# Chronique d’une fin annoncée

## Les enjeux de l’après-Windows XP

VOLKER JUNG, ANTHONY BYATT – Depuis plus de dix ans, Windows XP de Microsoft est le système d’exploitation le plus vendu au monde. Pourtant, malgré ses quelque 30 % d’utilisateurs inconditionnels dans l’univers Windows, il a fait son temps. D’où la décision de Microsoft, en avril 2014, de ne plus en assurer le support technique, ni les mises à jour automatiques, correctifs, etc. La sécurité, la fiabilité et la compatibilité avec la majorité des dernières générations d’ordinateurs, de composants informatiques, de périphériques et d’équipements réseau seront de moins en moins garanties. C’est dire combien l’arrêt d’XP bouscule nombre d’applications industrielles, obligeant ses utilisateurs à prendre les devants.

Il fut un temps où, dans l'industrie, personne ne voulait entendre parler de Windows ! Pourtant, quand Microsoft annonce XP en 2001, les industriels tendent l'oreille et font volte-face : le nouvel OS ne répond-il pas à leurs exigences de stabilité, de flexibilité et de fonctionnalité ? Dont acte : XP ne tardera pas à investir un nombre incalculable d'applications.

Hélas, tout règne a une fin : le 8 avril 2014, Microsoft sonne le glas du support XP. Si ses clients ont été amplement informés et préparés depuis longtemps à tourner la page, la même litanie d'interrogations demeure : un système XP autonome peut-il continuer à tourner sans encombre ? même intégré dans un autre système ? Faut-il investir dans de nouveaux matériels ? et à quel prix ? À combien se chiffre cette transition pour toute l'entreprise ? La virtualisation est-elle la solution ? De quelle assistance dispose-t-on pour accompagner la migration ?

Les réponses à ces questions ne vont pas de soi. La fin du support XP soulève en effet quatre grandes problématiques :

**Photo p. 39**
Le 8 avril 2014, Microsoft a mis un terme au support Windows XP. Quelles en sont les conséquences pour l'industrie ?

– La sécurité ;
– La conformité réglementaire ;
– L'absence de support par les éditeurs de logiciels indépendants ;
– L'assistance technique des constructeurs informatiques.

La sécurité arrive en tête des préoccupations.

## Alerte à l'usine

En 2010, le ver Stuxnet défraye la chronique en s'attaquant aux systèmes de contrôle-commande d'au moins 14 sites industriels en Iran, dont un centre d'enrichissement d'uranium. Ce code malveillant, d'à peine 500 kilo-octets, a sévi en trois temps : il a d'abord scruté les machines et réseaux Windows, puis visé les logiciels d'automatismes, également sous Windows, pour enfin s'infiltrer dans les automates programmables aux commandes des machines.

Depuis, les imposants systèmes d'information des complexes industriels sont la cible répétée de pirates informatiques qui affûtent sans relâche leurs armes. C'est l'exemple de l'attaque « par point d'eau » qui consiste à reconnaître ou à observer les sites web habituels d'une entreprise pour y déposer un code malveillant et, par ce biais, infecter les ordinateurs de ses visiteurs. Une stratégie de double « compromission », par le Web et la machine cible, d'autant plus pernicieuse qu'elle s'appuie sur des sites de confiance pour piéger en toute transparence les victimes du secteur d'activité ou de l'organisation ciblés.

Qui plus est, l'attaquant est capable de manipuler les profils utilisateurs authentifiés d'un système pour autoriser les accès de l'extérieur. Sont également visées les configurations informatiques dans lesquelles les PC peuvent, par exemple, héberger des « chevaux de Troie », ces codes malveillants contenus dans des programmes d'apparence saine qui permettent au pirate de prendre le contrôle d'une machine distante, à l'insu de son utilisateur. Ces chevaux de Troie pour accès distant ou *RAT* (*remote access trojan*) se glissent dans la simple pièce jointe d'un courriel. Une fois le PC hôte infiltré, l'intrus en profite pour diffuser d'autres chevaux de Troie et former ainsi un réseau de machines « zombies » ou *botnet* (contraction de *robot network*) qui propage l'infection.

**1 Systèmes de contrôle-commande et interfaces homme-machine concernés**

| Système | Remarques |
|---|---|
| 800xA | Noyau 800xA : versions 5.0 et antérieures |
| Freelance | Versions 6.2 à 9.1 |
| Power Generation Portal (PGP)/Tenore | Toutes les versions sous Windows |
| Conductor NT | Toutes les versions sous Windows (en nombre de serveurs, pas de systèmes) |
| Process Portal B (PPB) | Toutes les versions |

Cette mainmise à distance permet à l'attaquant d'exécuter à sa guise une longue liste d'actions malveillantes : suivre le comportement de l'utilisateur de la machine cible à l'aide d'enregistreurs de frappe ou autres logiciels espions, activer une webcam, accéder à des informations confidentielles, reformater des disques, effacer ou modifier des fichiers, etc.

En juin 2014, un nouveau RAT nommé Havex fait la une des journaux en s'attaquant aux systèmes de contrôle-commande (ICS) et de supervision (SCADA) de grands groupes industriels, notamment du secteur de l'énergie. Le mode opératoire est le même : les pirates commencent par distribuer de nouvelles versions du RAT pour s'introduire ensuite sur les sites des fournisseurs de solutions ICS/SCADA et détourner leurs bases de téléchargement de logiciels légitimes. Au total, 88 variantes de ce programme malveillant ont infiltré 146 serveurs après avoir « traqué » 1500 adresses IP pour identifier ses victimes. De quoi ébranler la forteresse industrielle !

> Un attaquant peut aller jusqu'à manipuler des profils utilisateurs authentifiés pour autoriser les accès de l'extérieur.

2 Stratégies de migration

| Windows XP | | Contrôle-commande | | | | |
|---|---|---|---|---|---|---|
| 800xA | 3.1<br>4.0<br>4.1<br>5.0 | Tous | → | 800xA | 5.1 | 6.0 |
| Freelance | 6.2<br>7.1<br>7.2<br>8.1<br>8.2<br>9.1 | Tous | → | Freelance | 2013 | 2015 |
| Conductor NT | Tous | DCI | → | 800xA | 5.1 | 6.0 |
| | | Freelance | → | Freelance | 2013 | 2015 |
| | | | → | 800xA | 5.1 | 6.0 |
| | | Harmony | → | 800xA | 5.1 | 6.0 |
| | | | → | Symphony + | 2.0 | |
| PPB | Tous | MOD 300 | → | 800xA | 5.1 | 6.0 |
| | | Freelance | → | Freelance | 2013 | 2015 |
| | | | → | 800xA | 5.1 | 6.0 |
| | | Harmony | → | 800xA | 5.1 | 6.0 |
| | | | → | Symphony + | 2.0 | |
| PGP/Tenore | Tous | Freelance | → | Freelance | 2013 | 2015 |
| | | | → | 800xA | 5.1 | 6.0 |
| | | Harmony | → | 800xA | 5.1 | 6.0 |
| | | | → | Symphony + | 2.0 | |

En juillet 2014, c'est au tour de l'attaque ciblée « *Energetic Bear* » d'infecter plus d'un millier d'entreprises du secteur de l'énergie, en Europe et aux États-Unis, dans le but théorique de prendre le contrôle des centrales.

Ces exemples pointent les vulnérabilités de l'informatique industrielle et, en l'absence des indispensables mises à jour de sécurité Windows XP, son exposition aux attaques virales, aux logiciels espions et autres malveillances visant à dérober ou à détruire les données et informations d'entreprises. Les antivirus n'assurant plus de protection complète, tout équipement encore sous XP est une porte d'entrée béante dans les réseaux informatiques ciblés. Et même les ordinateurs exploitant des OS supportés risquent la « compromission ».

## Matériel en sursis

Les constructeurs informatiques ont pour la plupart déjà cessé de supporter Windows XP sur leur nouveau matériel et retiré de leur catalogue les pilotes de périphériques XP (disques durs, imprimantes, cartes graphiques, équipements réseau, etc.). Acheter un ordinateur de rechange XP ne sera guère aisé ni économique ; obsolète, le matériel XP sera difficile à trouver. De même, les arrêts intempestifs dus à l'indisponibilité des composants vont devenir monnaie courante.

## Conformité

En restant sous XP, les entreprises et organismes très réglementés, comme ceux soumis aux États-Unis à la loi *HIPAA* (*Health Insurance Portability and Accountability Act*) sur la santé et l'assurance maladie, peuvent s'estimer dans l'incapacité de respecter leurs obligations. De nos jours, l'explosion du stockage des données personnelles et de la vie privée sur des serveurs fait de la sécurité informatique une priorité.

## Support : obsolescence programmée

De nombreux éditeurs de logiciels n'assurent plus le support de leurs produits sur XP puisqu'ils ne reçoivent pas de mises à jour. Pour preuve, la nouvelle suite Microsoft Office, par exemple, tourne sur le dernier-né de Windows mais plus sur XP.

## Antidotes

Devant ces problématiques, quelle démarche adopter ? Microsoft et tous les experts en sécurité recommandent aux fournisseurs de solutions de contrôle-commande distribué exploitant Windows XP et ses prédécesseurs ➔ 1, 2 de passer à Windows 7 ou 8.

Il est bien sûr possible de chiffrer le coût de la sécurisation des installations XP par rapport à celui de la migration. Conserver Windows XP oblige à beaucoup investir dans la maintenance et dans l'arsenal préconisé par les professionnels de la cyberdéfense. Voici un exemple de plan d'actions :

- Réduire le registre de services au strict nécessaire ;
- Utiliser la technique du « *DNS sinkholing* » qui consiste à rediriger les noms de domaine malveillants vers un ou plusieurs serveurs non menacés afin de bloquer l'accès au site web visé ;
- Déclencher une alerte sur détection d'une connexion au réseau virtuel ou à un poste bureautique distant par un équipement terminal ;
- Interdire aux utilisateurs temporaires l'exécution de binaires dans le système de fichiers ou, le cas échéant, lancer l'alerte ;
- Créer une liste blanche des binaires de service dans le système d'exploitation ;
- Alerter en cas de démarrage, d'arrêt et de changement de service ;
- Auditer les listes de contrôle d'accès, entre autres ;
- Effectuer des sauvegardes régulières du système de contrôle-commande ;
- Acheter un stock de composants informatiques compatibles XP.

Pour autant, conserver Windows XP est de moins en moins réaliste. L'évolution des systèmes d'information industriels est inéluctable ; leur parc logiciel, à l'image de Windows XP, n'échappe pas à la règle. La migration permettra aux utilisateurs de répondre aux exigences de sécurité, de compatibilité (matérielle et logicielle) et de conformité de l'informatique industrielle moderne.

ABB recommande vivement à ses clients exploitant XP de faire le point sur le cycle de vie de leurs systèmes et d'élaborer une stratégie de réduction des risques. Dans le même temps, ABB propose des palliatifs et des solutions pour les aider à mieux protéger leurs sites et leur personnel tout en garantissant la sécurité et la pérennité de l'activité. L'offre de services ABB est adaptée aux attentes et contraintes de chaque client, y compris celui qui n'a pas la possibilité d'évoluer tout de suite ou qui a fait le choix de rester sous XP.

**Volker Jung**
Process Automation Division
Mannheim (Allemagne)
volker.jung@de.abb.com

**Anthony Byatt**
Consultant rédacteur
Louth Village (Irlande)