L'obsolescence systémique et la télémétrie : Analyse de la vulnérabilité intrinsèque des infrastructures informatiques en fin de vie dès la connexion initiale

La compréhension traditionnelle de la cybersécurité repose souvent sur le postulat que la vulnérabilité d'un système informatique est une fonction de l'interaction humaine : une erreur de configuration, le clic sur un lien malveillant ou le téléchargement d'un fichier infecté. Cependant, l'évolution de l'architecture logicielle vers des modèles de dépendance continue aux services distants a engendré un nouveau paradigme de risque. Dans ce contexte, un système en fin de vie (End-of-Life, EOL) ne devient pas faillible par l'action de son utilisateur, mais par sa propre architecture. Il est intrinsèquement programmé pour initier des communications avec des infrastructures de confiance qui, une fois abandonnées par leurs fournisseurs d'origine, se transforment en vecteurs d'infection automatique.[1] Ce rapport explore la télémétrie comme surface d'attaque systématique, analysant comment les domaines orphelins et les infrastructures abandonnées sont réutilisés pour compromettre les systèmes dès les premiers instants de leur connexion à Internet.

La télémétrie comme automate de vulnérabilité : Mécanismes et flux silencieux

La télémétrie moderne ne se limite pas à l'envoi de rapports d'erreur ; elle constitue un système nerveux complexe assurant la validation des licences, la synchronisation temporelle, la vérification de la connectivité et la recherche de mises à jour. Ces flux sont caractérisés par leur nature "silencieuse" et autonome. Dès le démarrage d'un système d'exploitation ou d'un service réseau, des requêtes sont émises vers des points de terminaison souvent codés en dur (hardcoded) dans les binaires.[4]

Les premiers instants de la connexion : Le réveil de l'automate

Lorsqu'un système obsolète, tel qu'une instance de Windows XP ou Windows 7 encore présente dans des environnements industriels ou médicaux, établit une connexion réseau, il tente immédiatement de joindre ses serveurs de référence. Ces tentatives de connexion se produisent avant même qu'une session utilisateur ne soit pleinement opérationnelle.[7] Si les domaines associés à ces services ont été abandonnés ou ont expiré, un attaquant ayant racheté ces ressources peut intercepter ces requêtes et répondre avec des données

malveillantes.

Le risque est amplifié par le fait que ces services de maintenance fonctionnent généralement avec des privilèges de niveau "Système" ou "Root". Une réponse falsifiée à une requête de mise à jour peut ainsi mener à l'exécution de code à distance (RCE) sans aucune intervention ou notification pour l'utilisateur.[9] La vulnérabilité est donc une propriété déterministe du système : tant que le système est connecté et que l'infrastructure de destination est compromise, l'infection est inévitable.

Type de Flux Silencieux	**Protocole**	**Fonction de Maintenance**	**Risque en cas d'Obsolescence**
Télémétrie Analytique	HTTPS/UDP	Collecte de données d'usage et performance	Interception de métadonnées et redirection C2 [5]
Vérification NTP	NTP (Port 123)	Synchronisation de l'horloge système	Empoisonnement temporel et invalidation de certificats [11]
Requêtes WHOIS	WHOIS (Port 43)	Vérification de la propriété des domaines émetteurs	Exécution de code via parsing de réponse malveillante [2]
Mise à jour automatique	HTTP/HTTPS	Téléchargement de correctifs ou de signatures	Substitution de binaires par des portes dérobées (backdoors) [12]

Hardcoding et persistance des références obsolètes

Le problème fondamental réside dans la rigidité des références. De nombreux logiciels et systèmes d'exploitation utilisent des adresses IP ou des domaines statiques pour leurs fonctions critiques. Par exemple, des variantes de télémétrie Windows ont été observées utilisant des domaines comme alpha.telemetry.microsft.com (notez la faute de frappe potentielle ou le domaine spécifique) ou des adresses IP codées en dur pour contourner les échecs DNS.[5] Dans un scénario d'obsolescence, ces références deviennent des "points d'ancrage" pour les attaquants. Le système ne peut pas "apprendre" que le service a déménagé ou a cessé d'exister ; il continue de frapper à une porte désormais contrôlée par un tiers

malveillant.[3]

L'infrastructure fantôme : Analyse du détournement des domaines orphelins

Le concept de domaine orphelin ou abandonné est au cœur de cette surface d'attaque. Un fournisseur de services peut décider de migrer ses infrastructures vers de nouveaux domaines, laissant les anciens expirer sans réaliser que des milliers de clients legacy continuent de pointer vers eux.

L'affaire du TLD.MOBI : Une étude de cas sur l'infrastructure critique

En 2024, les recherches menées par watchTowr Labs ont révélé une faille systémique majeure concernant le domaine de premier niveau (TLD).mobi. Historiquement, le serveur WHOIS faisant autorité pour ce TLD était whois.dotmobiregistry.net. Suite à une migration technique, le service a été déplacé vers whois.nic.mobi, et le domaine original a été laissé à l'abandon jusqu'à son expiration en décembre 2023.[1]

L'acquisition de ce domaine pour seulement 20 dollars a permis aux chercheurs de prendre le contrôle d'une partie de l'infrastructure de confiance de l'Internet. Les résultats ont été immédiats :

- Plus de 135 000 systèmes uniques ont continué de contacter le serveur obsolète.[1]
- Plus de 2,5 millions de requêtes ont été enregistrées en quelques jours.[9]
- Des serveurs mail gouvernementaux et militaires (.gov,.mil) figuraient parmi les clients actifs, utilisant ces données pour valider la légitimité des communications entrantes.[1]

L'implication la plus grave a été la subversion du processus des Autorités de Certification (CA). Certaines CA utilisaient encore le serveur WHOIS obsolète pour vérifier la propriété d'un domaine lors de la délivrance de certificats TLS/SSL par validation e-mail. En contrôlant la réponse WHOIS, l'attaquant pouvait se désigner comme propriétaire légitime de n'importe quel domaine.mobi, permettant ainsi d'obtenir des certificats valides pour des domaines sensibles tels que google.mobi ou microsoft.mobi.[2]

Vulnérabilités de parsing et exécution de code

Le contrôle d'un serveur de télémétrie ou de WHOIS permet également d'exploiter des vulnérabilités de type "client-side". De nombreuses bibliothèques logicielles conçues il y a plus d'une décennie ne prévoyaient pas que l'infrastructure de confiance puisse devenir hostile.

- **CVE-2015-5243 (phpWHOIS) :** Cette bibliothèque utilise la fonction PHP eval() pour traiter les données renvoyées par le serveur WHOIS. En envoyant une chaîne de caractères spécifiquement formatée dans la réponse WHOIS, un attaquant peut obtenir une exécution de code à distance immédiate sur le serveur du client.[2]

- **Fail2Ban (CVE-2021-32749) :** Cet outil de sécurité populaire, qui surveille les logs pour bloquer les IP malveillantes, peut être configuré pour envoyer des e-mails d'alerte contenant des informations WHOIS. Une réponse malveillante peut déclencher une injection de commande lors de la génération de l'e-mail.[9]

Ces exemples soulignent que le système obsolète, en cherchant à se sécuriser ou à s'informer auprès de son infrastructure parente, devient l'instrument de sa propre perte.

La technique "Sitting Ducks" : L'exploitation systémique des configurations DNS

Le détournement de domaines ne nécessite pas toujours l'expiration du domaine lui-même, mais peut reposer sur des faiblesses de configuration DNS connues sous le nom de "Sitting Ducks". Cette attaque survient lorsqu'un domaine est délégué à un fournisseur DNS tiers, mais que la configuration chez ce fournisseur est absente ou invalide.[17]

Mécanisme de la délégation boiteuse (Lame Delegation)

Dans une configuration Sitting Ducks, le registraire pointe vers des serveurs de noms (Nameservers) faisant autorité, mais ces serveurs n'ont pas d'enregistrement pour le domaine en question. Un attaquant peut alors s'inscrire auprès du même fournisseur DNS et revendiquer le domaine sans aucune vérification de propriété, car le fournisseur DNS voit une requête légitime de délégation vers ses propres systèmes.[17]

Selon les données d'Infoblox, plus de 70 000 domaines ont été ainsi compromis au cours des cinq dernières années. Ce vecteur est particulièrement prisé par des groupes cybercriminels russes pour la distribution de malwares et la gestion de botnets.[18]

Groupe de Menace	Vecteur d'Attaque	Usage Principal
Vacant Viper	Sitting Ducks (404 TDS)	Distribution de spam, malwares et C2 pour RAT [18]
Vextrio Viper	Détournement DNS	Infrastructure de redirection pour programmes d'affiliation [18]
Hasty Hawk	Lame Delegation	Campagnes de phishing à grande échelle [18]

Horrid Hawk	Exploitation DNS	Fraude financière et vol d'identifiants [18]

L'aspect critique pour les systèmes en fin de vie est que ces domaines détournés sont souvent ceux utilisés par les anciens services de mise à jour ou de support. Lorsqu'un système EOL tente de résoudre l'adresse de son serveur de télémétrie, il reçoit une réponse authentique (du point de vue DNS) le dirigeant vers une infrastructure malveillante.[17]

Détournement de réseaux et "IP Zombies" : L'érosion du routage BGP

Le problème de l'obsolescence s'étend au-delà des noms de domaine pour toucher les ressources fondamentales du réseau : les adresses IPv4. En raison de la pénurie mondiale d'adresses, les blocs IP "hérités" (Legacy IP) appartenant à des entreprises disparues sont devenus des cibles de choix pour le détournement de trafic via le protocole BGP.[19]

Le cas Fiberlinkcc.com et IP Ocean

L'enquête sur le domaine fiberlinkcc.com a démontré comment une infrastructure de 30 ans peut être ressuscitée pour des activités illicites. Ce domaine, autrefois propriété de Fiberlink Communications (acquis par IBM en 2013), a été racheté par un acteur russe lié au fournisseur "IP Ocean".[9] Ce domaine a servi de pivot pour annoncer des routes BGP pour des blocs IP appartenant à Citigroup, AT&T et des organismes gouvernementaux canadiens qui n'étaient plus activement surveillés.[19]

Les "BGP Zombies" et l'instabilité du routage

Un "BGP Zombie" est une route qui persiste dans la table de routage globale (Default-Free Zone) même après avoir été retirée par l'émetteur original. Ces anomalies de routage peuvent durer de quelques minutes à plusieurs heures, créant des fenêtres d'opportunité pour l'interception de trafic.[20]

Pour un système en fin de vie, cette instabilité est fatale. Si le système possède des listes blanches d'IP pour ses communications de télémétrie, il continuera d'envoyer ses données vers ces blocs même s'ils ont été détournés. L'attaquant n'a pas besoin de compromettre le DNS s'il peut directement attirer le trafic IP vers ses propres serveurs.[19]

$$T_{convergence} \approx k \times \log(N)$$

Où $T_{convergence}$ est le temps de convergence du réseau après une modification BGP, k une constante liée aux délais de propagation et N le nombre de systèmes autonomes. Dans le cas

de routes zombies, ce temps peut être artificiellement prolongé, permettant une interception prolongée des flux de télémétrie.[20]

Les systèmes industriels (OT) et les objets connectés (IoT) illustrent parfaitement la thèse de la vulnérabilité par soi-même. Ces dispositifs sont souvent conçus pour être "déployés et oubliés", fonctionnant pendant des décennies sans mise à jour.[21]

Le protocole CWMP (TR-069) et l'exposition massive

Le protocole CWMP (CPE WAN Management Protocol) est utilisé pour la gestion à distance de millions de routeurs et d'appareils IoT. Une analyse a révélé que plus de 20 millions de dispositifs CWMP sont directement exposés sur Internet, fonctionnant souvent avec des logiciels obsolètes.[22]

- **Vecteur d'infection automatique :** De nombreux appareils sont configurés pour contacter périodiquement un serveur ACS (Auto Configuration Server). Si l'URL de l'ACS est obsolète et son domaine racheté, l'attaquant peut instantanément reconfigurer l'ensemble du parc d'appareils, injecter des backdoors ou transformer les dispositifs en nœuds de botnet.[22]
- **Identifiants par défaut et backdoors :** Des vulnérabilités comme CVE-2024-56316 montrent que des serveurs de gestion peuvent subir des dénis de service permanents ou des exécutions de code via des requêtes TR-069 malformées, affectant des millions de clients.[22]

Mirai et l'héritage de l'insécurité

Le botnet Mirai a marqué l'histoire en utilisant des scans automatiques pour infecter des systèmes IoT via des ports telnet et des identifiants par défaut. Ce qui est souvent ignoré, c'est que Mirai ciblait spécifiquement des dispositifs en fin de vie ou non maintenus. Une fois infectés, ces appareils contactaient des serveurs C2 via des domaines spécifiques. Même après le démantèlement des infrastructures Mirai originales, les appareils infectés continuent de tenter de joindre ces domaines. Quiconque reprend possession de ces noms de domaine hérite d'un botnet prêt à l'emploi.[23]

La menace des "Zombie Data" et de l'extorsion de chaîne d'approvisionnement

L'obsolescence ne frappe pas seulement le matériel et le logiciel, mais aussi les données résiduelles. Le concept de "Zombie Data" désigne les informations historiques stockées par des tiers longtemps après la fin de la relation commerciale.[3]

L'incident Mixpanel/Pornhub a démontré que des données analytiques de 2021 étaient encore présentes dans les systèmes d'un fournisseur en 2025, bien que le client ait cessé d'utiliser le

service.[25] Pour une entreprise utilisant des systèmes EOL, cela signifie que sa surface d'attaque s'étend à tous ses anciens fournisseurs dont l'infrastructure pourrait être compromise.

- **Extorsion contextuelle :** Les attaquants comme ShinyHunters ne se contentent plus de voler des numéros de cartes de crédit ; ils recherchent le contexte comportemental (habitudes de connexion, métadonnées de télémétrie) pour mener des campagnes de chantage ou de phishing hautement ciblées.[3]
- **Offboarding incomplet :** La plupart des programmes de gestion des risques tiers (TPRM) échouent car ils ne vérifient pas techniquement la suppression des données et la fermeture des flux de télémétrie lors de la mise hors service d'un système.[3]

Risque lié aux Données Zombies	Mécanisme de Menace	Impact
Rétention non autorisée	Échec du processus de purge des données chez le fournisseur	Violation de conformité (RGPD) et risque d'extorsion [25]
Profilage historique	Analyse des anciens logs de télémétrie	Identification des vulnérabilités non corrigées du système EOL [3]
Shadow API	Flux de données persistants vers des endpoints oubliés	Exfiltration continue de données sensibles [3]

La télémétrie comme vecteur de reconnaissance pour les APT

Pour les groupes d'attaquants parrainés par des États (APT), la télémétrie des systèmes obsolètes est une mine d'or pour la reconnaissance passive. En prenant le contrôle d'un nœud d'infrastructure abandonné, ils peuvent identifier précisément quelles organisations utilisent encore des technologies vulnérables.

L'écoute aux portes de l'infrastructure de confiance

Lorsqu'un système Windows 7 au sein d'une infrastructure critique contacte un serveur de télémétrie détourné, il révèle :

1. Son adresse IP publique (permettant la géolocalisation et l'identification de l'organisation).
2. Sa version précise de build et de patch (permettant de sélectionner l'exploit adéquat).
3. La liste des processus actifs ou des erreurs logicielles rencontrées.[6]

Cette méthode permet aux attaquants de cartographier des réseaux cibles sans jamais envoyer un seul paquet suspect vers la cible. C'est le système victime qui "se confesse" à l'attaquant.[3]

Stratégies de défense et perspectives de recherche

La lutte contre la vulnérabilité intrinsèque des systèmes EOL nécessite un changement radical d'approche. Puisque le système ne peut être corrigé, c'est l'environnement réseau qui doit devenir intelligent.

Vers une sécurité réseau consciente de l'obsolescence

Les travaux actuels se concentrent sur plusieurs axes pour atténuer ces risques :

- **Sinkholing Proactif :** Les organisations de sécurité comme la Shadowserver Foundation collaborent avec des chercheurs pour identifier et racheter préventivement les domaines de télémétrie obsolètes afin de rediriger le trafic vers des serveurs de recherche ("sinkholes") plutôt que vers des infrastructures criminelles.[1]
- **Micro-segmentation et Zero Trust :** Pour les systèmes hérités, le réseau doit appliquer une politique de "moindre privilège" absolu. Chaque requête de télémétrie doit être inspectée par une passerelle capable de valider non seulement la destination, mais aussi le contenu de la réponse.[28]
- **Remplacement des protocoles hérités :** Le passage de WHOIS à RDAP (Registration Data Access Protocol) et de l'OCSP temps réel aux mécanismes comme CRLite permet de réduire la dépendance aux infrastructures réseau potentiellement instables ou hostiles.[30]

Conclusion : La fin de l'innocence systémique

Le constat est sans appel : un système informatique en fin de vie, par ses mécanismes de télémétrie et ses dépendances hardcodées, est une bombe à retardement qui s'active dès sa connexion initiale. La transformation de domaines orphelins en systèmes d'infection généralisés n'est plus une hypothèse théorique, mais une réalité documentée affectant des gouvernements, des industries et des millions d'utilisateurs.

La sécurité de ces systèmes ne peut plus reposer sur la prudence de l'utilisateur, mais doit être traitée comme un problème d'infrastructure globale. L'obsolescence logicielle doit être gérée avec la même rigueur que le démantèlement de matières dangereuses : par une purge active des références, une surveillance étroite des ressources abandonnées et une isolation stricte des systèmes qui ne peuvent plus faire confiance à la "base" qu'ils ont été programmés pour appeler. La faillibilité intrinsèque est le prix de la connectivité permanente ; la vigilance infrastructurelle est la seule réponse viable.

Sources des citations

1. Expired Domains Allowed Control Over 4,000 Backdoors on ..., consulté le février 13, 2026, https://thehackernews.com/2025/01/expired-domains-allowed-control-over.html
2. Old WHOIS domain could have issued countless fraudulent TLS/SSL certificates | SC Media, consulté le février 13, 2026, https://www.scworld.com/news/old-whois-domain-could-have-issued-countless-fraudulent-tls-ssl-certificates
3. Supply Chain Vulnerabilities - Nocturnalknight's Lair, consulté le février 13, 2026, https://nocturnalknight.co/category/information-security/supply-chain-vulnerabilities/
4. Microsoft Security Intelligence Report, consulté le février 13, 2026, https://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf
5. German federal office publishes Windows 10 telemetry analysis | Hacker News, consulté le février 13, 2026, https://news.ycombinator.com/item?id=18527997
6. Windows® Administration at the Command Line, consulté le février 13, 2026, https://empyreal96.github.io/nt-info-depot/Misc/Command%20Line%20Administration%20for%20Vista%2C%202003%2C%20XP%20and%202000.pdf
7. Cybersecurity for SCADA Systems [2 ed.] 2020044734, 2020044735, 9781593705060, 9781593705053 - DOKUMEN.PUB, consulté le février 13, 2026, https://dokumen.pub/cybersecurity-for-scada-systems-2nbsped-2020044734-2020044735-9781593705060-9781593705053.html
8. Zones Of Control Perspectives On Wargaming 0262033992, 9780262033992 - DOKUMEN.PUB, consulté le février 13, 2026, https://dokumen.pub/zones-of-control-perspectives-on-wargaming-0262033992-9780262033992.html
9. We Spent $20 To Achieve RCE And Accidentally Became The ..., consulté le février 13, 2026, https://labs.watchtowr.com/we-spent-20-to-achieve-rce-and-accidentally-became-the-admins-of-mobi/
10. naorm/malware-text-db · Datasets at Hugging Face, consulté le février 13, 2026, https://huggingface.co/datasets/naorm/malware-text-db/viewer/default/train
11. Development of a tailored methodology and forensic toolkit for industrial control systems incident response - Calhoun, consulté le février 13, 2026, https://calhoun.nps.edu/server/api/core/bitstreams/ab27edfa-32d5-4bc9-86f9-d151c99d7377/content
12. China-Linked DKnife AitM Framework Targets Routers for Traffic Hijacking, Malware Delivery - The Hacker News, consulté le février 13, 2026, https://thehackernews.com/2026/02/china-linked-dknife-aitm-framework.html
13. Google Disrupts IPIDEA — One of the World's Largest Residential Proxy Networks, consulté le février 13, 2026, https://thehackernews.com/2026/01/google-disrupts-ipidea-one-of-worlds.html
14. Media Coverage | Page 9 | The Shadowserver Foundation, consulté le février 13, 2026, https://www.shadowserver.org/who-we-are/media-coverage/page/9/
15. [tl;dr sec] #248 - 10X Your Cloud Security, Secure by Design, AI OffSec

Benchmarks, consulté le février 13, 2026, https://tldrsec.com/p/tldr-sec-248
16. WHOIS Domain Control Validation Will Phase Out Starting Jan. 8 - The SSL Store, consulté le février 13, 2026, https://www.thesslstore.com/blog/whois-domain-control-validation-will-phase-out-starting-jan-8/
17. Eight-year-old “Sitting Ducks” DNS weakness exploited to hijack web domains with impunity, consulté le février 13, 2026, https://www.csoonline.com/article/3480542/eight-year-old-sitting-ducks-dns-weakness-exploited-to-hijack-web-domains-with-impunity.html
18. Known Brand, Government Domains Hijacked via Sitting Ducks ..., consulté le février 13, 2026, https://www.securityweek.com/known-brand-government-domains-hijacked-via-sitting-ducks-attacks/
19. Investigations | Expired and exploited: Reviving a 30 year old legacy ..., consulté le février 13, 2026, https://www.spamhaus.org/resource-hub/hijacking/expired-and-exploited-reviving-a-30-year-old-legacy-domain-for-hijacking/
20. bgp | Noise, consulté le février 13, 2026, https://noise.getoto.net/tag/bgp/
21. OT/IoT Security - Industry Insights - WWT, consulté le février 13, 2026, https://www.wwt.com/blog/otiot-security-industry-insights
22. Reading & Deepening for the CWMP Security Risk - Senki.org, consulté le février 13, 2026, https://www.senki.org/reading-deepening-for-the-cwmp-security-risk/
23. Case Studies of IoT Breaches: Detailed Analyses and Lessons Learned, consulté le février 13, 2026, https://breached.company/case-studies-of-iot-breaches-detailed-analyses-and-lessons-learned/
24. Automatic Verification and Execution of Cyber Attack on IoT Devices - MDPI, consulté le février 13, 2026, https://www.mdpi.com/1424-8220/23/2/733
25. Ramkumar Sundarakalatharan - Nocturnalknight's Lair, consulté le février 13, 2026, https://nocturnalknight.co/author/r-sundarakalatharangmail-com/
26. API Inventory - Wallarm Documentation, consulté le février 13, 2026, https://docs.wallarm.com/api-discovery/exploring/
27. Advances in Cybersecurity Incident Prevention and Analysis - Daniel Uroz - Ph.D. Dissertation - Universidad de Zaragoza, consulté le février 13, 2026, https://webdiis.unizar.es/~ricardo/files/PhDs/DUroz-PhD-Thesis.pdf
28. Zero Trust for Legacy Systems: Bridging the Gap Without Compromising Principles, consulté le février 13, 2026, https://msendpointmgr.com/2026/01/21/zero-trust-for-legacy-systems-bridging-the-gap-without-compromising-principles/
29. (PDF) NIST.SP.800-82r - Academia.edu, consulté le février 13, 2026, https://www.academia.edu/31524731/NIST_SP_800_82r
30. SSL Certificate Revocation Explained : What the End of OCSP Means for Website Security, consulté le février 13, 2026, https://shop.trustico.com/blogs/stories/ssl-certificate-revocation-explained-what-the-end-of-ocsp-means-for-website-security

31. Root Causes 94: Revocation Checking Through OCSP and CRL | Sectigo® Official, consulté le février 13, 2026, https://www.sectigo.com/root-causes/root-causes-94-revocation-checking-through-ocsp-and-crl