La Cybersécurité des Systèmes Automatisés

Florence LECROQ & Jean GRIEU

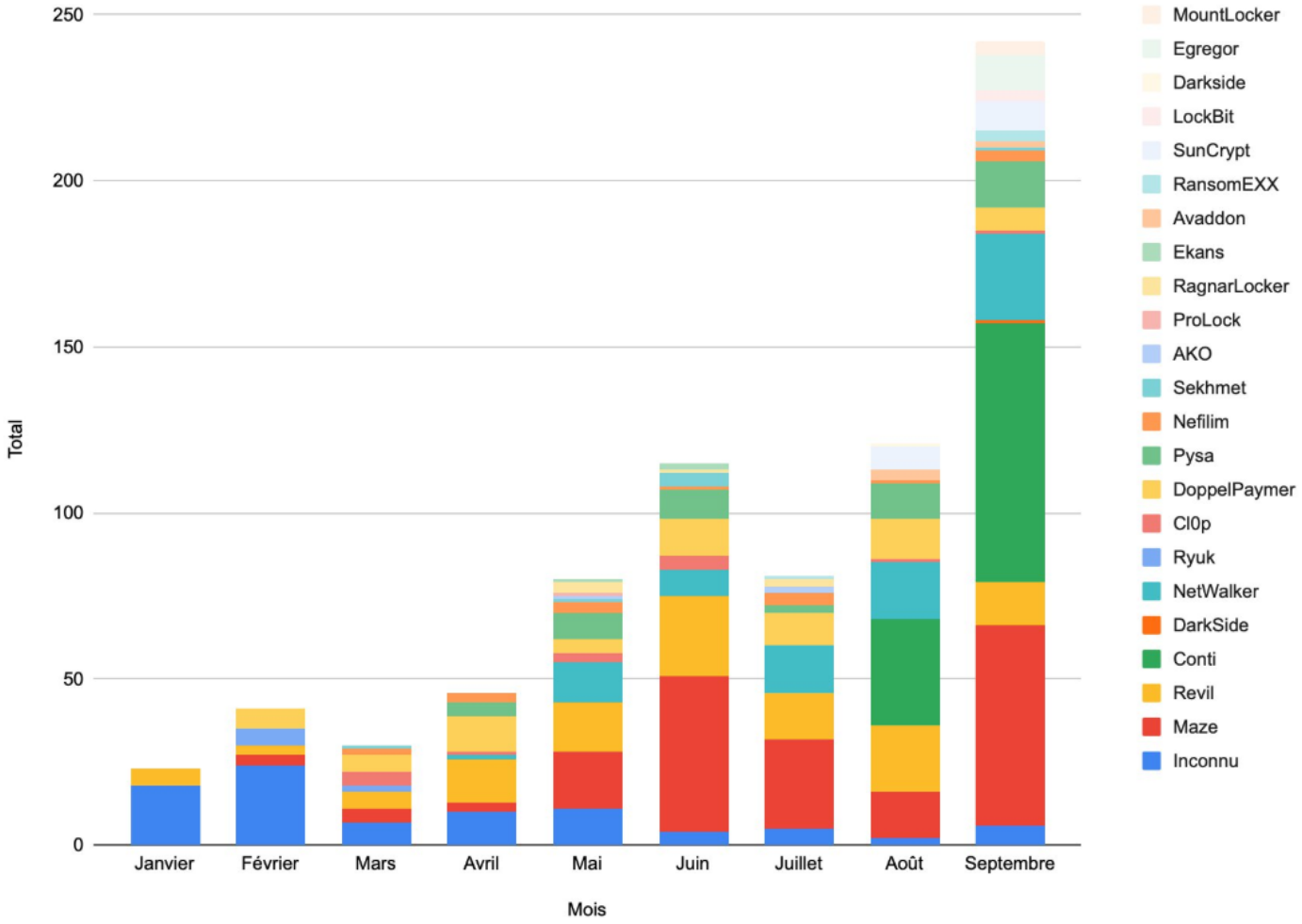
Institut Universitaire de Technologie, Université Le Havre Normandie

florence.lecroq@univ-lehavre.fr

Jean.grgieu@univ-lehavre.fr

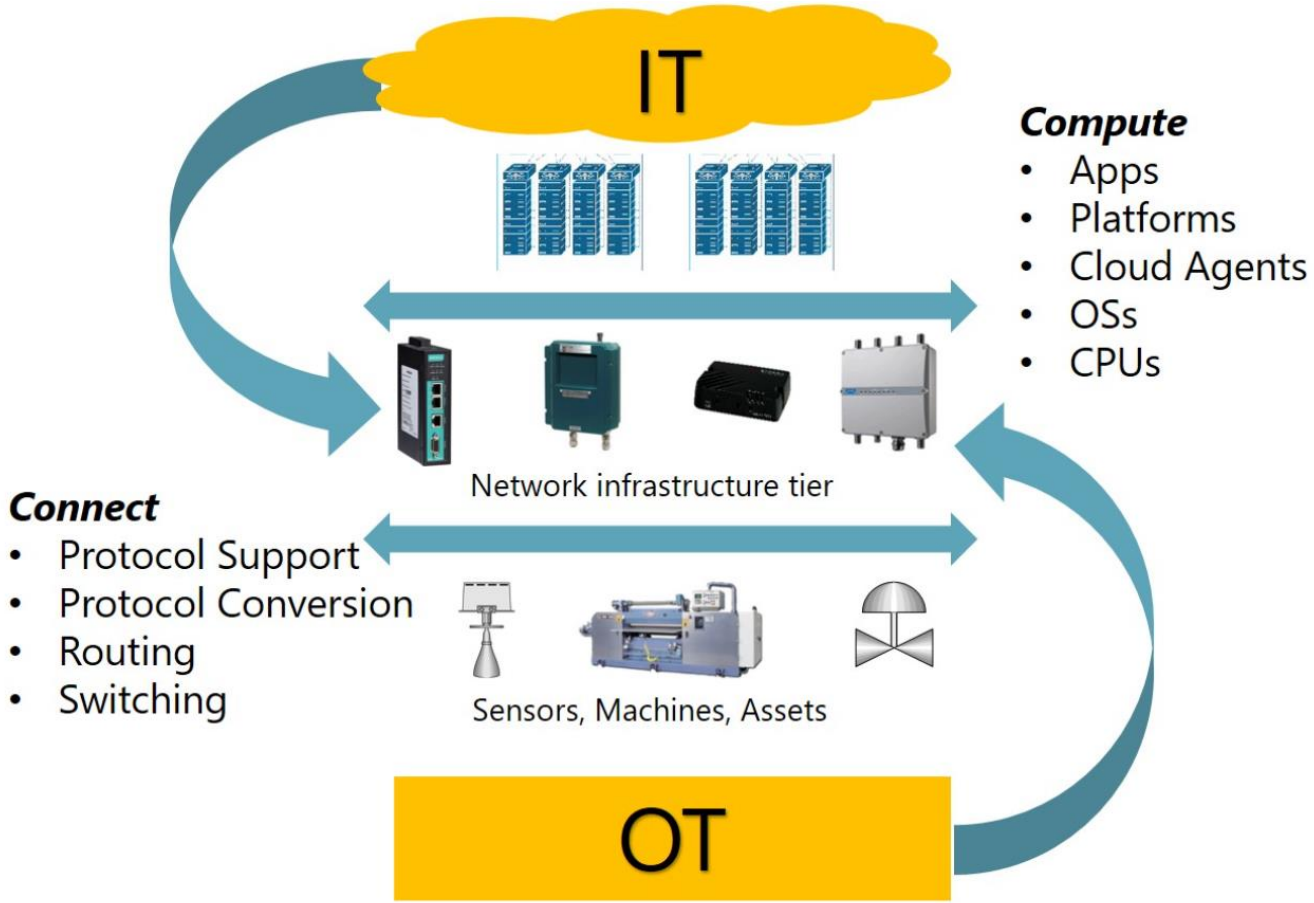

NORSE
ATTACK ORIGINS
COUNTRY
930 China
270 Netherlands
265 United States
259 Spain
216 Russia
135 South Korea
99 Iran
88 Brazil
46 Germany
32 France
ATTACK TYPES
PORT SERVICE TYPE
745 53413 netis-router
685 22 ssh
326 1433 ms-sql-s
184 3389 ms-wbt-server
182 5900 rfb
131 23 telnet
131 445 microsoft-ds
131 80 http
128 138 netbios-dgm
63 50864 xsan-filesystem
ATTACK TARGETS
COUNTRY
1582 United States
430 Australia
237 United Arab Emirates
67 Singapore
55 Germany
48 Hong Kong
44 Italy
39 Romania
29 Russia
27 France
LIVE ATTACKS
TIMESTAMP ATTACKER ATTACKER IP ATTACKER GEO TARGET GEO ATTACK TYPE PORT
16:55:23.586 Nap-De-Las-Americas-Madrid 85.112.12.142 Madrid, ES San Francisco, US http 80
16:55:23.522 Sk Broadband Co Ltd 180.71.47.253 Seoul, KR Seattle, US rfb 5900
16:55:23.445 Ripe Ncc 185.130.5.201 Amsterdam, NL Kirksville, US netis-router 53413
16:55:23.435 Crossnet Llc 81.89.219.18 Yerevan, AM Belconnen, AU microsoft-ds 445
16:55:23.365 Taipei Taiwan 114.44.15.74 Taipei, TW Belconnen, AU ms-wbt-server 3389
16:55:23.253 9net Srl 93.186.241.79 Milan, IT Milan, IT nethios-dgm 138
16:55:23.185 Tt Adsl-Ttnet_Dynamic_Gay 78.185.241.91 Siyavuspasa Ma... Oslo, NO netis-router 53413
16:55:23.186 Tt Adsl-Ttnet_Dynamic_Gay 78.185.241.91 Siyavuspasa Ma... Oslo, NO netis-router 53413
16:55:23.185 Tt Adsl-Ttnet_Dynamic_Gay 78.185.241.91 Siyavuspasa Ma... Oslo, NO netis-router 53413
16:55:23.185 Tt Adsl-Ttnet_Dynamic_Gay 78.185.241.91 Siyavuspasa Ma... Oslo, NO netis-router 53413
HOME
EXPLORE
WHY NORSE?

Attaques par ransomware en 2020 :

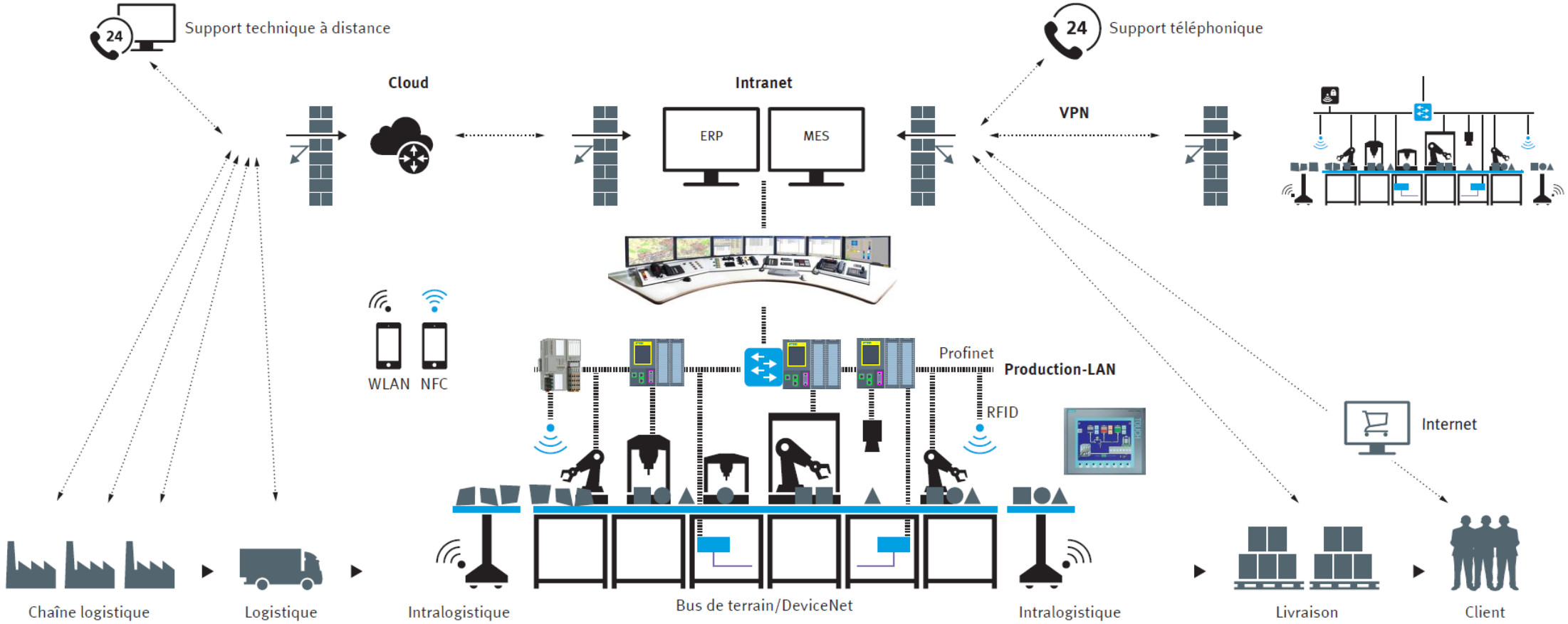


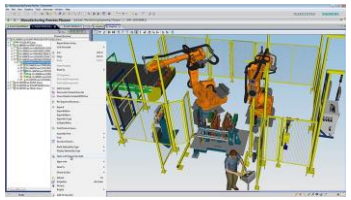
Durant l'année… l'effet COVID !

©V. Marchive LeMagIT


IT
Compute
• Apps
• Platforms
• Cloud Agents
• OSs
• CPUs
Network infrastructure tier
Connect
• Protocol Support
• Protocol Conversion
• Routing
• Switching
Sensors, Machines, Assets
OT

Une représentation de l'Usine du Futur :





Virtualisation / Jumeau numérique

www.festo-didactic.com

Des exemples d'attaques Cyber…

Prise de contrôle de l'aiguillage d'un tramway :

- Où, quand :

  Lodz, Pologne, 2008

- Conséquences :

4 tramways déraillés, 12 blessés légers

- Scenario de l'incident :

Prise de contrôle du système d'aiguillage par un adolescent

- Vulnerabilité :

Réseau radio sans authentification

Explosion d'un pipeline :

- Où, quand :

  Turquie, 2008

- Conséquences :

Destruction du pipeline de Baku-Tbilisi-Ceyhan (BTC), Destruction de matériel, 20 jours d'indisponibilité (plus de 1 Md$ de pertes en materiels et recettes)

- Scenario de l'incident :

Désactivation des systèmes de monitoring et d'alarmes puis explosion

Attaque combine physique et cyber

- Vulnerabilité :

Logiciel des cameras, accès aux vannes, réseau radio exposé

© Document Clusif

Empoisonnement de l'eau potable :

- Où, quand :

  Etat de Georgie, USA, 2013

- Conséquences :

400 foyers privés d'eau potable

- Incident scenario :

Modification des réglages des taux de fluor et de chlore

- Vulnerabilité :

Manque de surveillance de l'installation. Accès physique possible sans levée d'alerte

© Document Clusif

Trafic de drogue dans des conteneurs :

- Où, quand :

  Port d'Anvers, Belgique, 2011

- Conséquences :

Pas de detail sur les pertes, montre le niveau de technicité atteint par les narcotrafiquants

- Scenario de l'incident :

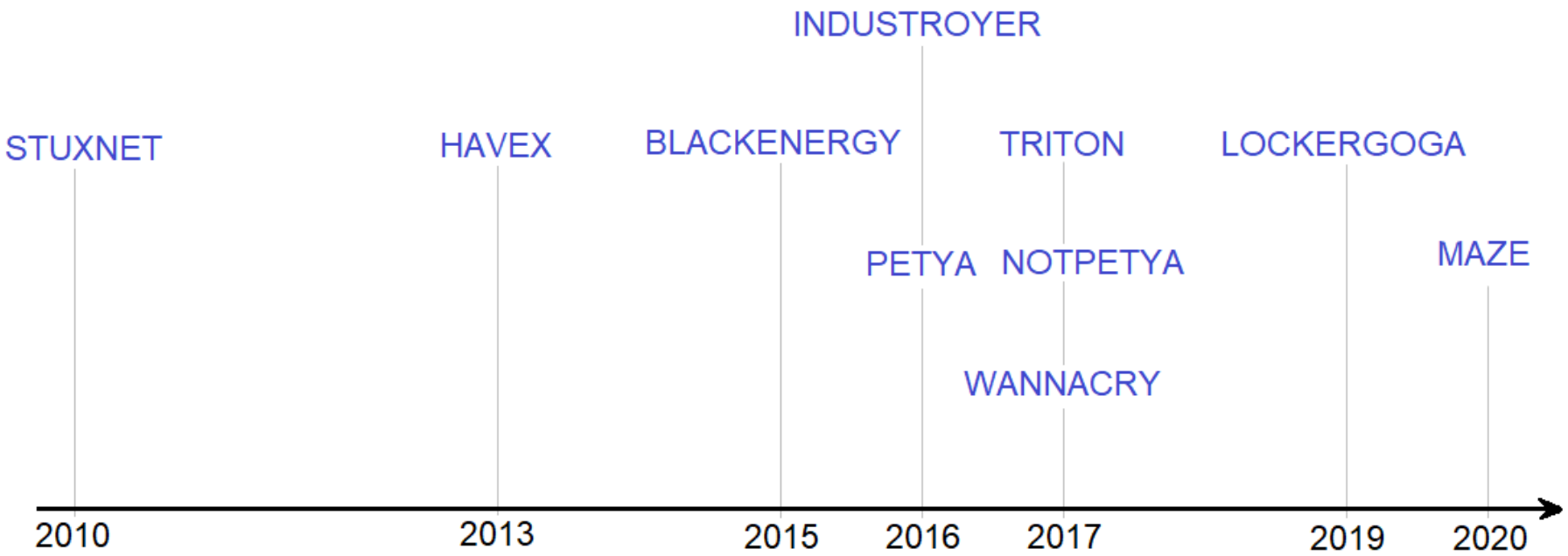
Suivi des conteneurs intéressants par leur voyage.

- Vulnerabilité :

Agents portuaires ciblés via un malware.

Failles dans le logiciel de gestion des conteneurs.

© Document https://www.colsbleus.fr/articles/6515

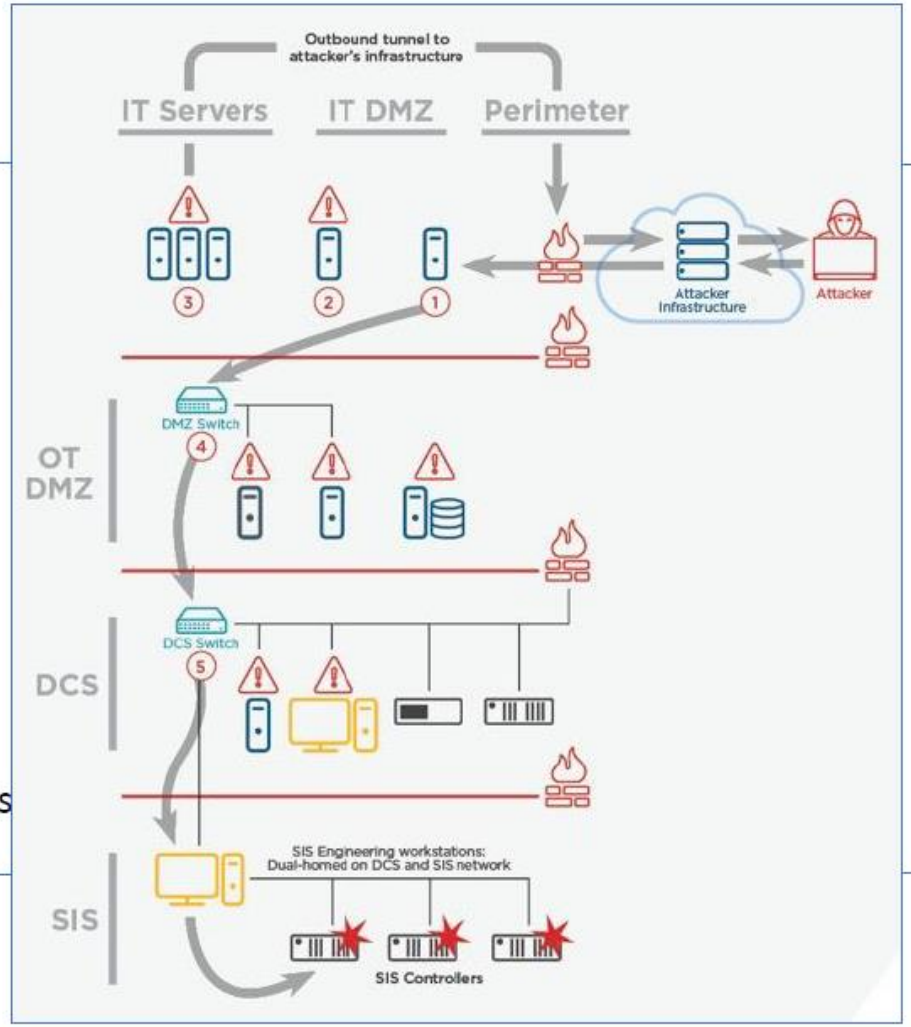


Étude chronologique des principales cyberattaques directes ou indirectes observées contre les systèmes industriels

Le schéma d'attaque "Triton"

IT

L'IT a d'abord été visé pour avoir accès à la DMZ permettant d'avoir la main à distance et de faire de la reconnaissance de réseaux.



OT DMZ

La DMZ OT est une cible principale pour permettre de pivoter vers les systèmes de DCS et SIS.

DCS

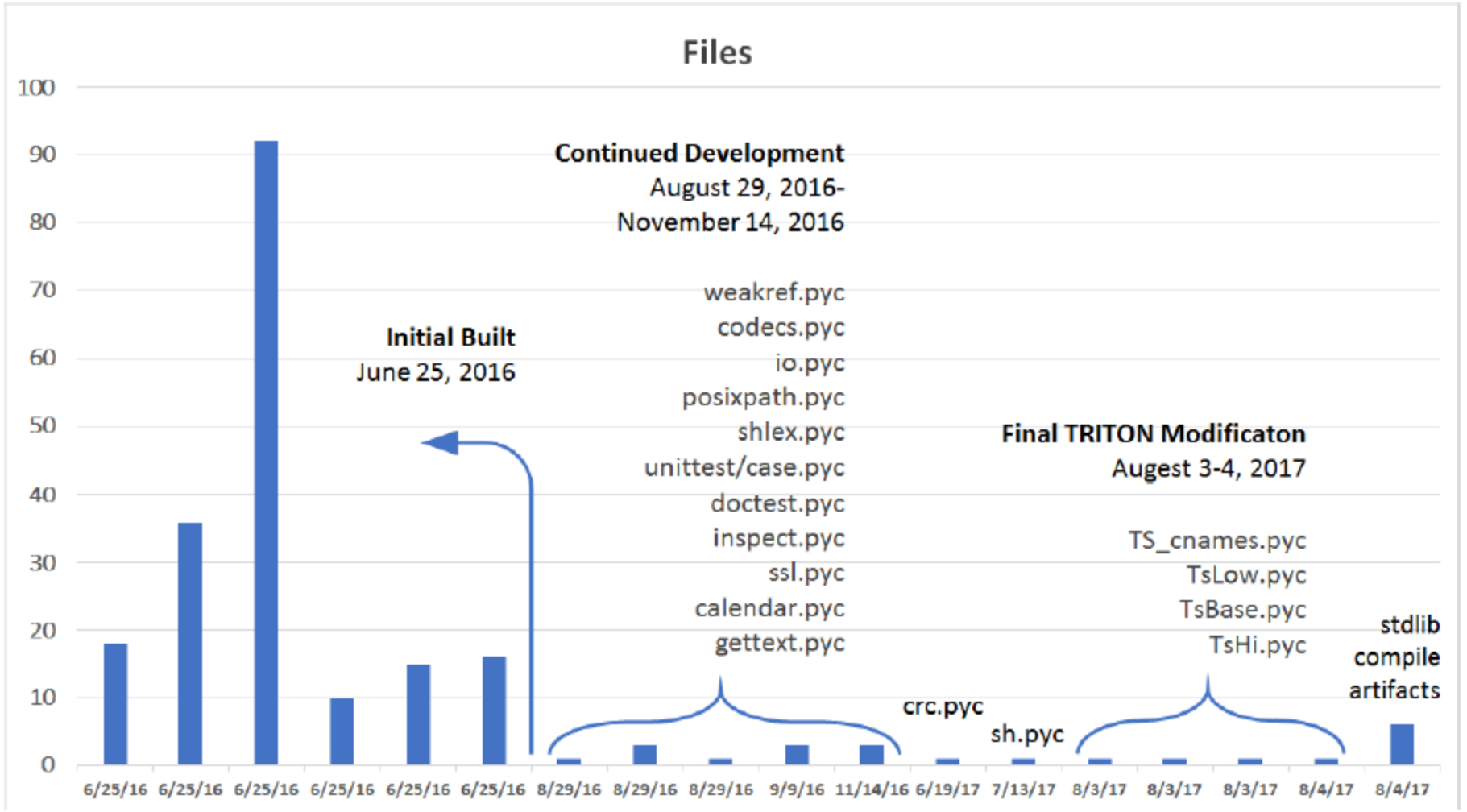
L'attaquant a visé les systèmes DCS

SIS

TRITON a été utilisé ensuite pour cibler les Triconex SIS

©FireEye

Nuit du Samedi 3 juin 2017
Nuit du vendredi 4 août 2017



©FireEye

Nuit du Samedi 3 juin 2017
Nuit du vendredi 4 août 2017

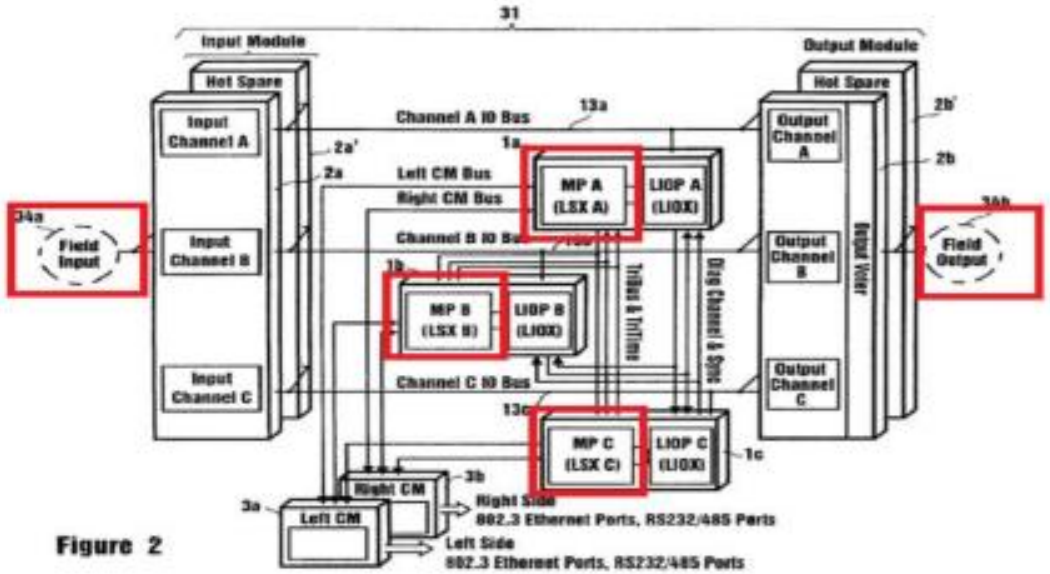
Pourquoi cela a échoué…

- Nouveau matériel avec une triple redondance

Invesys patent: System and Method for Validating Channel Transmission - A system for validating communications between a plurality of processors

Filed: Oct. 24, 2007

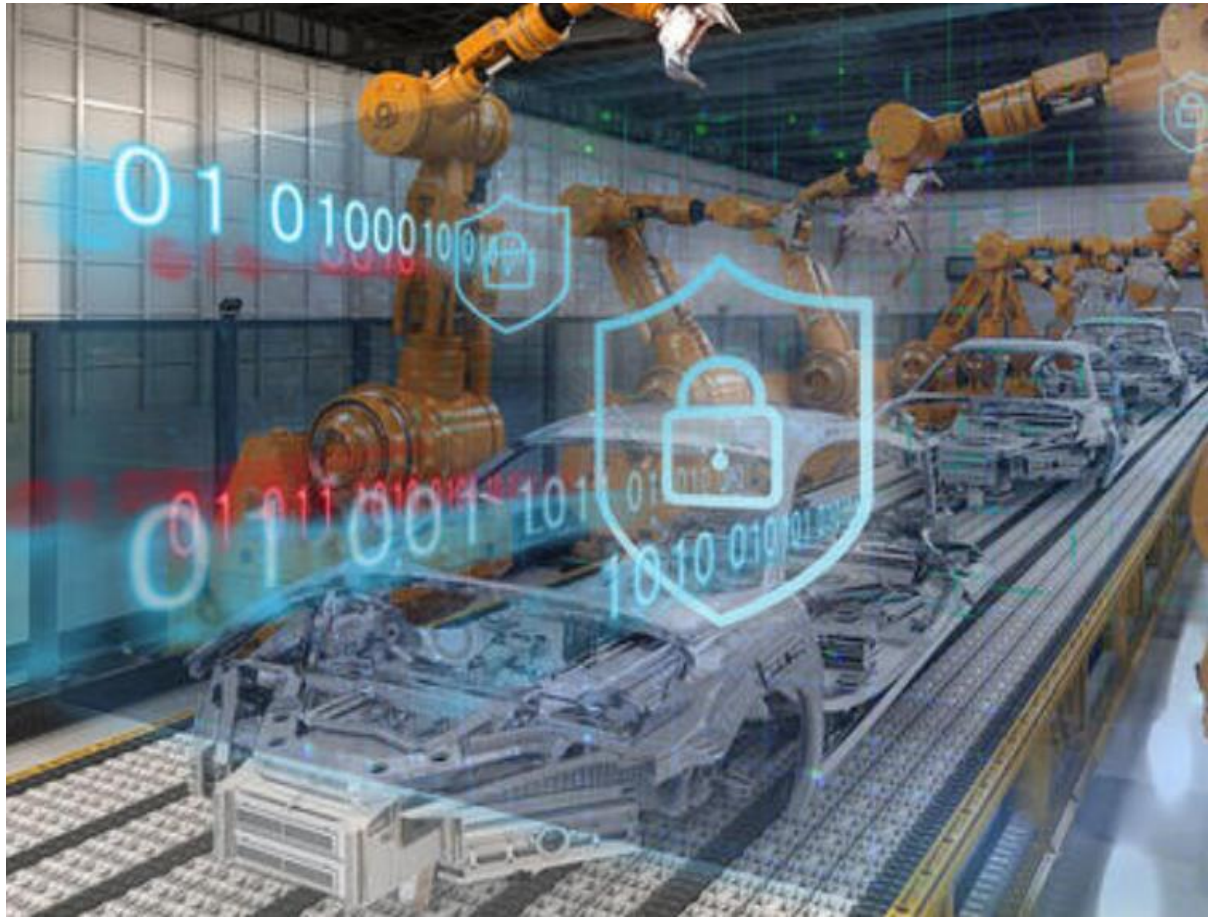
https://patents.google.com/patent/US8037356



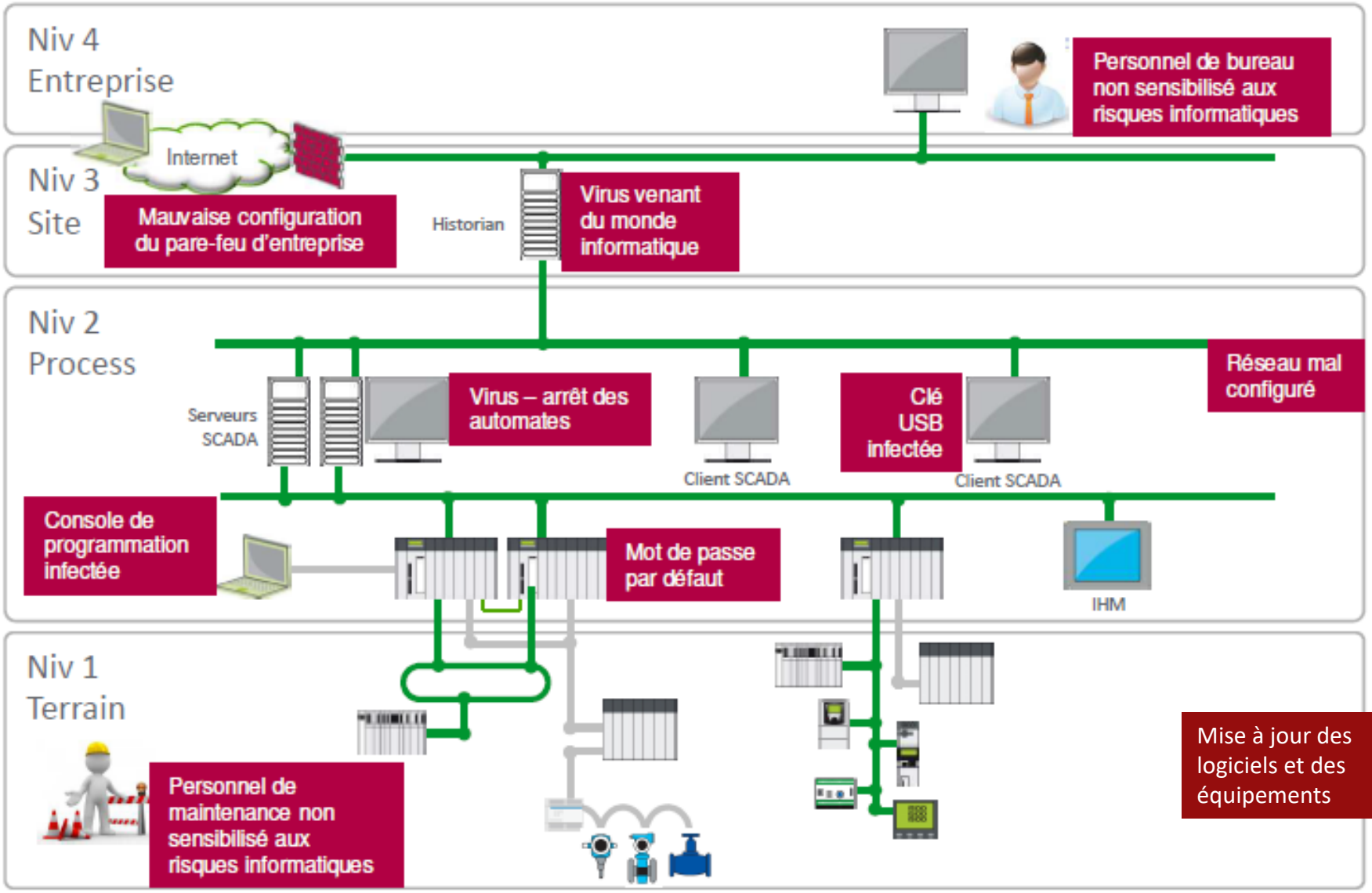
Overall Block diagram of the system -> triple redundant controller (from the patent)

©FireEye

Les vulnérabilités d’un système industriel :



Les principales vulnérabilités d'un système industriel



Utiliser les référentiels existants

- BP01 : Contrôler l'accès physique aux équipements et aux bus de terrain
- BP02 : Segmenter les réseaux
- BP03 : Gérer les médias amovibles
- BP04 : Gérer les comptes
- BP05 : Durcir les configurations
- BP06 : Gérer les journaux d'événements et d'alarmes
- BP07 : Gérer les configurations
- BP08 : Sauvegarder / restaurer
- BP09 : Protéger la documentation
- BP10 : Mettre à jour logiciels / appliquer les correctifs
- BP11 : Sécuriser les automates
- BP12 : Sécuriser les stations d'ingénierie, postes de développement

CyberEdu

La sécurité par l'enseignement supérieur des NTIC

BAC+2 :

IUT LE HAVRE

GÉNIE ÉLECTRIQUE
INFORMATIQUE
INDUSTRIELLE

BAC + 3 :

Merci pour votre attention