ᐱᓕᕆᔾᔪᑎᓄᑦ ᑐᓴᒐᒃᓴᑦ
Technical Bulletin
Qaritauyaliqutinut Takuyauyaghat
Bulletin technique

Rapport du gouvernement du Nunavut sur l’attaque par rançongiciel

14 juillet 2020

Table des matières

Objectif du présent document (éléments inclus et exclus)

Le présent rapport vise à examiner l'attaque du gouvernement du Nunavut (GN) par rançongiciel du 2 novembre 2019. Entièrement rédigé du point de vue de la Division de la gestion de l'information (GI) et des technologies de l'information (TI) du ministère des Services communautaires et gouvernementaux (SCG), il décrit le contexte de l'incident, l'attaque en soi et les mesures correctives prises pour rétablir les services.

Le présent rapport ne présente pas les répercussions de l'incident sur les autres ministères ou organismes du GN. Pour en savoir plus à ce sujet, veuillez vous informer auprès des entités concernées.

Contexte

Les TI sont considérés comme des services gouvernementaux stratégiques. La Division de la GI et des TI des SCG, dirigée par le directeur général de l'information pour la fonction publique, est la seule direction du GN qui se consacre entièrement à fournir des services de TI au gouvernement dans l'ensemble du territoire. Les services de TI pour les ministères du GN et, de fait, pour les résidents du Nunavut, sont offerts au moyen d'un réseau composé de services à large bande par satellite efficaces et fiables, de réseaux de câbles à fibre optique ainsi que d'autres infrastructures de soutien.

Situées dans 25 localités du Nunavut, ainsi que dans deux bureaux du sud du pays (Ottawa et Winnipeg), les installations du GN donnent toutes une impression d'isolement géographique en raison de leur éloignement et de la vaste distance qui les sépare. Les communications entre les bureaux gouvernementaux se font uniquement par satellite : les connexions terrestres sont établies au moyen de services spécialisés offerts par des installations d'Ottawa et de Saskatoon. Par conséquent, les services de TI – en particulier, les services de télécommunication – offerts au GN et aux Nunavummiuts sont parmi les plus chers et les plus limités au pays.

Malgré ces grands défis, la Division de la GI et des TI des SCG réalise des progrès vers l'amélioration des infrastructures informatiques du GN, qui consiste à élargir considérablement les applications de TI, l'accès aux réseaux et les services de connexion internet pour les programmes ministériels dans toutes les localités du Nunavut.

Attaque du gouvernement du Nunavut par rançongiciel

Le samedi 2 novembre 2019, l'ensemble du réseau informatique du GN a été attaqué par une nouvelle catégorie sophistiquée de rançongiciel, qui a chiffré des fichiers de différents serveurs, postes de travail et dispositifs de stockage externes sur tout le territoire. Le même jour, une fois la menace décelée, la Division de la GI et des TI a mis le réseau hors service, recensé les services touchés, mis en œuvre un plan d'intervention d'urgence et communiqué avec des spécialistes de la cybersécurité et les fournisseurs de logiciels pour déployer les mesures de rétablissement.

Les ministères du GN ont déclenché des plans d'urgence pour continuer d'offrir les services essentiels aux Nunavummiuts en réduisant les interruptions au minimum.

Dans une publication sur Facebook à propos de l'attaque du GN, un employé a fourni une image de la demande de rançon telle qu'elle s'affichait à l'écran des postes de travail (voir l'**annexe A :** Demande de rançon affichée sur les ordinateurs qui a été publiée).

L'équipe de direction a décidé de ne pas payer la rançon, puisque rien ne garantissait que toutes les données du GN pourraient être récupérées ni que ses systèmes seraient en sécurité dans l'avenir. À la suite de cette décision, la Division de la GI et des TI a formé des équipes d'intervention pour rétablir le réseau, récupérer la totalité des données des systèmes en utilisant les copies de sauvegarde, et reconfigurer les ordinateurs des utilisateurs finaux.

Les sous-ministres ont été convoqués à une réunion d'urgence visant à les mettre au fait de la situation. Toutes les unités opérationnelles ont déployé leur plan de continuité des opérations (PCO) pour assurer le maintien des services aux Nunavummiuts. La Division de la GI et des TI a offert de l'assistance aux ministères pour veiller à ce que la mise en œuvre de leur PCO se poursuive. Sous la direction du Comité des sous-ministres, on a recensé les services essentiels afin de déterminer l'ordre de priorité des services à rétablir (santé, services à la famille, justice, éducation et finances).

Une stratégie de communication a été mise en œuvre afin que les sous-ministres se réunissent deux fois par jour pour échanger des renseignements, prendre des décisions importantes et faire le point sur les efforts de reprise.

Intervention et enquête sur l'attaque par rançongiciel du gouvernement du Nunavut

La Division de la GI et des TI a pris des mesures pour assurer une reprise complète après l'attaque par rançongiciel.

Elle a créé un plan pour rétablir complètement le réseau et les systèmes du GN et remettre en état les postes de travail des 25 localités du Nunavut et des bureaux régionaux d'Ottawa et de Winnipeg.

Chaque étape du plan comportait des tâches spécifiques pour la Division de la GI et des TI, qui pouvait aussi faire appel aux ressources des ministères afin d'obtenir de l'assistance, au besoin.

La stratégie consistait à exécuter en parallèle une approche par étape en répartissant toutes les ressources disponibles (Division de la GI et des TI et ministère) entre un groupe de rétablissement des systèmes dorsaux et trois équipes affectées à la remise en état des ordinateurs, soit une par région du Nunavut (Kitikmeot, Kivalliq et Qikiqtaaluk). La « cellule de crise » établie à Iqaluit servait de centre de commande pour rétablir les systèmes du GN et offrir du soutien aux équipes à distance.

Cellule de crise d'Iqaluit.

Membres de la Division de la GI et des TI montant à bord d'un aéronef en direction de Grise Fiord pour reconfigurer tous les postes de travail de la localité.
Des membres de la Division se sont rendus dans les 25 localités du Nunavut pour reconfigurer les ordinateurs des utilisateurs du GN.

- L'équipe de gestion de la Division de la GI et des TI, la sous-ministre et le ministre des SCG ont assumé d'autres responsabilités :
    - Le ministre des SCG s'est chargé d'informer le Conseil des ministres et les députés de l'Assemblée législative du progrès de la reprise.
    - La sous-ministre des SCG a dirigé le comité de surveillance des sous-ministres pour la planification et l'exécution des activités de reprise.
    - Le directeur général de l'information pour la fonction publique a agi à titre de point de contact unique, assurant la liaison entre la Division de la GI et des TI et les ministères, ainsi qu'entre les sous-ministres et les équipes des Communications.
    - Le directeur de l'information gouvernementale et de la planification a dirigé la remise en état des terminaux des clients (approvisionnement, reconfiguration des postes de travail et déploiement communautaire) dans toutes les localités.
    - Le directeur des technologies de l'information et de la communication a dirigé l'enquête, la reconfiguration, le rétablissement des serveurs et la reprise des services dans toutes les localités.

L'équipe de gestion de la Division de la GI et des TI s'est réunie pour évaluer l'état d'avancement de la reprise. Bien que le GN compte des spécialistes parmi son personnel, on a décidé de faire appel à des experts de l'industrie spécialisés dans les attaques de maliciels pour participer au processus d'enquête et de reprise. De plus, la GRC a lancé une enquête sur l'attaque des systèmes du GN.

Munie des conclusions de l'enquête, qui lui ont été fournies rapidement, l'équipe de rétablissement des systèmes dorsaux de la Division de la GI et des TI – en collaboration avec Teknicor, un fournisseur de services gérés – a commencé les activités de reprise des réseaux et des systèmes du GN. En parallèle, les équipes de rétablissement des systèmes frontaux de la Division de la GI et des TI ont commencé la planification et le déploiement de Windows 10 sur les postes de travail des 25 localités du Nunavut ainsi que des bureaux d'Ottawa et de Winnipeg. La Division de la GI et des TI a travaillé avec différents fournisseurs, comme FireEye Mandiant, une entreprise spécialisée en cybersécurité, et l'équipe DART (*Detection and Response Team*) de Microsoft, composée d'éminents experts de la sécurité et de la reprise des systèmes, qui ont validé le plan de reprise du GN au fil de sa mise en œuvre. Les fournisseurs ont aussi offert des outils supplémentaires et de l'assistance durant le déploiement des mesures de sécurité appropriées (renforcement) dans l'environnement et des nouvelles solutions infonuagiques de sécurité et de productivité (voir l'**annexe B :** Rapport de Microsoft).

L'exécution de la reprise était un effort collectif. Certaines personnes se sont vu assigner différentes tâches qui ne font pas partie de leur description de poste habituelle, car la Division de la GI et des TI devait affecter des ressources à des tâches qu'elles n'effectueraient pas autrement et qui nécessitaient du renfort. La priorité était de réactiver le centre de données principal d'Iqaluit de sorte que toutes les localités puissent s'y connecter pour utiliser les applications opérationnelles essentielles. Le rétablissement des applications du GN à Iqaluit a commencé par la réactivation de la messagerie vocale, des systèmes, des applications et des données des utilisateurs. L'équipe parallèle a entamé les préparatifs pour reconnecter toutes les autres localités. Les activités de rétablissement comprenaient une reconfiguration complète du réseau du GN dans toutes les localités ainsi que de ses systèmes dorsaux, l'installation de Windows 10 sur tous les ordinateurs du GN dans toutes les localités, et le déploiement de nouveaux outils de productivité infonuagiques.

Le GN a des systèmes de sauvegarde très sophistiqués qui sont utilisés quotidiennement pour protéger ses données dans tout le territoire ainsi que dans tous ses centres de données. La Division de la GI et des TI a créé un environnement séparé, déconnecté de tout le reste, pour récupérer les données de sauvegarde et s'assurer que les données gouvernementales sont bien protégées. Les équipes ont trié les données de sauvegarde au moyen de différents filtres de FireEye pour confirmer qu'elles ne comprenaient pas des fichiers infectés ou compromis. Cette mesure s'est avérée efficace. Ce processus très rigoureux a pris beaucoup de temps, mais il était essentiel à la réussite de la reprise. Lorsqu'il a été confirmé que les données de sauvegarde étaient sures, actuelles (fin de la journée du 1er novembre 2019) et accessibles, on a décidé de récupérer et de rétablir les données gouvernementales.

Il y a eu quelques exceptions :

- Il a fallu rétablir les données du système de comptabilité Multiview du Collège de l'Arctique du Nunavut en date de la fin de journée du 31 octobre 2019 : on a donc dû rentrer manuellement les données d'une journée.

- Les données stockées sur les lecteurs « C » que les utilisateurs n'ont pas sauvegardées dans des dossiers personnels ou partagés du réseau.

- Les données stockées sur des clés USB ou des disques durs externes que les utilisateurs n'ont pas sauvegardées dans des dossiers personnels ou partagés du réseau.

Applications du GN

Dans le cadre du processus de rétablissement, il a été décidé que pour être intégrées au réseau, les applications devaient satisfaire à de nouvelles exigences strictes en matière de sécurité.

1. Les applications du GN qui satisfaisaient aux nouveaux critères de sécurité ont été réinstallées et remises en ligne dans l'ordre de priorité établi, en commençant les applications liées aux services essentiels, suivies des applications nécessaires aux ministères, puis des autres applications, au fur et à mesure qu'elles devenaient disponibles.

2. Les anciennes applications du GN qui ne satisfaisaient pas aux nouveaux critères de sécurité ont été stockées dans un emplacement sécuritaire du réseau (derrière des pare-feux) auquel l'accès est strictement limité. La Division de la GI et des TI a travaillé pour réactiver ces applications et avisé les ministères clients lorsqu'il était impossible de les intégrer au réseau dans leur état initial pour des raisons de sécurité.

   Il a été recommandé de collaborer avec les ministères clients et les fournisseurs d'application afin de trouver une solution durable pour les applications ministérielles non conformes. Il s'agissait soit de les améliorer pour qu'elles satisfassent à nos nouvelles exigences relatives à la sécurité, soit de les remplacer.

3. Transfert des applications de productivité vers le nuage :
   a) La Division de la GI et des TI a déterminé que la façon la plus efficace et sécuritaire de rétablir certaines applications de l'organisation était de les convertir en solutions infonuagiques, notamment les suivantes :

i) Office 365
    1. Courriel
    2. Microsoft Teams
    3. OneDrive
    4. SharePoint

La solution de services de courriel sur place a été remplacée par la solution infonuagique Office 365 dans tout le territoire. Durant le déploiement d'Office 365, la Division de la GI et des TI a activé l'application Microsoft Teams pour les messages instantanés et les vidéoconférences, ainsi que SharePoint Online et OneDrive pour le partage de fichiers et la collaboration.

<u>Postes de travail du GN</u>

Parallèlement aux activités liées aux systèmes dorsaux, les équipes du GN chargées des systèmes frontaux de toutes les régions ont commencé à reconfigurer les postes de travail du GN. Comme la majorité des localités où se trouvent des installations du GN n'ont pas de service de dépannage, le personnel a pris des vols nolisés et réguliers pour effectuer la remise en service dans toutes les localités. Des équipes ont été formées dans les régions du Qikiqtaaluk, du Kivalliq et du Kitikmeot pour gérer la reconfiguration des postes de travail. Au cours du passage à Windows 10 et de l'installation des nouvelles mesures de sécurité, on a constaté que plus de 1 400 postes de travail ne pouvaient pas les exécuter ou offraient une piètre performance aux utilisateurs, et ont donc été remplacés.

Installations de reconfiguration et de remplacement d'Iqaluit, de Rankin Inlet et de Cambridge Bay : tous les postes de travail ont été récupérés, puis reconfigurés ou remplacés.

La logistique de l'approvisionnement des postes de travail, leur expédition vers les localités et la réservation de vols et d'hôtels représentaient des défis de taille. On a réservé des vols nolisés et réguliers pour optimiser les interventions des équipes, de sorte à remettre rapidement en service les systèmes de toutes les localités. Les équipes se sont heurtées à de nombreux obstacles, comme des retards causés par des intempéries, des aéronefs ayant des problèmes mécaniques, des problèmes liés à l'hébergement et une évaluation médicale d'urgence sur l'un des vols nolisés, pour n'en nommer que quelques-uns. Le 21 décembre 2019, la connexion de base aux systèmes du GN de toutes les localités du Nunavut était rétablie.

Cout

En réponse à l'attaque par rançongiciel, le GN a engagé des dépenses liées aux heures supplémentaires du personnel, aux ressources contractuelles, au remplacement de plus de 1 400 postes de travail, à la réservation de vols nolisés et réguliers, aux licences des nouveaux services infonuagiques et au recours à des services de soutien à la sécurité de tiers. Le cout associé à la Division de la GI et des TI des SCG pour l'intervention en réponse à l'attaque par rançongiciel durant la période du 2 novembre 2019 au 31 mars 2020 s'élève à 5 439 950 dollars pour l'ensemble du territoire.

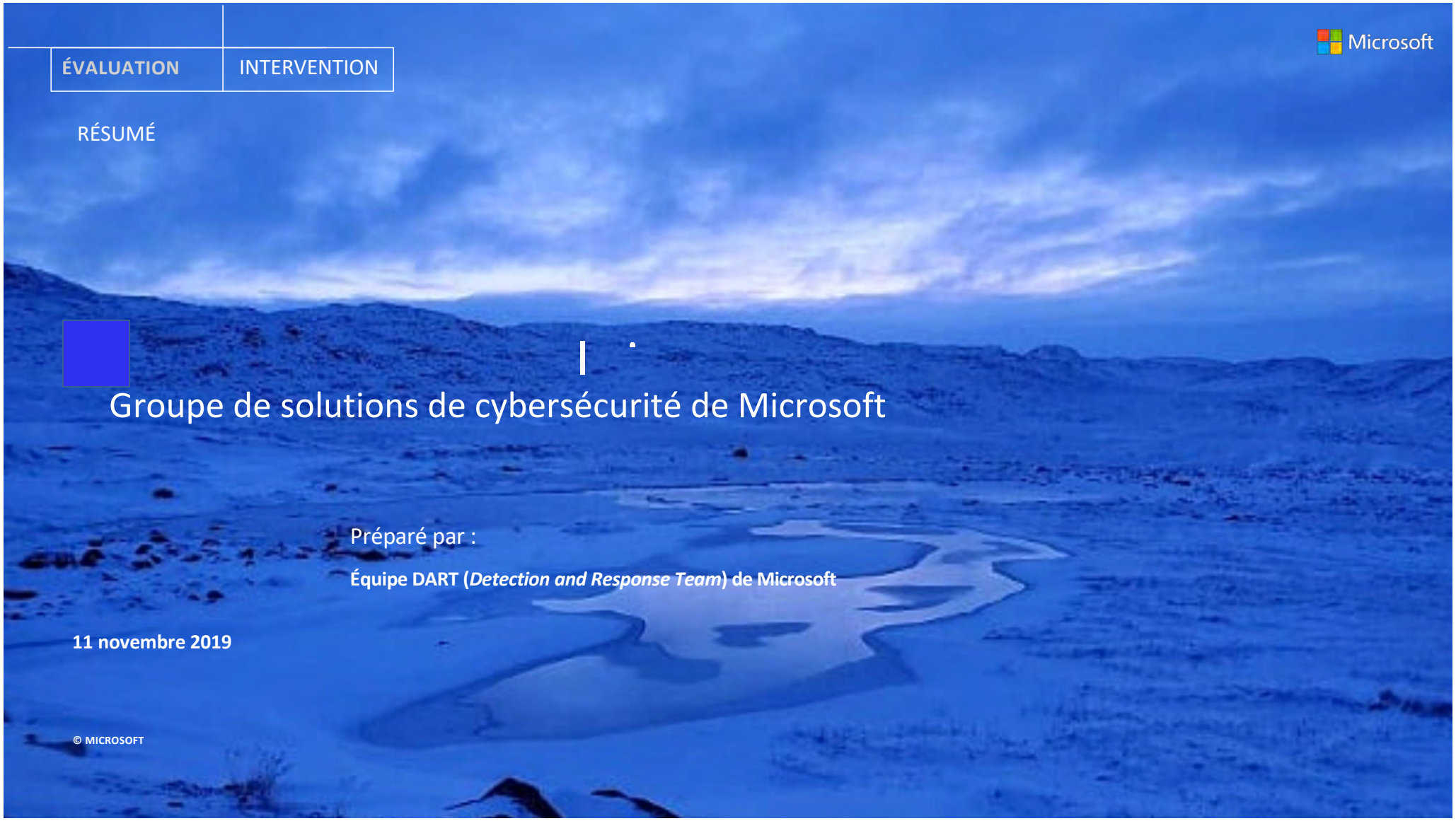
Notre personnel est notre force.

L’équipe du GN

Le 2 novembre 2019, le GN a subi une attaque par rançongiciel sophistiqué. En six semaines, la connexion de base était rétablie dans toutes les localités du Nunavut et les deux bureaux du sud du pays, et les applications étaient graduellement remises en service. La réponse du GN à l’attaque et son rétablissement ont été formidables, et c’est au personnel que nous devons cette grande réussite.

Annexe A : Demande de rançon affichée sur les ordinateurs qui a été publiée

```
[illegible] - Notepad
File  Edit  Format  View  Help
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorythm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

        DO NOT RESET OR SHUTDOWN - files may be damaged.
        DO NOT RENAME OR MOVE the encrypted and readme files.
        DO NOT DELETE readme files.
        DO NOT use any recovery software with restoring files overwriting encrypted.
        This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at your personal page:

        1. Download and install Tor Browser: [redacted]
        2. After a successful installation, run the browser and wait for initialization.
        3. Type in the address bar:

           [redacted]

        4. Follow the instructions on the site
        5. You should get in contact in 48 HOURS since your systems been infected.
        6. The link above is valid for 14 days.
           After that period if you not get in contact link and the key for your data
           would be erased completely.
        7. Questions? e-mail: [redacted]
           If email not working - new one you can find on a tor page.

The faster you get in contact - the lower price you can expect.
[redacted]
```


ÉVALUATION
INTERVENTION
Microsoft
RÉSUMÉ
Groupe de solutions de cybersécurité de Microsoft
Préparé par :
Équipe DART (*Detection and Response Team*) de Microsoft
11 novembre 2019
© MICROSOFT

Résumé

Au moment où l'équipe DART de Microsoft est arrivée, le 11 novembre, un incident lié au rançongiciel DoppelPaymer s'était récemment produit (1er novembre). L'équipe DART devait non seulement offrir l'expertise habituelle en matière d'intervention en cas d'incident, mais aussi assurer la continuité et la reprise des activités.

Selon les données recueillies, le niveau de risque de l'environnement est **FAIBLE**. Cette cote est établie d'après les éléments suivants :

- *Confinement des appareils et comptes de niveau 0 :* Des mesures ont été prises pour protéger les appareils et comptes de niveau 0 des attaques et pour renforcer les contrôleurs de domaine.
- *Administrateurs locaux :* La solution de mot de passe administrateur local (LAPS) a été déployée dans l'organisation, ce qui réduit considérablement les possibilités de mouvements latéraux pour les maliciels et les adversaires humains déterminés.
- *Azure et Office 365 :* La suite Office 365 a été déployée, et les courriels ont été réactivés. On a aussi déployé les solutions de protection avancée contre les menaces Microsoft Defender et Azure, ainsi que Microsoft Cloud App Security et Azure Sentinel afin de pouvoir surveiller les activités dans l'ensemble de l'organisation.

Le « cas primaire » de cet incident est un poste de travail où un utilisateur a cliqué sur un lien dans un courriel de harponnage. Le maliciel de vol d'identifiants Dridex a été téléchargé, et deux comptes système cachés ont été utilisés pour le déploiement latéral de DoppelPaymer.

Dans le cadre de cette intervention, des mesures ont été prises pour dresser la liste des actifs de niveau 0 (comptes et ordinateurs) et les protéger au moyen de méthodes éprouvées, ainsi que pour veiller à ce que 1) les titulaires de comptes niveau 0 ne puissent pas se connecter à des ordinateurs de niveau inférieur, et 2) les titulaires de comptes de niveau inférieur ne puissent pas se connecter à des ordinateurs de niveau 0.

N.B. : Les cotes sont des indicateurs « ponctuels » de la posture de sécurité relative du client, mais ne garantissent pas la protection contre les atteintes à la sécurité.

Incident : Chronologie

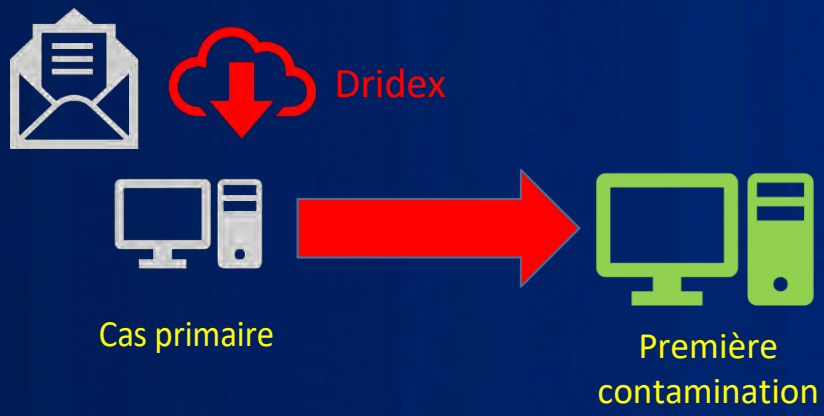
Cas primaire

Incident : Chronologie

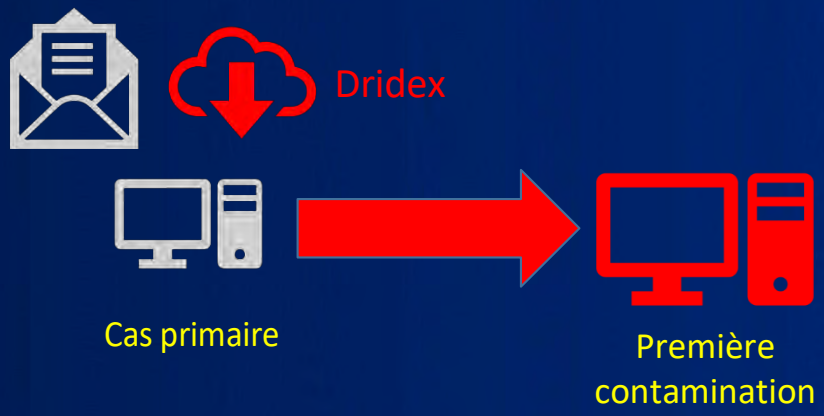
Cas primaire

Incident : Chronologie

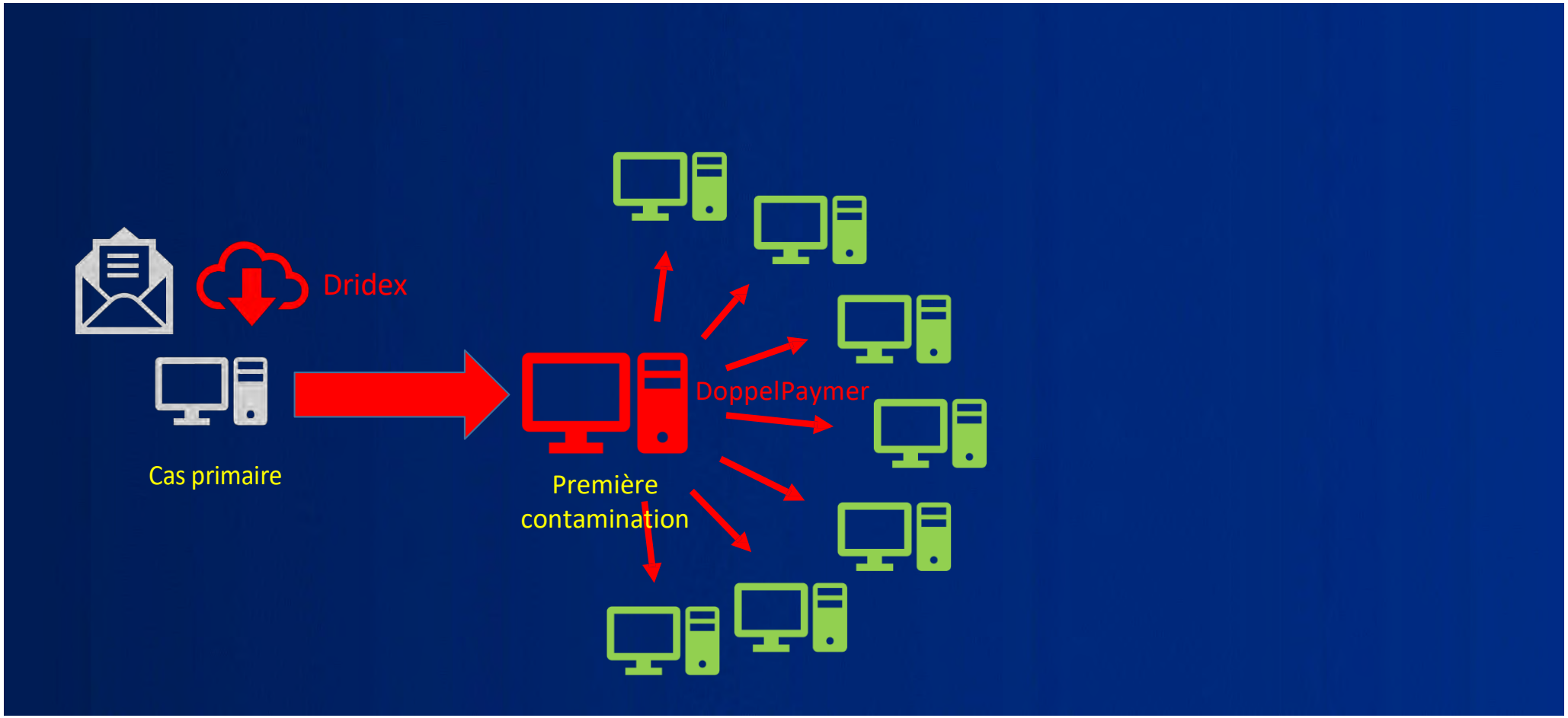
Incident : Chronologie



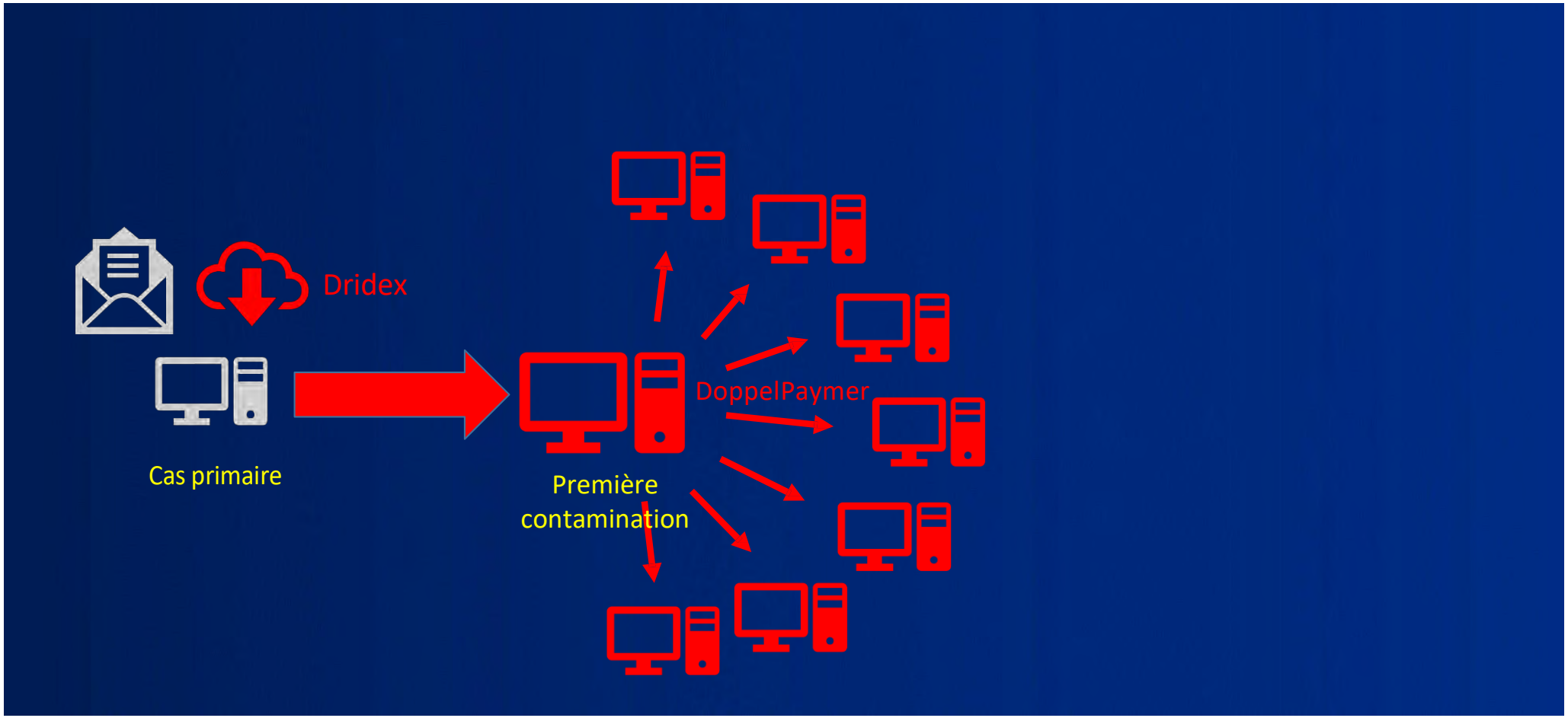
Incident : Chronologie



Incident : Chronologie

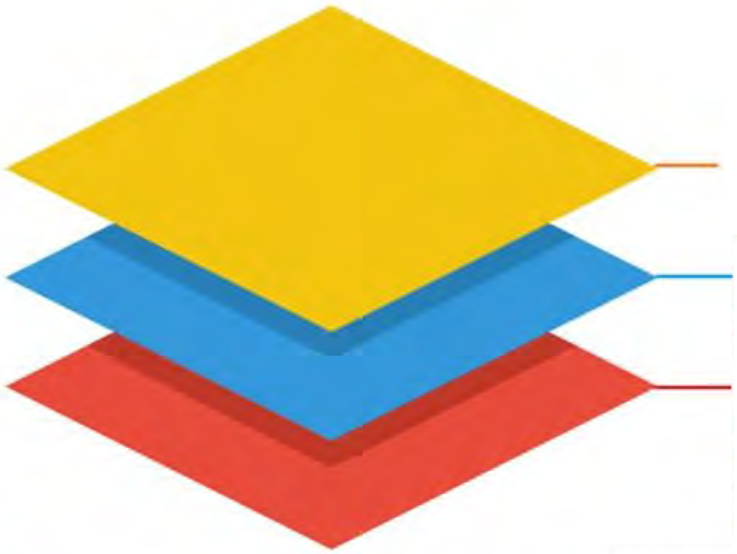


Incident : Chronologie



Recommandations et prochaines étapes

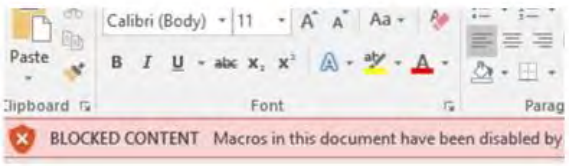
Protection en profondeur



Hygiène de messagerie (identité de l'expéditeur : vérification de l'expéditeur, de sa réputation et du contenu du message)

Stratégie de groupe sur la suite Office 2013-2016 pour empêcher l'exécution de macros de documents téléchargés en ligne (prévention des maliciels Emotet et Trickbot)

Formation des utilisateurs : chaque employé ou fournisseur est responsable de la sécurité Message d'avertissement dans les courriels entrants



Expéditeur : Elliot Munro <elliot@externaldomain.com>
Envoyé le : Vendredi 27 octobre 2017 16:14:53
Destinataire : Elliot Munro **Objet :** Test
ATTENTION : Ce courriel provient d'un expéditeur externe. Ne cliquez sur aucun lien et n'ouvrez pas de pièces jointes, sauf si vous reconnaissez l'expéditeur et savez que le contenu est sûr.

Multiples couches et pour une contrôles protection collective.

Si une couche échoue, les autres continuent d'assurer une protection et d'atténuer les risques.

#ProtectionEnProfondeur

- Mettre à jour tous les domaines avec vérification du domaine de l'expéditeur (trois domaines sont en attente du SPF; la norme DKIM ne s'applique pas à tous les domaines).
- Retirer les courriels et les boites de réception de tout compte d'administrateur général.
- Correctif : Un administrateur de comptes de domaine était demandé pour la synchronisation d'annuaires lorsque seul l'administrateur de l'organisation est requis (créer une demande Support Microsoft).
- Déploiement d'Exchange sur place pour les numériseurs et le transfert de courriels internes.
- Établir une règle de transport pour les messages entrant afin de demander aux utilisateurs d'internet de faire preuve de prudence avant de cliquer sur des liens ou d'ouvrir des pièces jointes.
- Déployer des objets de stratégie de groupe pour empêcher l'exécution de macros de documents téléchargés en ligne (formation supplémentaire pour les utilisateurs et les groupes qui doivent ouvrir des documents avec macros envoyés par courriel).

#RéactionAuxIncidents (les images parlent plus que les courriels)

- Tableaux de bord de sécurité en ligne de Microsoft (Azure Advanced Threat Protection, solution de protection avancée contre les menaces Microsoft Defender, Cloud App Security, Office 365, Azure Active Directory).
- **Créer un écran unique** avec [l'interface de programmation Graph Security/Power BI] comprenant des indicateurs de comportements suspects : écran ACL dans l'aire des TI, Raspberry Pi, etc
- **Poser des affiches aux entrées principales et aux ascenseurs** sur le rôle de responsable de la sécurité (ne pas utiliser d'identifiants de l'organisation sur des sites de tiers, ni cliquer sur les liens des courriels suspects).
- Imprimer des copies du document *Mitigating Pass-the-Hash and Other Credential Theft* (en anglais seulement) et en distribuer à tous les ingénieurs du soutien informatique ainsi qu'aux nouveaux employés pour expliquer l'isolement des tiers et du réseau ainsi que l'approche consistant à prendre pour acquis qu'il y a intrusion.
- Lien de téléchargement : http://aka.ms/drew.

Il est recommandé de consulter un technicien d'entretien principal ou Microsoft Consulting Services pour faire un examen indépendant de votre utilisation de nos produits de sécurité afin d'optimiser l'utilisation et la visibilité.

Déployer une stratégie exhaustive de correction des programmes pour tous les systèmes de

Microsoft et de tiers. Ceci est essentiel. Continuer le déploiement et le peaufinement du modèle de niveau administratif Active Directory (0/1/2).

Empêcher les comptes de service d'utiliser des connexions interactives : contrôle par accès conditionnel.

Normaliser les contrôleurs de domaine et réduire la surface d'attaque.

Standardize DCs and reduce attack surface.

Déployer l'authentification multifacteur pour les administrateurs de domaine et d'entreprise, les comptes infonuagiques et tous les utilisateurs de réseau privé virtuel (RPV).

Installer la solution de protection avancée contre les menaces Microsoft Defender sur tous les ordinateurs.

Surveiller activement les alertes et agir rapidement en cas de problème dans la console.

Faire appel aux spécialistes des menaces Microsoft pour la surveillance.

Continuer de déployer Windows 10 et Windows Server 2019 dans l'organisation d'ici la fin de 2019.
(La prise en charge de Windows 7 et de Windows Server 2008 se termine le 14 janvier 2020.)

Activer CredentialGuard, DeviceGuard, ExploitGuard, Windows Hello entreprise, SmartScreen, le contrôle d'application, l'accès contrôlé aux dossiers, la réduction de surface d'attaque, Bitlocker, Secure Boot, etc.

- Désactiver SMBv1.
- Désactiver NTLM.
- Cesser d'utiliser TLS 1.0 et 1.1 (leur prise en charge se terminera dans la première moitié de 2020).
- Mettre à jour tous les services et toutes les applications qui utilisent SMTP, Telnet, FTP, IMAP, etc. pour les remplacer par des options sans texte en clair; cette mesure est *nécessaire* pour désactiver l'authentification héritée dans Office 365 et pour activer l'accès conditionnel.
- Utiliser une connexion centrale des outils en ligne de commande pour archiver les activités.
- Installer la version la plus récente de PowerShell pour obtenir des fonctionnalités supplémentaires.

Recommandations <aussi importantes>

Applications d'inventaire

- Activer AppLocker en mode d'audit pour l'inventaire des applications.
- Analyser les applications non autorisées et les mettre sur une liste noire.
- Idéalement, mettre les applications approuvées sur une liste blanche.

Examen de la stratégie de groupe

- Mettre en œuvre un programme d'évaluation de la stratégie de groupe pour l'analyser et l'optimiser.

Utilisation du Pare-feu Windows

- Le Pare-feu Windows protège les ordinateurs contre les attaques réseau.
- Surveiller les modifications de la configuration du pare-feu sur les terminaux.

Plan exhaustif d'intervention en cas d'incident

- Continuer de produire des plans officiels en prévision des incidents de sécurité, y compris l'isolement de l'hôte, les communications hors bande, le déploiement rapide de changements, etc.

Solution de protection avancée contre les menaces Microsoft Azure

- Surveiller la solution de protection avancée Azure pour détecter les connexions inhabituelles et les attaques avancées (Golden Ticket, Skeleton Key, Pass-The-Hash, etc.)

Solution de protection avancée contre les menaces Microsoft Azure

- Appliquer les mêmes étapes que celles pour le niveau 0 : trouver des façons de protéger les systèmes de niveau 1 les plus précieux et essentiels.

Recommandations
<aussi importante

Recommandations relatives à Office 365

- Exiger l'authentification multifacteur pour les utilisateurs d'Office 365
- Remplacer les serveurs Exchange locaux par Office 365.
- Désactiver les anciens protocoles d'authentification.
- Adopter l'accès conditionnel.
- Possibilité de faire examiner Office 365 par l'équipe DART.

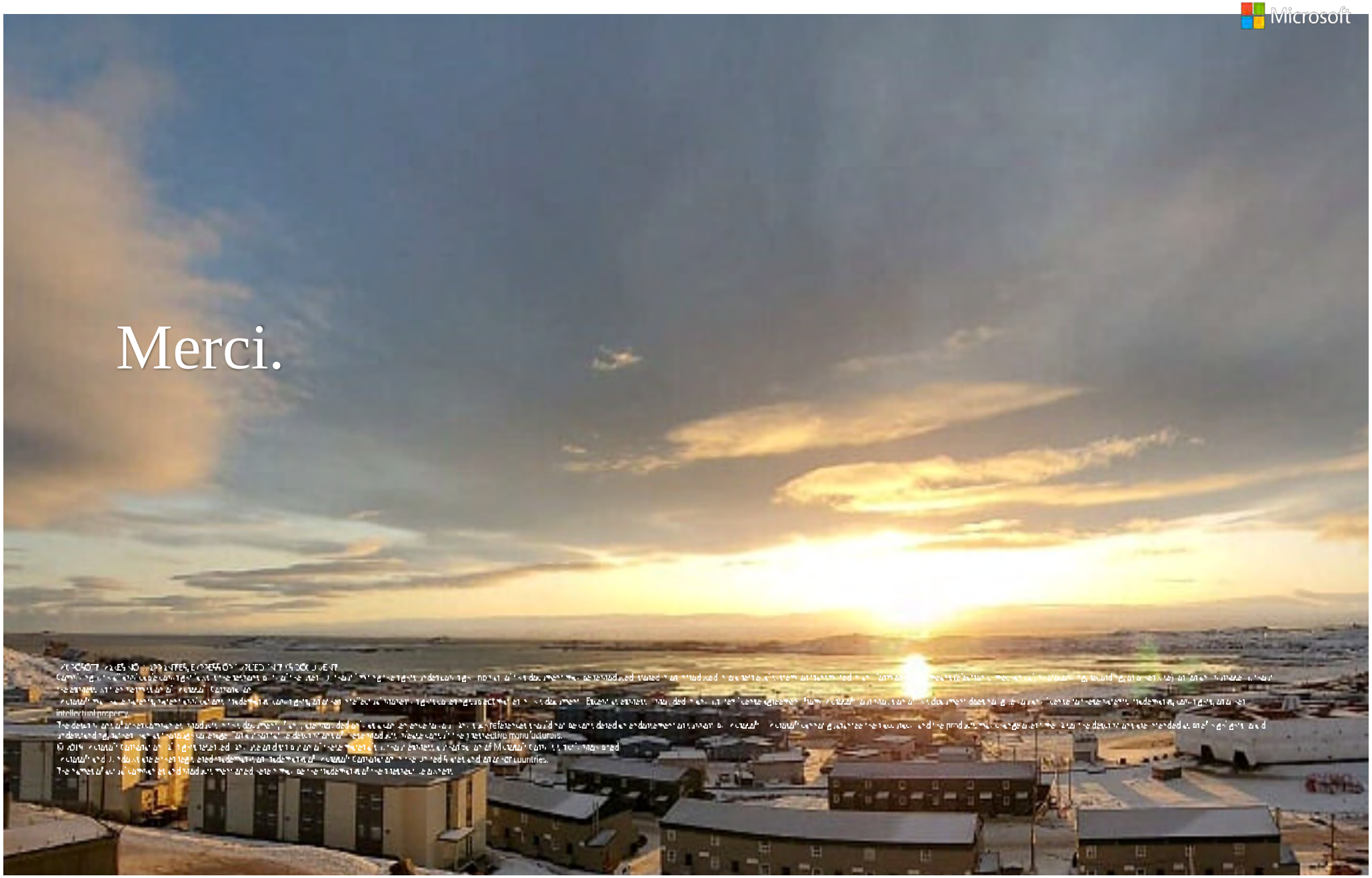
Utilisation optimale des services de Microsoft

- Les techniciens d'entretien principaux et Microsoft Consulting Services peuvent vous aider à appliquer toutes ces recommandations

- L'équipe DART offre des services d'opérations de cybersécurité (version proactive des services d'intervention en cas d'incident).

Surveillance continue de la sécurité

- Veiller à ce que les capteurs soient surveillés en tout temps et à ce que des mesures soient prises rapidement en cas d'alerte.


Merci.