NOZOMI NETWORKS LABS

Résumé exécutif

Rapport sur la sécurité des systèmes industriels et IoT

Informations sur la cyberguerre, menaces, tendances et recommandations

1er semestre 2022 | août 2022

Introduction

Le paysage des cybermenaces est en constante évolution, et il est plus important que jamais de comprendre l'impact qu'il a sur votre entreprise. Au cours des six derniers mois, nous avons constaté une augmentation de la fréquence et de la complexité des attaques, ainsi que l'utilisation de nouvelles tactiques par les groupes de pirates. Des menaces qui étaient autrefois considérées comme improbables sont soudainement devenues monnaie courante.

Par exemple, des entreprises qui n'étaient pas ciblées auparavant par les rançongiciels se retrouvent aujourd'hui confrontées à ces attaques. Outre cette évolution, les cybercriminels continuent de dissimuler leurs activités malveillantes pour éviter qu'elles ne soient détectées par les solutions de sécurité.

Afin de renforcer la sécurité et minimiser les menaces futures, les entreprises ont besoin d'une visibilité en temps réel sur leur exposition aux cyber-risques, qui leur permette de prendre les décisions appropriées quant à la meilleure façon de se protéger.

Dans ce rapport, nous :

- **Examinons** l'état actuel de la cybersécurité.
- **Identifions** les principales tendances du paysage des menaces et proposons des solutions pour y faire face.
- **Récapitulons** la crise entre la Russie et l'Ukraine, en soulignant les nouveaux outils malveillants et les logiciels malveillants introduits, ainsi que la façon dont ce conflit peut nous éclairer sur les moyens à disposition des attaquants.
- **Présentons** les botnets ciblant l'Internet des objets (IoT), les indicateurs de compromis (IoC) correspondants, ainsi que les tactiques, techniques et procédures (TTP) des groupes de pirates.
- **Émettons** des recommandations et des analyses prévisionnelles.

PAYSAGE DES MENACES, 1er semestre 2022

Depuis le début de l'invasion de l'Ukraine par la Russie en février, nous avons noté :

Activité des hacktivistes

Groupes soutenus par des États et cybercriminels

Logiciel malveillant Wiper

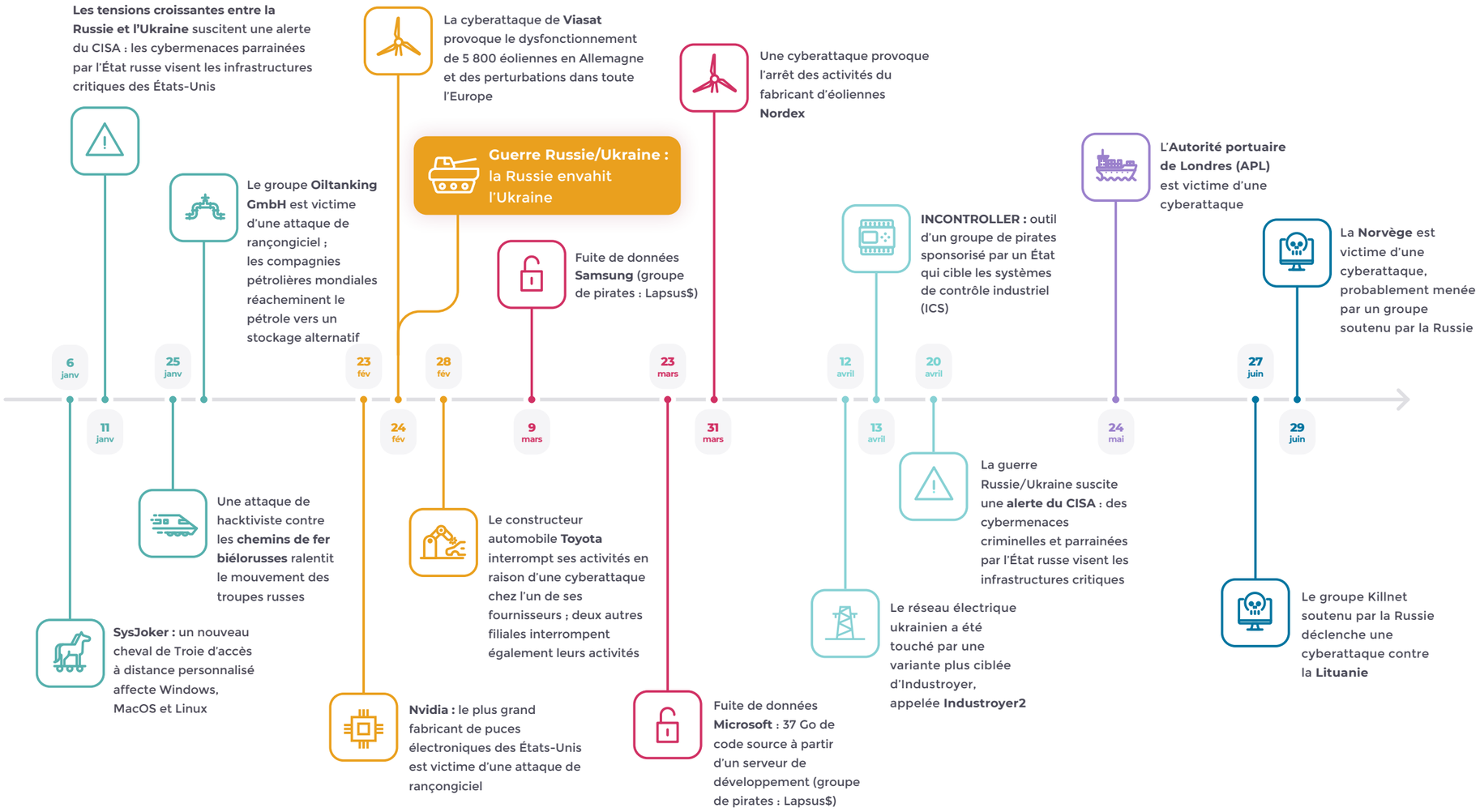
Industroyer2

Chronologie des événements notables du 1er semestre 2022

La chronologie de cette page présente plusieurs événements importants survenus entre janvier et juin 2022 qui ont façonné le paysage actuel des cybermenaces.

Depuis que la Russie a commencé son invasion de l'Ukraine en février 2022, nous avons constaté l'activité de plusieurs types de pirates, notamment des hacktivistes, des groupes soutenus par des États, et des cybercriminels.

Nous avons également constaté une forte utilisation des logiciels malveillants de type « wiper » (effacement de données) et une variante d'Industroyer baptisée Industroyer2, qui a été développée pour détourner le protocole IEC-104 couramment utilisé dans les environnements industriels.



Le paysage des botnets ciblant l'IoT

Les pièges de type « honeypot » de Nozomi Networks Labs collectent des données qui, une fois analysées, fournissent des informations intéressantes sur l'activité des groupes de pirates. Au cours du premier semestre 2022, nous avons observé les tendances suivantes :

- **Pays les plus menaçants :** La principale cyberactivité provient d'adresses IP associées à la Chine et aux États-Unis. Leurs surfaces d'attaque sont probablement plus importantes en raison de leurs industries technologiques et manufacturières sophistiquées.
- **Protocoles avec identifiants codés en dur :** Mirai est un botnet populaire qui utilisait Telnet initialement, mais qui a été modifié pour cibler SSH et d'autres protocoles depuis que ses auteurs ont rendu le code source public.
- **Principaux identifiants utilisés :** Les identifiants « root » et « admin » sont des cibles attrayantes évidentes utilisées dans de nombreux cas, car ils peuvent permettre aux cybercriminels d'accéder à toutes les commandes d'un système et aux comptes utilisateur.
- **Nombre maximum d'adresses IP uniques des attaquants :** D'après nos pièges collectant les adresses IP associées aux activités malveillantes, le mois d'avril a été le plus actif avec près de 5 000 adresses IP d'attaquants uniques recueillies.
- **Commandes les plus exécutées :** Nous avons identifié les 10 commandes les plus exécutées, avec `enable`, `shell`, `system` et `which ls` dans la liste.
  Environ 12 500 bots ont exécuté chacune de ces commandes.

Avril
a été le mois le plus actif pour les botnets avec près de

5 000
adresses IP uniques d'attaquants collectées.

Lisez le **Rapport complet** pour en savoir plus sur l'activité des botnets IoT au cours du premier semestre 2022.

Paysage des vulnérabilités

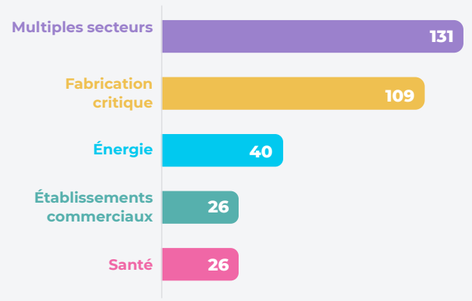
La sécurité de nombreux produits matériels et logiciels ICS est impactée par des vulnérabilités découvertes principalement par des chercheurs en sécurité. Au premier semestre 2022, 560 vulnérabilités et expositions communes (CVE) ont été publiées par l'ICS-CERT, dont 303 ont été nouvellement annoncées en 2022. 14 % de CVE en moins ont été signalées par rapport au second semestre 2021.

Parmi les CVE signalées, 131 affectaient plusieurs secteurs. La fabrication de produits critiques a été le secteur le plus directement touché, avec 109 CVE signalées. 40 pour l'énergie, et 26 pour les établissements de santé et commerciaux en troisième position. 60 fournisseurs différents ont été mentionnés dans les avis des CVE, avec 172 produits concernés. Le nombre de fournisseurs touchés a augmenté de 27 % et le nombre de produits touchés a augmenté de 19 % par rapport au second semestre 2021.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

560
CVE émises

SECTEURS LES PLUS TOUCHÉS



Recommandations

Il est de plus en plus nécessaire de prendre des mesures de sécurité proactives pouvant être mises en œuvre par les différentes parties prenantes d'une entreprise, notamment les équipes informatiques, les responsables de la conformité et les gestionnaires de risques, qui peuvent avoir des points de vue différents sur les questions de sécurité. Les pratiques de sécurité prioritaires devraient inclure :

- L'inventaire précis des ressources
- La mise en œuvre des tous derniers correctifs sur la technologie VPN
- La gestion des accès privilégiés
- L'utilisation d'une authentification multifacteur (MFA) renforcée, qui ne soit pas vulnérable au vishing et à l'échange de cartes SIM
- Le changement fréquent de mot de passe
- La formation des collaborateurs sur le vishing et l'ingénierie sociale en général

Mesures d'atténuation supplémentaires :

- **Sauvegardes :** Pour éviter qu'une attaque de rançongiciel ou de wiper n'entraîne une perte totale de données, sauvegardez régulièrement vos données, testez votre système de sauvegarde, et veillez à ce que votre sauvegarde soit stockée hors site et non sur le même réseau que vos serveurs.
- **Renseignements sur les menaces :** Le renseignement sur les cybermenaces est la pratique consistant à recueillir, analyser et diffuser des informations sur les cybermenaces, afin d'aider les entreprises à protéger leurs systèmes et leurs données. Ces informations peuvent inclure des signatures de logiciels malveillants, des vecteurs d'attaque et des indicateurs de compromis (IoC).
- **Sécurité du Cloud :** Veillez à ce que votre prestataire de services dans le Cloud jouisse d'une solide réputation et qu'il respecte les normes du secteur, telles que les certifications ISO 27001 ou SOC 1/2/3, qu'il chiffre les données stockées ou en mouvement, et qu'il utilise des outils de gestion des identités et de 2FA.
- **Détection des menaces :** La détection des menaces permet de détecter et de traiter les menaces potentielles en temps réel, et d'émettre des alertes sur des événements futurs. Les systèmes de détection des menaces recherchent les activités suspectes sur le réseau, telles qu'une quantité inhabituelle de trafic provenant d'une adresse IP ou un grand nombre de connexions à un service particulier. Cela peut se faire en surveillant le réseau, ou en l'analysant pour y rechercher des vulnérabilités connues.
- **Nomenclature des logiciels (SBOM) :** Elle vous apporte une visibilité sur le nombre de versions différentes de chaque composant existant et où elles sont utilisées, afin que vous puissiez suivre les changements au fil du temps et vous assurer qu'ils ne causent pas de problèmes avec d'autres composants. Elle peut également vous aider à comprendre quels composants sont plus exposés ou plus vulnérables que d'autres, et comment atténuer ces vulnérabilités. Bien que les SBOM ne soient pas encore largement utilisées, il est intéressant de suivre l'évolution de cette technologie.

PRINCIPALES MESURES D'ATTÉNUATION DES MENACES POUR RENFORCER LA SÉCURITÉ

Prévisions

Voici quelques-unes des principales tendances de cybersécurité que nous prévoyons pour le reste de l'année 2022, à partir de cette toute dernière analyse :

- Plus d'attaques ciblant les systèmes de contrôle industriel
- Les opérateurs de rançongiciels continueront de viser les entreprises d'infrastructures critiques
- Davantage d'attaques contre les grandes entreprises
- Vol de code source
- Plus de cyberpolitiques et de cybergouvernance, les initiatives privées et gouvernementales établies plus tôt cette année prenant forme

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 rançongiciels et de botnets IoT
- Les tendances en matière de vulnérabilités et d'exploitation des appareils ICS, industriels et IoT
- Les étapes à suivre pour améliorer vos stratégies de remédiation des cybermenaces

Télécharger

Nozomi Networks

La solution leader de sécurité et de visibilité pour les systèmes industriels et de l’IoT

Nozomi Networks accélère la transformation digitale en protégeant les infrastructures critiques, les entreprises industrielles et les gouvernements du monde entier contre les cybermenaces. Notre solution offre une visibilité exceptionnelle sur le réseau et les ressources, une détection des menaces et des informations pour les environnements industriels et l’IoT. Les clients comptent sur nous pour minimiser les risques et la complexité tout en maximisant la résilience.

NN-SEC-RP-ES-FR-2022-1H-001

nozominetworks.com