Alerte de prévention des cybermenaces de la part de Bell – Juillet 2018

Les gouvernements mondiaux frappés par des attaques de harponnage masquées

Lorsque les ministères des Affaires étrangères européens et nord-américains ont reçu un courriel d'apparence officielle en février dernier ayant pour objet une « Invitation à un événement concernant la défense », peu de destinataires ont deviné qu'il contenait un logiciel malveillant prêt à s'attaquer à leurs systèmes et à exposer des renseignements potentiellement sensibles.

Fonctionnement
Attaque dissimulée dans des macros Excel

L'hameçonnage est un cybercrime par lequel son auteur tente d'amener les utilisateurs à ouvrir des pièces jointes ou des liens malveillants programmés pour dérober des renseignements sensibles ou pour installer un logiciel malveillant. Les tentatives d'hameçonnage font appel à une mystification par courriel ou à d'autres techniques pour donner l'impression que la missive provient d'une source officielle, comme un établissement financier ou un détaillant.

Les attaques par hameçonnage classiques ratissent large, tandis que celles par harponnage sont extrêmement ciblées. Les attaquants choisissent leurs victimes délibérément. Ils personnalisent leurs courriels de manière à dissiper les soupçons, souvent en se faisant passer pour une personne ou une organisation dont les destinataires n'ont aucune raison de se méfier.

Dans l'attaque de février 2018, le courriel avait en pièce jointe un document Excel qui contenait une macro malveillante. Par défaut, Microsoft Office désactive les macros pour assurer la protection contre ce genre d'attaques. Cependant, ce message invitait les destinataires à activer les macros s'ils avaient de la difficulté à afficher la pièce jointe, ce qu'ils ont fait parce que le fichier était programmé pour masquer un certain contenu. Les destinataires qui ont suivi ces instructions voyaient alors s'afficher ce qui semblait être une liste légitime d'événements à venir pendant que la macro s'exécutait en tâche de fond.

Cette macro était programmée pour décompresser et installer un logiciel malveillant qui donnait aux attaquants la maîtrise totale du système infecté. Ce qui rendait difficile la détection de cette menace, c'était que le fichier malveillant exécutable était intégré au document Excel. Cela permettait au logiciel malveillant de s'installer sans établir de connexion avec une ressource réseau externe, rendant ainsi impossible sa détection par l'analyse des activités réseau à la recherche d'adresses IP suspectes.

L'attaquant
Fancy Bear

Fancy Bear, un groupe de pirates informatiques bien connu, serait derrière ces attaques. Classé comme un groupe de menace persistante évoluée (MPE), il se consacre au cyberespionnage et au vol de données au moyen de courriels de harponnage et de logiciels malveillants qui compromettent l'intégrité des réseaux, dont certains sont accessibles au public et d'autres qui ont été développés par Fancy Bear pour cibler plusieurs systèmes d'exploitation.

Ce groupe est actif depuis 2007 et emploie plusieurs autres pseudonymes connus, dont APT28 et Sofacy.

Bell

Le document Excel, avant et après l'activation des macros :

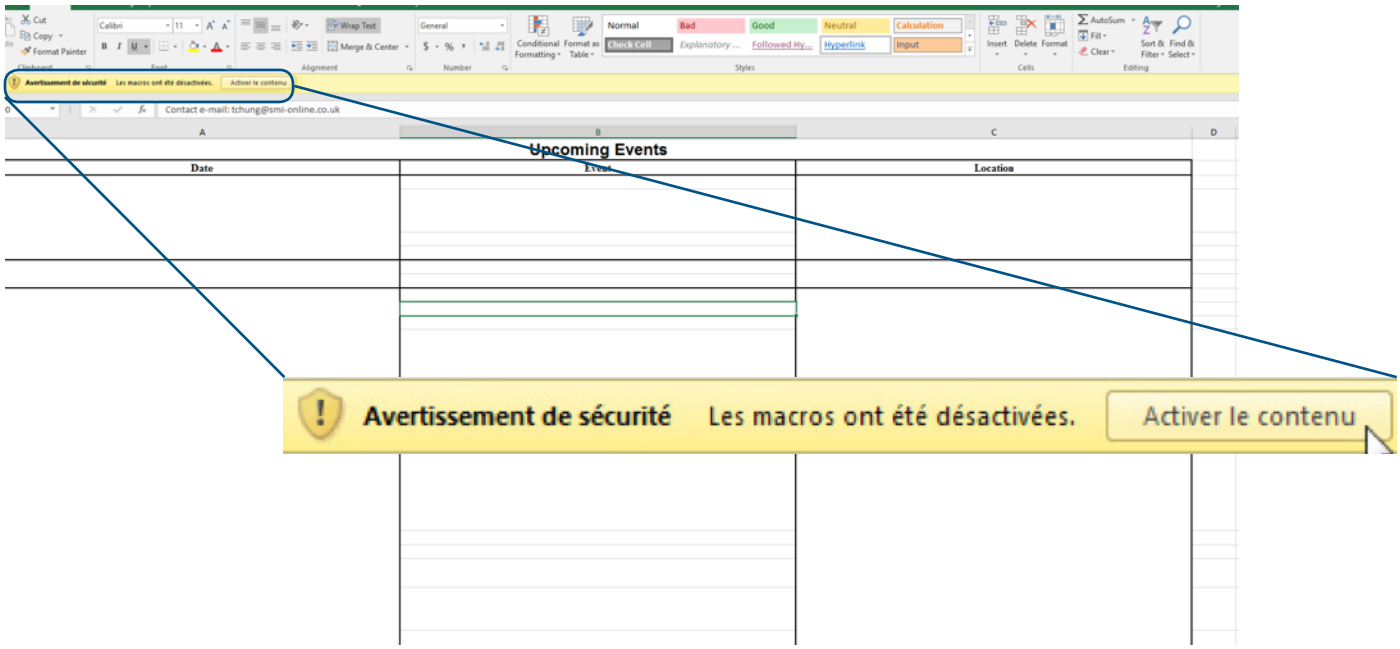

Figure 1 : La pièce jointe avec les macros désactivées – et le message invitant à les activer.

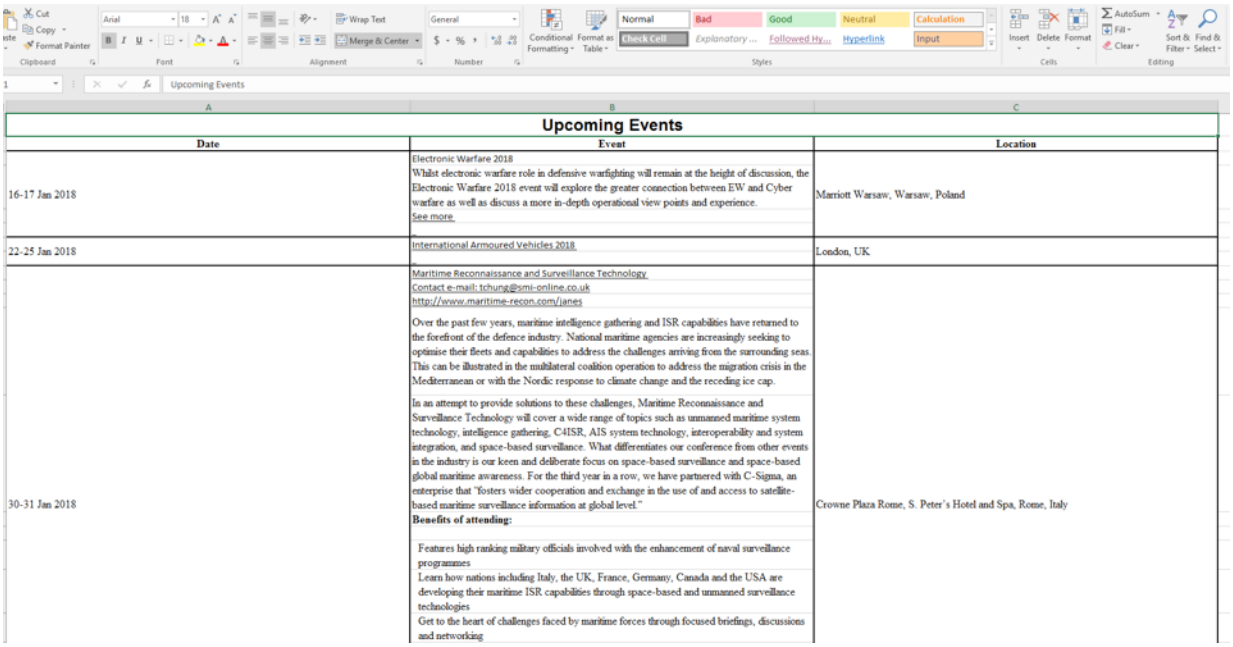

Figure 2 : La pièce jointe avec les macros activées.

Comment les experts en sécurité de Bell ont détecté la menace

Extraction des macros pour voir ce qu'elles font

L'équipe Renseignements sur les cybermenaces de Bell surveille continuellement les activités des groupes de menace persistante évoluée qui sévissent partout sur la planète afin de vérifier s'ils sont actifs au Canada. Lorsque Bell a appris que cette menace était hautement active au Canada, ses experts ont analysé un échantillon du fichier afin d'en étudier le comportement et de définir des stratégies de prévention.

```
 1:       107 '\x01CompObj'
 2:      3460 '\x05DocumentSummaryInformation'
 3:       208 '\x05SummaryInformation'
 4:    212412 'Workbook'
 5:       594 '_VBA_PROJECT_CUR/PROJECT'
 6:       134 '_VBA_PROJECT_CUR/PROJECTwm'
 7: M     4661 '_VBA_PROJECT_CUR/VBA/LinesOfBusines
 8: M     1048 '_VBA_PROJECT_CUR/VBA/Module1'
 9: m      991 '_VBA_PROJECT_CUR/VBA/Sheet1'
10: m      999 '_VBA_PROJECT_CUR/VBA/ThisWorkbook'
11:      3078 '_VBA_PROJECT_CUR/VBA/_VBA_PROJECT'
12:      1841 '_VBA_PROJECT_CUR/VBA/__SRP_0'
13:       241 '_VBA_PROJECT_CUR/VBA/__SRP_1'
14:       312 '_VBA_PROJECT_CUR/VBA/__SRP_2'
15:       426 '_VBA_PROJECT_CUR/VBA/__SRP_3'
16:       620 '_VBA_PROJECT_CUR/VBA/dir'
```

Figure 3 : Objet suspect intégré dans le document.

L'équipe d'analyse des menaces de Bell a exploré le document Excel et a découvert qu'il renfermait deux macros. La première était codée de manière à appeler une fonction dans la deuxième qui lançait l'installation d'un fichier malveillant exécutable sur le système du destinataire. Bell a découvert que la macro accédait à du contenu masqué à la fin du fichier Excel (à la fin de lignes vides dans le document Excel, là où les victimes avaient peu de chance de les voir).

Une deuxième macro fusionnait le contenu des cellules masquées pour créer des fichiers .txt et .exe qui donnaient accès au système de fichiers de l'ordinateur cible. Le fichier exécutable ainsi généré exécutait le gros de l'activité malveillante – il se rendait persistant même après un redémarrage, il pouvait se connecter à une adresse IP ou à un domaine externe pour transmettre et recevoir des données, et plus encore.

Comment prévenir ces attaques

La sécurité du réseau et la formation des employés sont la clé

Les entreprises peuvent protéger leurs utilisateurs et leurs systèmes de TI des attaques par harponnage comme celle de Fancy Bear par les mesures suivantes :

- Prévenir l'activation de fichiers exécutables à divers endroits
- Désactiver la possibilité pour les utilisateurs d'activer l'exécution de macros non fiables
- Bloquer les pièces jointes de courriels de sources inconnues, dont les types de fichiers qui soulèvent des soupçons
- Balayer les pièces jointes avec plusieurs moteurs antivirus et différentes technologies d'environnement d'essai en vase clos
- Former et sensibiliser les employés sur la façon de gérer adéquatement les courriels suspects

Parallèlement à ces mesures, Bell peut procéder périodiquement à une évaluation de la sécurité ou à un bilan de santé organisationnel pour aider à cerner les lacunes en matière de sécurité des TI et à concentrer les correctifs sur les éléments les plus importants.

Vous voulez vous assurer que votre entreprise est protégée contre les cybermenaces comme celles-ci? Visitez Bell.ca/cybersecurite pour savoir comment nous pouvons vous aider.

Bell