au public et le moment où l'exploit correspondant est publié.
CVE	Common Vulnerabilities and Exposure (vulnérabilités courantes et exposition) : identifiant commun des vulnérabilités connues. Le présent document utilise les termes « CVE » et « vulnérabilité » de manière interchangeable.
CPE	Common Platform Enumeration (recensement commun des plateformes).
CVSS	Common Vulnerability Scoring System (système commun d'évaluation des vulnérabilités). Le présent rapport se réfère à la norme CVSS version 2.

Tableau 6. Définition des termes clés

VIII. À PROPOS DE TENABLE

Tenable®, Inc. est la société spécialisée en Cyber Exposure. Plus de 24 000 entreprises du monde entier lui font confiance pour comprendre et réduire leur cyber-risque. Après avoir créé Nessus®, Tenable a enrichi son expertise en matière de vulnérabilités pour proposer Tenable.io®, la première plateforme au monde capable de détecter et de sécuriser tous les assets numériques, quelle que soit la plateforme informatique. Parmi les clients de Tenable figurent plus de 50 % des entreprises du classement Fortune 500, plus de 20 % des entreprises du classement Global 2000, ainsi que de grandes administrations publiques. Pour en savoir plus, rendez-vous sur www.tenable.com.

7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046, États-Unis

Amérique du Nord : +1 (410) 872 0555

www.tenable.com

03/05/2018 V01