NOZOMI NETWORKS

Résumé exécutif

Rapport sur la sécurité des systèmes industriels et IoT

Une étude approfondie du paysage des menaces ICS

2e semestre 2022 | janvier 2023

Résumé exécutif

Le paysage des cybermenaces se transforme constamment à mesure que de nouvelles tactiques et de nouveaux acteurs malveillants apparaissent.

Avec les progrès technologiques, les cybercriminels utilisent des méthodes de plus en plus avancées pour accéder à des informations confidentielles ou lancer des cyberattaques perturbatrices. Avec l'émergence de l'Internet des objets (IoT), ils ont également accès à une pléthore d'équipements connectés et sont désormais en mesure de pénétrer dans les réseaux par de multiples points d'entrée.

Au cours des six derniers mois, le nombre de cyberattaques a augmenté de manière significative, provoquant des perturbations majeures, notamment dans les secteurs des transports et de la santé. Les chemins de fer en particulier ont fait l'objet d'attaques, ce qui a conduit à la mise en œuvre de mesures destinées à protéger les opérateurs ferroviaires et leurs biens.

Des hacktivistes ont par ailleurs utilisé des logiciels malveillants de type « wiper » (effaceurs des données) pour tenter de déstabiliser des infrastructures critiques et faire avancer leur agenda politique dans la guerre Russie/Ukraine.

Avec l'évolution et l'intensification des cybermenaces, il est important pour les entreprises de comprendre comment les auteurs de menaces ciblent les technologies industrielles et IoT, et les actions requises pour défendre les ressources critiques.

Dans ce rapport, nous couvrons les :

- **Cyberattaques** sur les infrastructures critiques au cours des 6 derniers mois
- **Hacktivistes** qui utilisent des logiciels malveillants pour lancer des attaques destructrices
- **Systèmes hospitaliers** de plus en plus ciblés
- **Cyberattaques contre les infrastructures ferroviaires** et les nouvelles directives de protection
- **Alertes sur les intrusions** qui affectent les environnements industriels
- **Catégories de logiciels malveillants** qui affectent les entreprises, les technologies industrielles et l'IoT
- **Recommandations** et **prévisions** pour 2023

PAYSAGE DES MENACES, 2e semestre 2022

Juillet à décembre 2022

Informations exclusives relevées dans les pièges posés par Nozomi Networks :

- **Protocoles avec identifiants codés en dur**
- **Pays les plus menaçants**
- **Identifiants les plus utilisés**
- **Adresses IP uniques des attaquants**
- **Adresses IP des attaquants**
- **Commandes les plus exécutées**

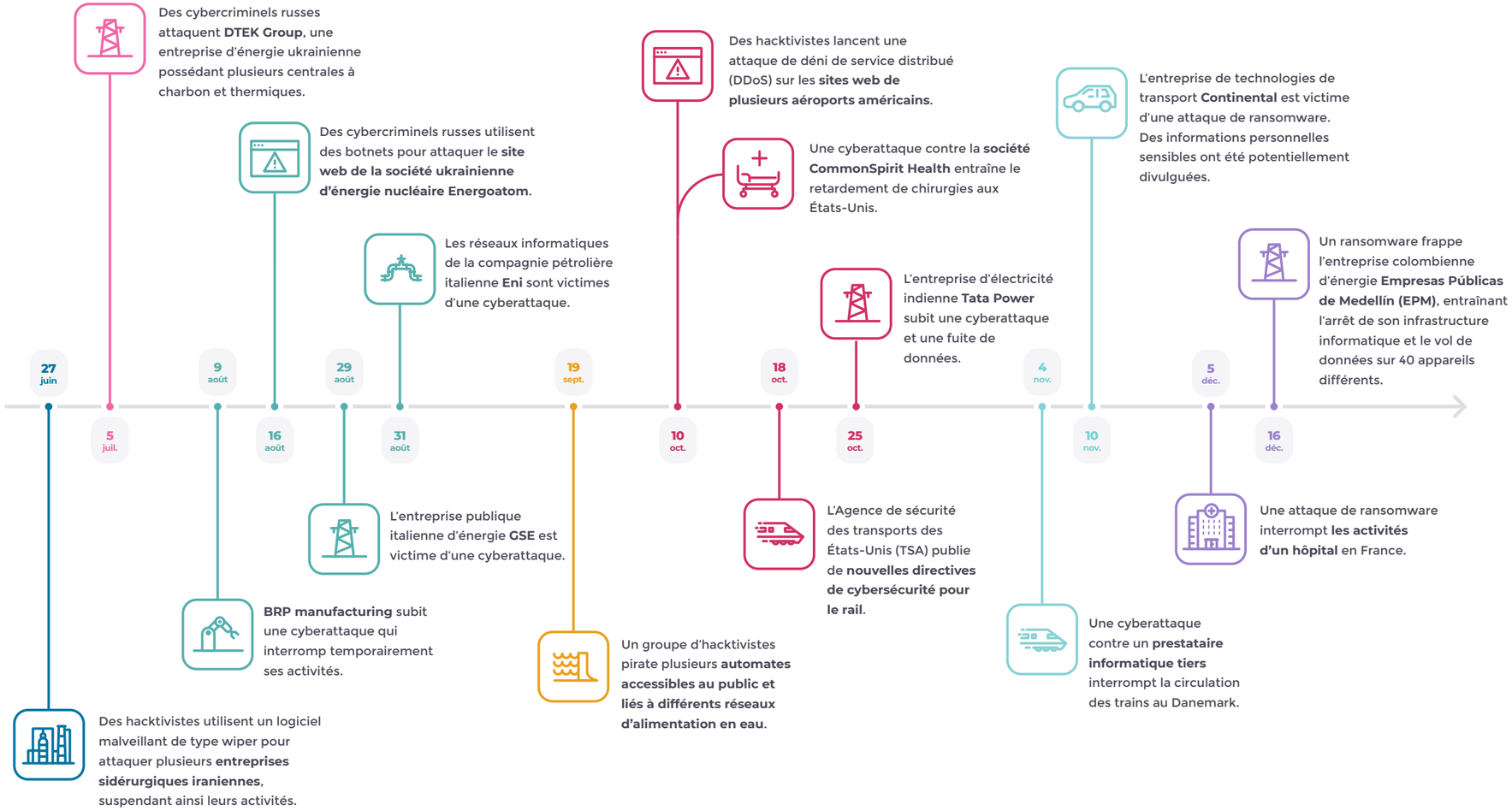
Chronologie des événements notables au cours du 2e semestre 2022 :

Cette chronologie résume les événements les plus importants de juillet à décembre 2022 : cyberattaques, nouvelles règlementations, logiciels malveillants, etc.

Au cours du premier semestre, nous avons constaté l'impact de la guerre Russie/Ukraine sur le paysage des cybermenaces.

Au cours de la seconde moitié de 2022, nous avons continué de noter des cyberattaques perturbatrices sur les infrastructures critiques, notamment les chemins de fer, les hôpitaux, la fabrication et l'énergie.

Les hacktivistes changent de tactique, passant du vol de données et des attaques de déni de service distribué (DDoS) à l'utilisation de logiciels malveillants d'effacement de données pour perturber les infrastructures critiques.



Dans ce rapport, nous dévoilons des données uniques collectées par les pièges de Nozomi Networks Labs. Ces systèmes de sécurité passive appelés « honeypots » sont utilisés pour détecter des attaques potentielles en imitant une ressource de valeur pour les attaquants. Nous avons observé ce qui suit au cours du second semestre 2022 :

- **Protocoles avec identifiants codés en dur :** Telnet est actuellement plus ciblé que SSH, avec 70 % pour Telnet contre 30 % pour SSH.
- **Pays les plus menaçants :** Les attaquants utilisent davantage des appareils aux États-Unis, en Chine et en Corée du Sud pour lancer des attaques dans d'autres pays.
- **Identifiants les plus utilisés :** Les identifiants par défaut continuent d'être utilisés, mais à une fréquence double ou triple, ce qui indique la présence de botnets supplémentaires qui tentent d'obtenir un accès.
- **Nombre maximum d'adresses IP uniques des attaquants :** Le nombre d'adresses IP uniques ciblant les technologies industrielles et IoT a connu des pics importants en juillet, octobre et novembre.
- **Adresses IP des principaux attaquants :** Des adresses IP malveillantes ont tenté d'accéder à nos pièges IoT, avec plus de 60 000 tentatives d'accès sur le point d'entrée principal, soit le double par rapport à notre précédent rapport.

TOP 4 DES COMMANDES LES PLUS EXÉCUTÉES :

1. enable
2. shell
3. sh
4. system

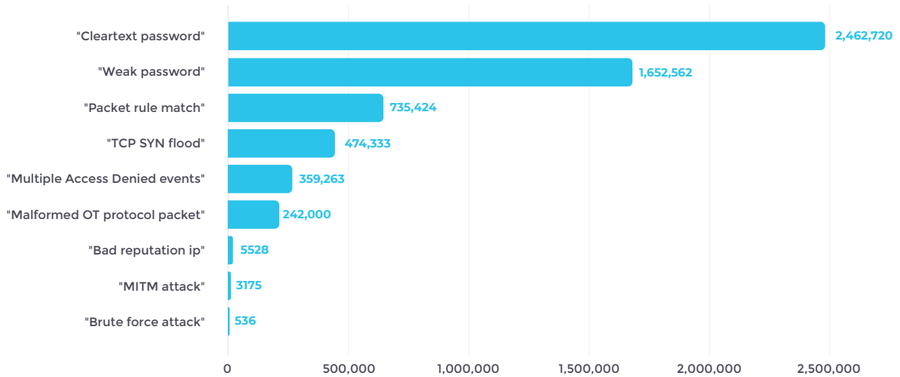
Ces commandes sont **plus répandues** par rapport aux autres commandes et **sont présentes dans les scripts de plusieurs familles de logiciels malveillants**.

Statistiques d'attaques dans le domaine des ICS

Juillet à décembre 2022

Types d'alertes pour intrusions les plus critiques

Les cybercriminels peuvent voler des **« mots de passe en clair »** et des **« mots de passe faibles »** pour obtenir un accès non autorisé aux appareils. Ces alertes, associées à de **« multiples événements de refus d'accès »** dans un court laps de temps, pourraient indiquer une attaque potentielle par force brute. D'autres alertes telles que **« TCP SYN flood »**, dans laquelle l'auteur de la menace inonde un serveur de demandes de connexion, pourraient également indiquer une tentative d'attaque de déni de service (DoS).



Voir le rapport complet pour toutes les données.

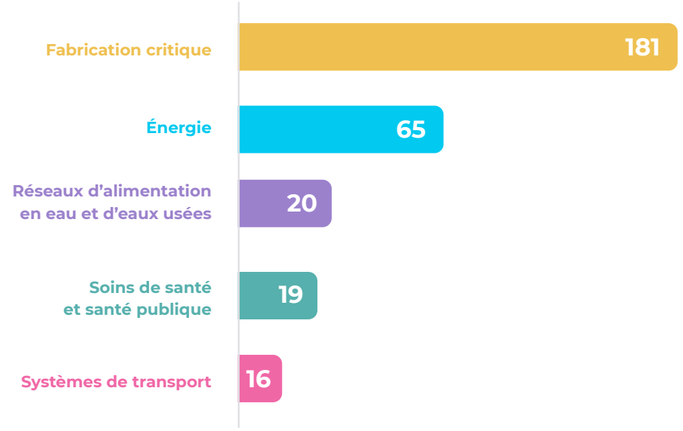
Catégories de logiciels malveillants les plus couramment détectés

Au cours des six derniers mois, les **chevaux de Troie** ont été les logiciels malveillants les plus couramment détectés ciblant les réseaux d'entreprise, les **outils d'accès à distance** ont ciblé les technologies industrielles et les **logiciels malveillants DDoS** ont ciblé les équipements IoT.

Le paysage des vulnérabilités

Nous avons analysé les avertissements ICS-CERT publiés par la CISA de juillet à décembre 2022.

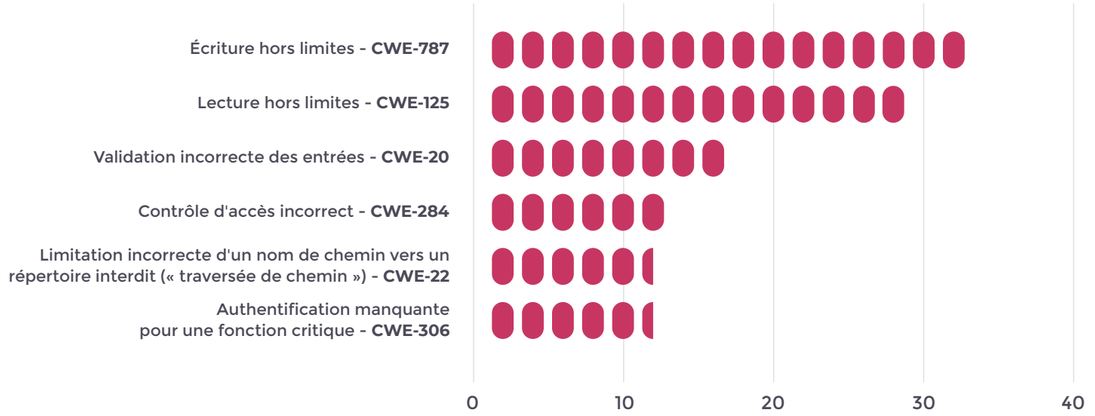
Les 5 secteurs les plus touchés par les vulnérabilités révélées



Deux nouveaux secteurs vulnérables sont apparus : les réseaux d'alimentation en eau et d'eaux usées, et les systèmes de transport.

Cela reflète les différentes cyberattaques que nous avons signalées cette année sur les installations de traitement des eaux et les systèmes ferroviaires/de transport en commun.

Ce graphique illustre les principales vulnérabilités courantes (CWE) associées aux CVE publiées au cours du second semestre 2022.



Les écritures hors limites (CWE 787) et les lectures hors limites (CWE 125) ont augmenté de manière significative par rapport au premier semestre de l'année.

La compréhension de ces failles de sécurité logicielles et matérielles courantes peut fournir aux entreprises des indications sur la manière de mieux sécuriser leurs réseaux.

Recommandations

Par rapport à ce que nous avons observé en 2022, le paysage des cybermenaces en 2023 devrait être marqué par une complexité et une sophistication continues, les attaquants faisant évoluer leurs stratégies d'exploitation des systèmes et des réseaux vulnérables.

Pour se protéger contre les menaces potentielles, les entreprises d'exploitation d'infrastructures critiques devraient accorder la priorité à des stratégies de défense proactives :

- Segmentation du réseau
- Découverte des ressources
- Gestion des vulnérabilités
- Correctifs
- Journalisation
- Détection sur les terminaux
- Renseignements sur les menaces

Les entreprises devraient protéger leurs systèmes de manière proactive dès maintenant, afin d'être en meilleure position pour combattre les cybermenaces qui pourraient survenir en 2023.

À quoi faut-il s'attendre en 2023 ?

1. Tactiques de menaces hybrides

Il sera de plus en plus difficile de classer les auteurs de menaces en fonction de leurs TTP et de leurs motivations, ce qui facilitait les attributions jusqu'à présent.

3. Exploitation des dispositifs médicaux

Outre l'utilisation de scanners pour exploiter des vulnérabilités, les cybercriminels peuvent accéder aux systèmes médicaux utilisés pour regrouper les données des dispositifs à des fins d'analyse et de surveillance étendue. Cette manipulation peut entraîner des dysfonctionnements, des mesures erronées, voire des surdoses dans l'administration automatique de médicaments.

5. Chatbots intelligents utilisés à des fins malveillantes

À mesure que ces systèmes deviennent plus sophistiqués, les acteurs malveillants pourraient les utiliser pour rédiger du code malveillant ou exploiter des vulnérabilités. Ils peuvent également être utilisés pour générer des textes de phishing/d'ingénierie sociale plus convaincants et grammaticalement corrects. Tout cela pourrait réduire le temps nécessaire à l'élaboration de campagnes de menaces ciblées, et augmenter la fréquence des cyberattaques.

2. Préparation et menaces quantiques

Alors que les cybercriminels commencent à engranger des données chiffrées en préparation au futur déchiffrement quantique, la CISA publie des conseils pour aider les entreprises à protéger leurs données maintenant afin de réduire les risques liés au déchiffrement quantique.

4. Point d'inflexion de la cyberassurance

Les cybercriminels se renseignent sur les polices d'assurance et adaptent leurs demandes de rançon pour qu'elles correspondent au montant d'un paiement par l'assurance. Cela pourrait soit entraîner une augmentation significative des cotisations, soit même assécher les ressources des assureurs, ce qui rendrait plus difficile les demandes d'indemnités.

6. Les professionnels de la cybersécurité devront acquérir de nouvelles compétences

Ils devront s'adapter rapidement à l'émergence de nouvelles menaces et trouver de nouveaux moyens de défendre leurs environnements.

Téléchargez le Rapport sur la sécurité des systèmes industriels et IoT

Nozomi Networks Labs analyse le paysage actuel des menaces et précise :

- Les récentes attaques de hacktivistes contre des infrastructures critiques
- Les tendances en matière de vulnérabilités et d'exploitation des équipements ICS, industriels et IoT
- Les prévisions concernant le paysage de la cybersécurité en 2023

Télécharger

nozominetworks.com

Cybersécurité et analytique pour tous vos objets connectés

Nozomi Networks est le leader de la sécurité et de la visibilité sur les systèmes industriels et IoT L'entreprise accélère la transformation digitale en unifiant la visibilité de la cybersécurité pour les plus grandes infrastructures critiques de, l'énergie, la fabrication, l'extraction minière, le transport, la construction automatisée dans le monde entier. Par l'innovation et la recherche, Nozomi Networks rend possible la gestion des cyber-risques grandissants grâce à la visibilité sur le réseau, la détection des menaces et l'expertise opérationnelle de grande qualité.

NN-SEC-RP-ES-2022-2H-FR-001