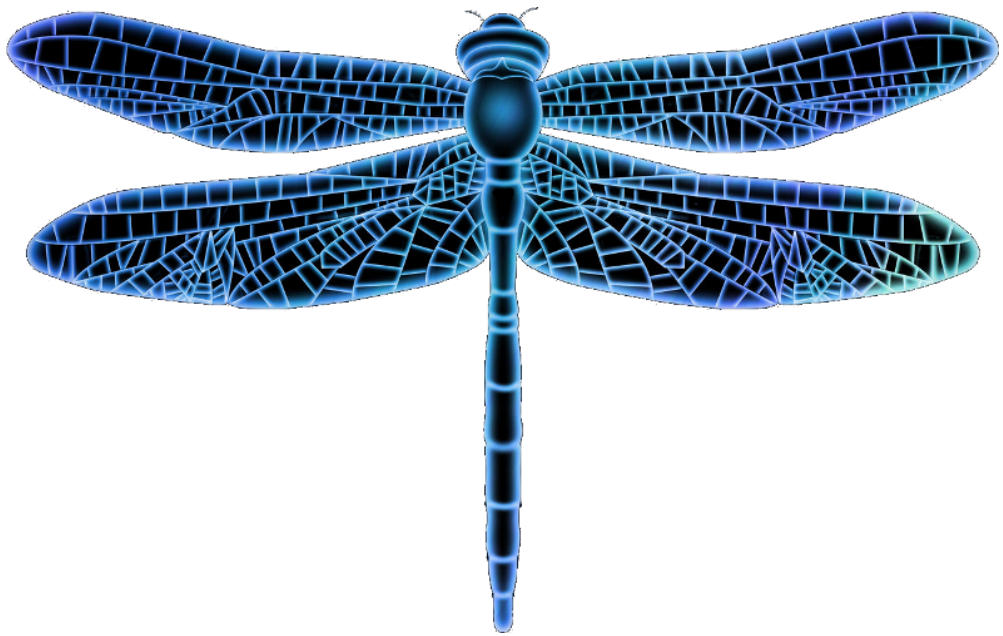
DragonFly

Éric BERTHOMIER
eric.berthomier@free.fr

March 16, 2022



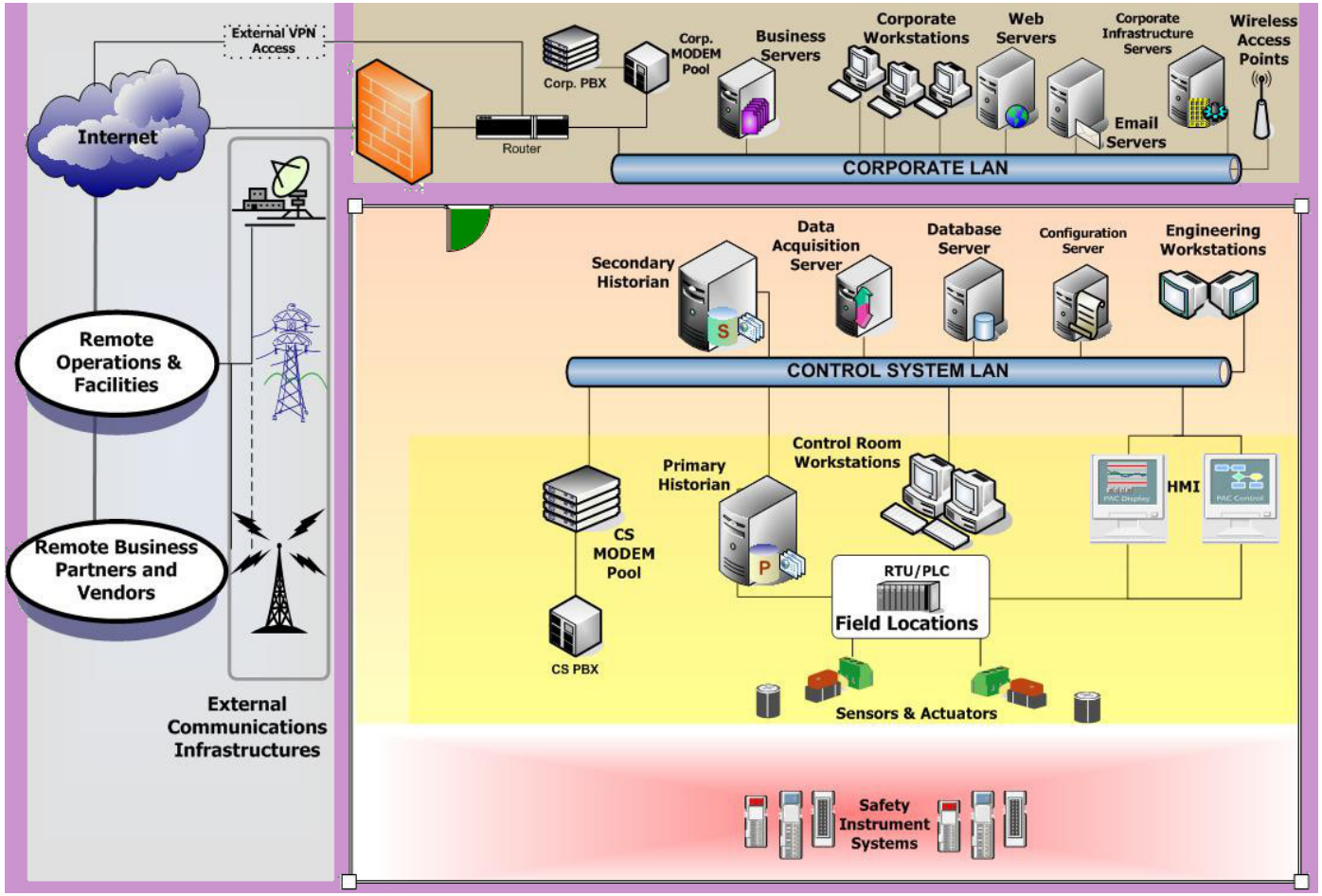
Version 1.0 - Version Stagiaire

Préambule

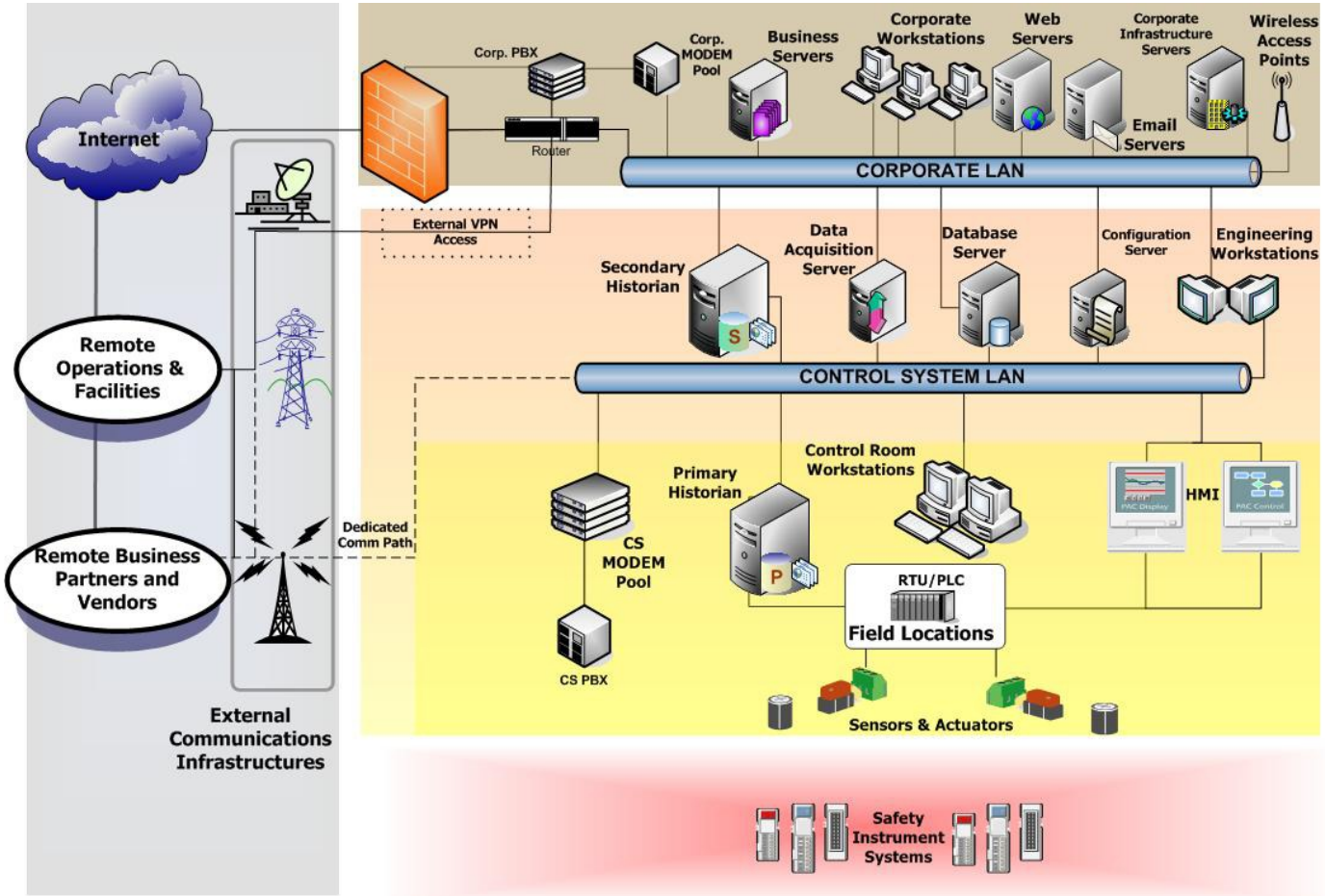
Ce cours a été réalisé grâce à l'étude effectuée par Belden.

http://www.belden.com/docs/upload/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks.pdf

Réseau d'entreprise - Réseau d'automates confiné
Avant



Réseau d'entreprise - Réseau d'automates
Tendance Actuelle



DragonFly : Cibles

- FT.col 30 Juin 2014 - "Les systèmes de contrôle industriel des centaines d'entreprises Européennes et Américaines ont été infecté par une cyber-arme sophistiquée. . . "

DragonFly : Cibles

- FT.col 30 Juin 2014 - "Les systèmes de contrôle industriel des centaines d'entreprises Européennes et Américaines ont été infecté par une cyber-arme sophistiquée..."
- BBC.com, 1er Juillet 2014 - "...plus de 1000 entreprises liées à l'énergie ont été la cible d'une attaque par malware en Europe et en Amérique du Nord..."

DragonFly : Cibles

- FT.col 30 Juin 2014 - "Les systèmes de contrôle industriel des centaines d'entreprises Européennes et Américaines ont été infecté par une cyber-arme sophistiquée..."
- BBC.com, 1er Juillet 2014 - "...plus de 1000 entreprises liées à l'énergie ont été la cible d'une attaque par malware en Europe et en Amérique du Nord..."
- Conclusion d'autres entités

DragonFly : Cibles

- FT.col 30 Juin 2014 - "Les systèmes de contrôle industriel des centaines d'entreprises Européennes et Américaines ont été infecté par une cyber-arme sophistiquée..."
- BBC.com, 1er Juillet 2014 - "...plus de 1000 entreprises liées à l'énergie ont été la cible d'une attaque par malware en Europe et en Amérique du Nord..."
- Conclusion d'autres entités
  - Cîble : Entreprises pharmaceutiques

DragonFly : Cibles

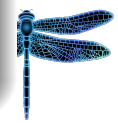
- FT.col 30 Juin 2014 - "Les systèmes de contrôle industriel des centaines d'entreprises Européennes et Américaines ont été infecté par une cyber-arme sophistiquée..."
- BBC.com, 1er Juillet 2014 - "... plus de 1000 entreprises liées à l'énergie ont été la cible d'une attaque par malware en Europe et en Amérique du Nord..."
- Conclusion d'autres entités
  - Cîble : Entreprises pharmaceutiques
  - But : Vol d'informations.

DragonFly : Cibles

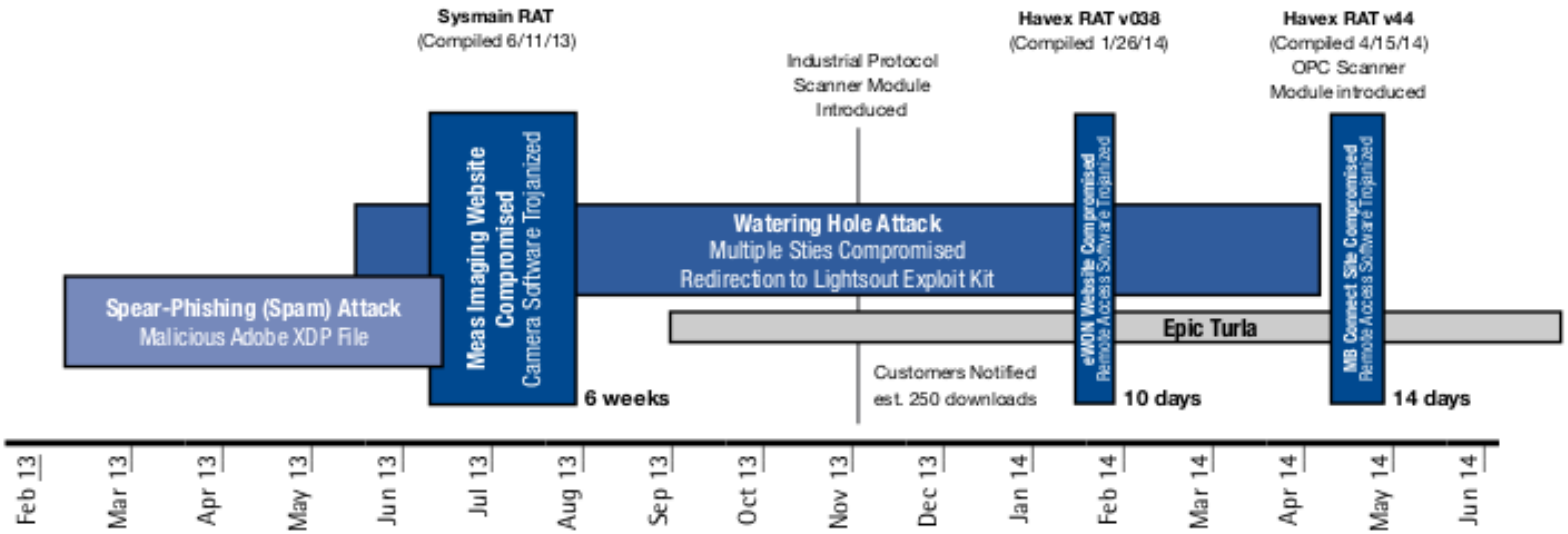
- FT.col 30 Juin 2014 - "Les systèmes de contrôle industriel des centaines d'entreprises Européennes et Américaines ont été infecté par une cyber-arme sophistiquée. . . "
- BBC.com, 1er Juillet 2014 - ". . . plus de 1000 entreprises liées à l'énergie ont été la cible d'une attaque par malware en Europe et en Amérique du Nord. . . "
- Conclusion d'autres entités
  - Cîble : Entreprises pharmaceutiques
  - But : Vol d'informations.

Remarque

Le but n'est pas de causer des dégâts.
Le but n'est pas de stopper des serveurs.
Le but est le vol de propriétés intellectuelles, comme par exemple des secrets de fabrication.



DragonFly : Chronologie d'une attaque



Vecteur 1 - Email Spear Phishing Campaign
Février à Juin 2013

- SPAM avec des pièces jointes de type PDF infectées.

Vecteur 1 - Email Spear Phishing Campaign
Février à Juin 2013

- SPAM avec des pièces jointes de type PDF infectées.
- 37 employés ont été **sélectionnés** au travers de 7 entreprises.

Vecteur 1 - Email Spear Phishing Campaign
Février à Juin 2013

- SPAM avec des pièces jointes de type PDF infectées.
- 37 employés ont été **sélectionnés** au travers de 7 entreprises.
- Faille : CVE-2011-0611.

Vecteur 1 - Email Spear Phishing Campaign
Février à Juin 2013

- SPAM avec des pièces jointes de type PDF infectées.
- 37 employés ont été **sélectionnés** au travers de 7 entreprises.
- Faille : CVE-2011-0611.
- Permet le **déchiffrement** et l'installation de Havex avec une DLL **portable**

Vecteur 1 - Email Spear Phishing Campaign
Février à Juin 2013

- SPAM avec des pièces jointes de type PDF infectées.
- 37 employés ont été **sélectionnés** au travers de 7 entreprises.
- Faille : CVE-2011-0611.
- Permet le **déchiffrement** et l'installation de Havex avec une DLL **portable**
- **Havex : RAT - Remote Access Trojan**

HAVEX - Fonctionnement Général

- Envoi de données sur la victime à un serveur HTTP
  - Id - Identification
  - Havex Version
  - Version de l'OS
  - Méthode d'infection

HAVEX - Fonctionnement Général

- Envoi de données sur la victime à un serveur HTTP
  - Id - Identification
  - Havex Version
  - Version de l'OS
  - Méthode d'infection
- Réception de modules complémentaires à partir du serveur HTTP
  - Information contenue entre les balises <!– havex havex –>
  - Information chiffrée RSA 1024 bits

Vecteur 2 - Watering Hole Attacks
Mai 2013 à Avril 2014

- Compromission de sites Web - CMS (WordPress, Drupal ou Joomla)

Vecteur 2 - Watering Hole Attacks
Mai 2013 à Avril 2014

- Compromission de sites Web - CMS (WordPress, Drupal ou Joomla)
- Redirection des visiteurs sur d'autres pages Web à leur insu.
  - Exploitation des failles JAVA - CVE-2012-1723, CVE-2013-2465
  - Exploitation des failles Internet Explorer - CVE-2012-4792, CVE-2013-1347

Vecteur 2 - Watering Hole Attacks
Mai 2013 à Avril 2014

- Compromission de sites Web - CMS (WordPress, Drupal ou Joomla)
- Redirection des visiteurs sur d'autres pages Web à leur insu.
  - Exploitation des failles JAVA - CVE-2012-1723, CVE-2013-2465
  - Exploitation des failles Internet Explorer - CVE-2012-4792, CVE-2013-1347
- **Ces exploits permettent d'installer Havex ou Karagny sur le poste de travail.**

Karagny

- Backdoor

Karagny

- Backdoor
- Capacités de base
  - Envoi, réception, exécution de fichiers
  - Fonction de maintenance pour se mettre à jour
  - Capacité de s'auto-supprimer sans laisser de traces
  - Fonction d'extraction utilisateur / mot de passe sur les sessions HTTP non chiffrées

Karagny

- Backdoor
- Capacités de base
  - Envoi, réception, exécution de fichiers
  - Fonction de maintenance pour se mettre à jour
  - Capacité de s'auto-supprimer sans laisser de traces
  - Fonction d'extraction utilisateur / mot de passe sur les sessions HTTP non chiffrées
- Capacités étendues
  - Prise de capture d'écran
  - Recherche de fichiers spécifiques

Karagny : Recherche de fichiers spécifiques

Critère de Recherche	Usage Courant
pass.*	Fichier de mots de passe local
secret.*	Fichier de mots de passe local
*.pgp	Clés PGP publiques ou privés
*.pst	Boîte aux lettres Outlook
*.p12	Clés privées et Certificats
*.tc	Volume Truecrypt

Vecteur 3 - Compromission de site Web de Système de Contrôle Industriel

Remplacement des fichiers de mise à jour

Remplacement des logiciels légitimes (mise à jour) par ces mêmes logiciels avec des composants malicieux.

Vecteur 3 - Compromission de site Web de Système de Contrôle Industriel
Remplacement des fichiers de mise à jour

Remplacement des logiciels légitimes (mise à jour) par ces mêmes logiciels avec des composants malicieux.

Parmi les composants ajoutés, on retrouve ceux précédemment décrits mais aussi leurs variantes et un petit nouveau : SysMain.

- Exécution de commandes Shell

SysMain

- Exécution de commandes Shell
- Exécution de modules complémentaires qui peuvent avoir été transmis via les attaquants.

SysMain

- Exécution de commandes Shell
- Exécution de modules complémentaires qui peuvent avoir été transmis via les attaquants.
- Examen du système de la victime

SysMain

- Exécution de commandes Shell
- Exécution de modules complémentaires qui peuvent avoir été transmis via les attaquants.
- Examen du système de la victime
- Récupération arbitraire de fichiers

SysMain

- Exécution de commandes Shell
- Exécution de modules complémentaires qui peuvent avoir été transmis via les attaquants.
- Examen du système de la victime
- Récupération arbitraire de fichiers
- Capacité à changer la clé de chiffrement des communications du malware

SysMain

- Exécution de commandes Shell
- Exécution de modules complémentaires qui peuvent avoir été transmis via les attaquants.
- Examen du système de la victime
- Récupération arbitraire de fichiers
- Capacité à changer la clé de chiffrement des communications du malware
- Capacité de nettoyer l'ensemble des ses traces

Durée d'hébergement des versions malveillantes des logiciels

- Constructeur de caméras industrielles : 6 semaines

Durée d'hébergement des versions malveillantes des logiciels

- Constructeur de caméras industrielles : 6 semaines
- Constructueur de routeur VPN industriel pour accès distant et télémaintenance : 10 jours

Durée d'hébergement des versions malveillantes des logiciels

- Constructeur de caméras industrielles : 6 semaines
- Constructueur de routeur VPN industriel pour accès distant et télémaintenance : 10 jours
- Constructeur de solution de maintenance à distance : 2 semaines

Exemple d'un module d'Havex : Scanner de protocole Industriel

- Écoute des ports communément associé aux protocoles industriels
  102,502,11234,12401,44818

Exemple d'un module d'Havex : Scanner de protocole Industriel

- Écoute des ports communément associé aux protocoles industriels
  102,502,11234,12401,44818
- SCADA : 12401 / 44818

Exemple d'un module d'Havex : Scanner de protocole Industriel

- Écoute des ports communément associé aux protocoles industriels
  102,502,11234,12401,44818
- SCADA : 12401 / 44818
- Advisory (ICSA-11-263-01)

Exemple d'un module d'Havex : Scanner de protocole Industriel

- Écoute des ports communément associé aux protocoles industriels
  102,502,11234,12401,44818
- SCADA : 12401 / 44818
- Advisory (ICSA-11-263-01)
  - Measuresoft ScadaPro Vulnerabilities

Exemple d'un module d'Havex : Scanner de protocole Industriel

- Écoute des ports communément associé aux protocoles industriels
  102,502,11234,12401,44818
- SCADA : 12401 / 44818
- Advisory (ICSA-11-263-01)
  - Measuresoft ScadaPro Vulnerabilities
  - Vulnérabilité de type "stack overflow" permettant à un attaquant de causer un Déni de Service (DoS) ou d'exécuter un code à distance sur la machine infectée.

Les défenses inutiles contre cette attaque

- Liste blanche d'applications.

Les défenses inutiles contre cette attaque

- Liste blanche d'applications.
- Anti-virus : la plupart des applications demandent la désactivation de l'antivirus pour s'installer. Signatures antivirales en retard.

Les défenses inutiles contre cette attaque

- Liste blanche d'applications.
- Anti-virus : la plupart des applications demandent la désactivation de l'antivirus pour s'installer. Signatures antivirales en retard.
- Restriction des droits de l'utilisateur : utilisation de malware autonomes n'ayant pas besoin de s'installer. Utilisation de `AllUsers`.

Les défenses inutiles contre cette attaque

- Liste blanche d'applications.
- Anti-virus : la plupart des applications demandent la désactivation de l'antivirus pour s'installer. Signatures antivirales en retard.
- Restriction des droits de l'utilisateur : utilisation de malware autonomes n'ayant pas besoin de s'installer. Utilisation de `AllUsers`.
- Firewall basés sur les protocoles : utilisation des protocoles courants pour communiquer notamment HTTP.

Les défenses inutiles contre cette attaque

- Liste blanche d'applications.
- Anti-virus : la plupart des applications demandent la désactivation de l'antivirus pour s'installer. Signatures antivirales en retard.
- Restriction des droits de l'utilisateur : utilisation de malware autonomes n'ayant pas besoin de s'installer. Utilisation de `AllUsers`.
- Firewall basés sur les protocoles : utilisation des protocoles courants pour communiquer notamment HTTP.
- VPN

Les défenses inutiles contre cette attaque

- Liste blanche d'applications.
- Anti-virus : la plupart des applications demandent la désactivation de l'antivirus pour s'installer. Signatures antivirales en retard.
- Restriction des droits de l'utilisateur : utilisation de malware autonomes n'ayant pas besoin de s'installer. Utilisation de `AllUsers`.
- Firewall basés sur les protocoles : utilisation des protocoles courants pour communiquer notamment HTTP.
- VPN
- Politique de mise à jour

Les défenses utiles contre cette attaque

- Segmentation du réseau - Zone démilitarisée (DMZ)

Les défenses utiles contre cette attaque

- Segmentation du réseau - Zone démilitarisée (DMZ)
- ISA/IEC 62443 : Assurance Qualité de Production (SSI)

Les défenses utiles contre cette attaque

- Segmentation du réseau - Zone démilitarisée (DMZ)
- ISA/IEC 62443 : Assurance Qualité de Production (SSI)
- ISA/IEC 62443 : Segmentation des zones

Les défenses utiles contre cette attaque

- Segmentation du réseau - Zone démilitarisée (DMZ)
- ISA/IEC 62443 : Assurance Qualité de Production (SSI)
- ISA/IEC 62443 : Segmentation des zones
- Limitation du trafic aux seuls protocoles autorisés
- DPI - Deep Packet Inspection - Vérification du contenu des trames

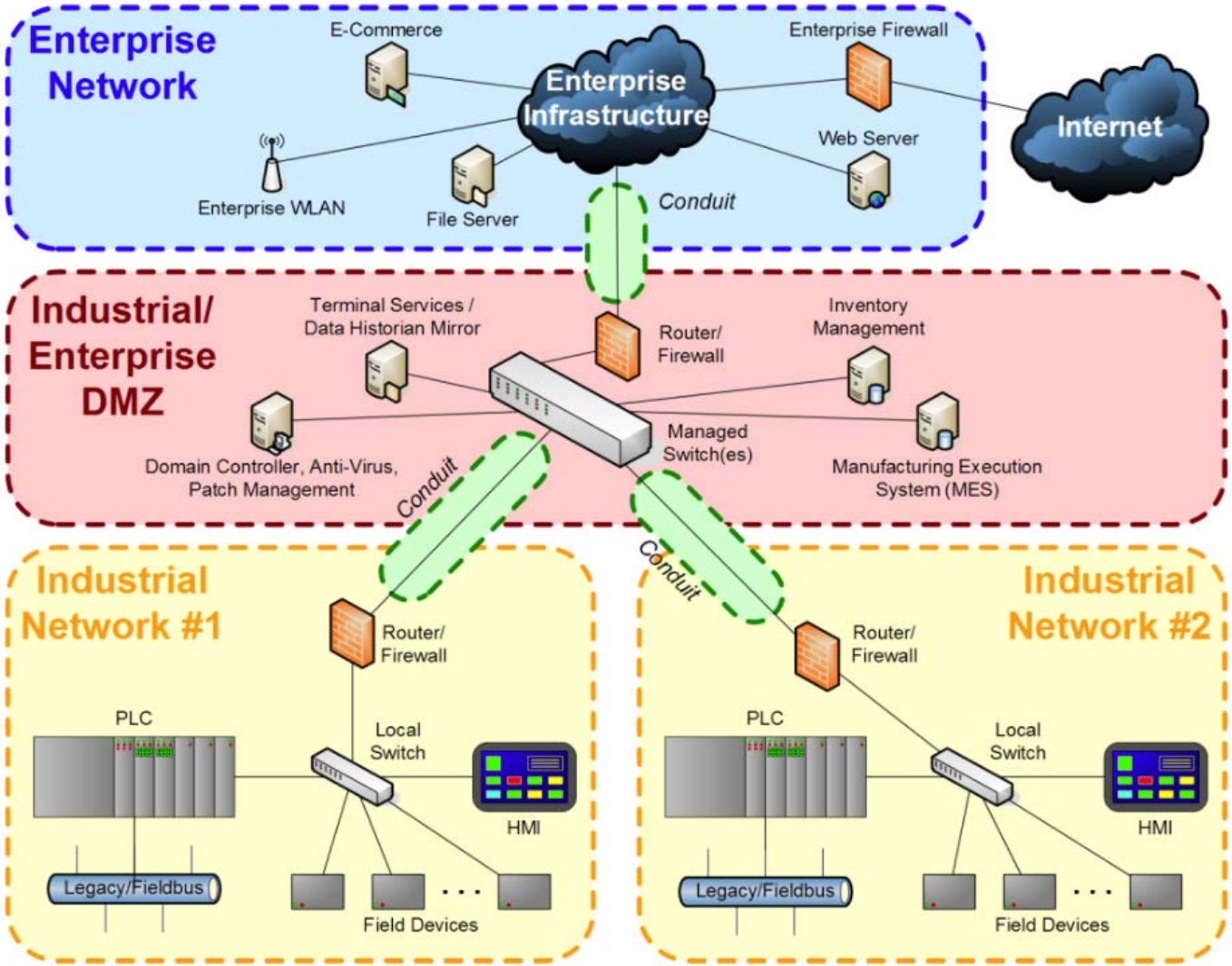
Les défenses utiles contre cette attaque

- Segmentation du réseau - Zone démilitarisée (DMZ)
- ISA/IEC 62443 : Assurance Qualité de Production (SSI)
- ISA/IEC 62443 : Segmentation des zones
- Limitation du trafic aux seuls protocoles autorisés
- DPI - Deep Packet Inspection - Vérification du contenu des trames
- VPN - Restriction de la visibilité et de l'interopérabilité

Les défenses utiles contre cette attaque

- Segmentation du réseau - Zone démilitarisée (DMZ)
- ISA/IEC 62443 : Assurance Qualité de Production (SSI)
- ISA/IEC 62443 : Segmentation des zones
- Limitation du trafic aux seuls protocoles autorisés
- DPI - Deep Packet Inspection - Vérification du contenu des trames
- VPN - Restriction de la visibilité et de l'interopérabilité
- Filtrage Email : Interdiction des toutes les adresses "gratuites"

Réseau Industriel - Segmentation



Structure documentaire CEI-62443 (2013)

Ancienne référence : ISA 99

ISA France