Computer Emergency Response Team
Industrie Services Tertiaire

Les attaques APT
Advanced Persistent Threats

Forum 2011

David TRESGOTS
Cert-IST

Sommaire

- APT : De quoi parle-t-on ?
- En quoi les APT diffèrent-elles des autres attaques?
- Est-ce vraiment nouveau ?
- Pourquoi en parle-t-on ?
- Mesures de protection contre les APT
- Une attaque APT hors-norme : Stuxnet !

Computer Emergency Response Team
Industrie Services Tertiaire

APT : De quoi parle-t-on ?

Signification

- *Advanced Persistent Threat*

- *Au sens large, une APT est une catégorie d'attaques mettant en œuvre de nombreuses techniques d'attaques (injection SQL, XSS, etc.).*

- *À ne pas confondre avec AET (Advanced Evasion Techniques)* qui est une technique dite d'évasion

Signification

Advanced Persistent Threat

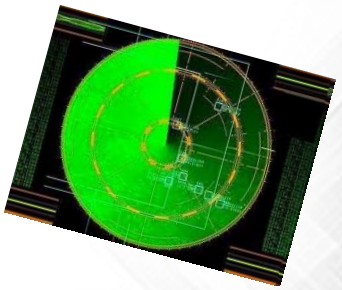
- Attaque dite “avancée” au sens où elle utilise tout un arsenal de techniques d’attaques et d’outils pour atteindre son objectif.
- Unitairement les composants d’une telle attaque ne sont pas forcément “évolués” techniquement (phishing, malware, XSS, etc.). Des outils de génération de composants d’attaques existent (ex. Poison Ivy, etc.)
- La combinaison des méthodes et outils d’attaques en font une attaque avancée.

Industrie Services Tertiaire

Signification

Advanced Persistent Threat

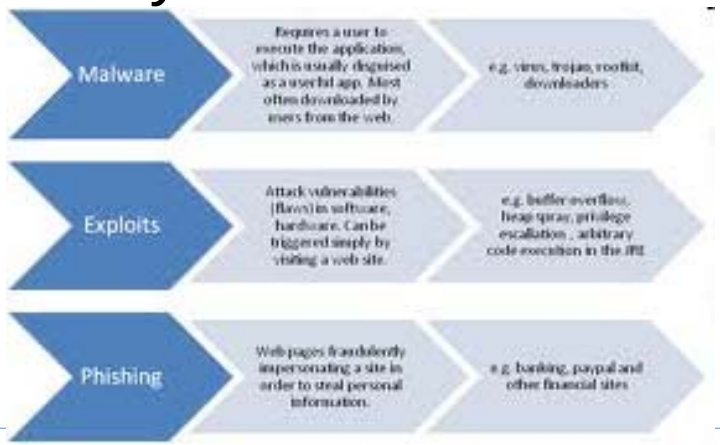
- Attaque basée sur une stratégie dont l'objectif est de rester le plus longtemps possible sans éveiller les soupçons (furtivité), par opposition une attaque "opportuniste".
- L'attaque est scénarisé par les attaquants, et des objectifs précis sont établis pour compromettre toute une chaine de systèmes. Des cibles de replis peuvent être définis.
- L'objectif est de rester sous les "radars" ("low and slow")



Signification

Advanced Persistent Threat

- C’est bien sûr une menace.
- Elle implique une coordination de moyens techniques et humains.
- Elle est généralement peu automatisée (bien que les compromissions de systèmes puissent l’être).
- Les attaquants sont très motivés et dotés de compétences techniques et de moyens inhabituels.



Industrie Services Tertiaire

Origine

L'acronyme « serait » né dans les années 2000. Les agences d'intelligence américaine l'auraient employé pour la première fois pour qualifier une vague d'attaques de cyber-espionnage contre les industries de défense US.

Computer Emergency Response Team
Industrie Services Tertiaire

En quoi les APT diffèrent-elles des autres attaques?

APT vs Attaques traditionnelles

Attaques « Traditionnelles »

- Elles sont généralement menées par un pirate ou un petit groupe de pirates.
- Leurs impacts varient (souvent mineurs et rarement majeurs).
- La cible est généralement découverte de façon opportuniste.
- Les objectifs ne sont pas forcément définis. Ils vont jusqu'où le système permet d'aller, et là où les données sont intéressantes.
- Les compétences du pirate varient (du script-kiddie au blackhat guru)
- La furtivité n'est pas une priorité (tout dépend du niveau de compétences de l'attaquant).
- Les attaques sont souvent menées contre des systèmes faiblement patchés, ou mal/peu administrés.
- La recherche du gain (si tant est qu'il y en ait un) est rapide.
- Les pirates recherchent généralement une sorte de reconnaissance après leurs méfaits.

Attaques APT

- Elles sont dites à « signaux faibles » mais leur impact est majeur (Low-frequency & high-impact)
- Elles sont basées sur des objectifs et une stratégie (pas d'improvisation)
- Les techniques employées sont sophistiquées.
- Elles nécessitent de la coordination entre les pirates qui les conduisent.
- Elles nécessitent des bonnes compétences techniques (pas tout le temps)
- L'attaque doit rester furtive
  - Ne pas générer de bruits (sous le radar)
- Le gain financier ou industriel n'est pas immédiat
  - L'attaque doit durer jusqu'à l'atteinte de l'objectif.
  - Dans le cas de vol d'information et d'exfiltration de données, cela peut être très long.
- Elles ont un coût non-négligeables
  - Exit les script-kiddies et les hackers en quête de notoriété
  - A priori elles sont orchestrées par le crime organisé, des groupes militants, voire des Etats

Industrie Services Tertiaire

Vecteurs d'attaque

- Distants (ex. via Internet)
  - Phishing
  - Drive by download
  - Clickjacking
  - Pièce jointe piégée transmise par email ou hébergée
  - Détournement de trafic
  - Partage réseau piégé (WebDAV, FTP...)
  - Réseaux sociaux,
  - Forum communautaire piégé,
  - Logiciels piégés (chevaux de Troie, Backdoors, etc.)
  - Etc.
- Locaux (ex. accès physique)
  - Supports amovibles infectés (clé USB, CD/DVD, cartes mémoires…)
  - Partages réseaux Intranet (SMB, ...)
  - Attaques MITM
  - Etc.
- Humains
  - Spear Phishing
  - Réseaux sociaux,
  - Forum piégé,
  - Chat
  - Etc.

Industrie Services Tertiaire

Particularités des APT

- Les attaques APT utilisent les mêmes vecteurs d'attaques que les attaques traditionnelles pour compromettre leurs cibles, et ce malgré la présence de protections périmétriques (firewall, IDS, IPS, etc.).

- Elles ne cherchent pas systématiquement à exploiter une vulnérabilité. Si l'attaquant peut passer par la porte, il l'utilisera (ex. vol de comptes d'accès VPN, identifiants, etc.). C'est le meilleur moyen de rester furtif (pas de blocage du système ou d'une application, pas de logs générés, etc.)

- Le facteur humain (social engineering, réseaux sociaux, forum, chat, etc.) est plus souvent utilisé dans les attaques APT que dans les attaques classiques.

  L'utilisateur a tendance à dire beaucoup de choses (trop) et ne pas mesurer les informations qu'il manipule.

- On notera que les attaques APT mettent rarement en œuvre des attaques de type « déni de service » ou des « defacements ».

Anatomie d'une attaque APT

- Préparation de l'attaque et des objectifs
- Elaboration de la stratégie d'attaque
- Intrusion furtive dans l'infrastructure de la cible
- Repérage et état des lieux de l'écosystème cible (scan, capture réseau, etc.)
- Compromission de systèmes, récupération d'identifiant, de comptes, d'adresse
- Exécution de code (backdoors, chevaux de Troie, proxy, etc.) et déploiement d'outils (ex. RAT, kits etc.)
- Recherche de nouvelles cibles & développement de codes malveillants ciblés
- Utilisation de privilèges obtenus pour accéder aux données
- Exfiltration des données (protocoles légitimes, emails, covert-channels)

Industrie Services Tertiaire

Est-ce vraiment nouveau ?

CERTIST
Industrie Services Tertiaire

- Le vol d'informations, l'espionnage industriel, l'atteinte à l'image, la déstabilisation (pour ne citer qu'eux), ont toujours existé dans le monde de l'entreprise, de l'industrie (sous une forme ou sous une autre) et plus généralement dans notre société.

- Aujourd'hui, la forme des attaques a changé. « L'ennemi d'antan » est toujours le même, les armes, les motivations et les objectifs sont différents.

- Les attaques informatiques ont également évoluées.
  - Dans les années 1990, les attaquants étaient motivés par des aspects ludiques, voire technologiques (époque des virus, des buffers overflow « smashing the stack for fun and profit », etc.), par le fait de pousser la technologie au maximum, par la recherche de la reconnaissance...
  - Ensuite les pirates ont acquis de la compétence, et leurs objectifs ont changé. Ils ont créé des marchés parallèles dans l'underground pour échanger des méthodes d'attaques, des outils et surtout des données collectées, voire aussi pour les vendre.
  - Maintenant, ils se sont « professionnalisées », les attaques sont plus abouties, et techniquement évoluées. Leurs compétences sont souvent en avance sur la sécurité.

- Aujourd'hui, les pirates ont une capacité d'adaptation et d'appropriation des nouvelles technologies (et de leurs faiblesses), qui leur donnent une avance non négligeable. Il est récurrent d'entendre que la sécurité est en retard sur les attaquants.

Evolution des contextes

- Le nature du contexte industriel a changé.
- La concurrence entre les sociétés est plus forte.
- Les contextes géopolitiques sensibles poussent les Etats à se protéger et à se donner des moyens d'attaquer (ex. Stuxnet).

  Certains Etats seraient (ont déjà) mis sur pied des cyber-armées.
- Les attaques liées aux APT ne sont donc pas nouvelles en soit.
- Ce qui a fondamentalement changé ce sont les motivations de ces attaques et leur mise en œuvre.

Pourquoi en parle-t-on ?

CERTIST
Industrie Services Tertiaire

On en parle car :

- Les cibles sont sensibles
  - Sociétés, industriels majeurs
  - Entités gouvernementales, politiques, etc.
  - OIV (énergies, télécommunications, etc.)
  - Etc.
- Les intérêts sont nombreux :
  - Commerciaux
  - Concurrentiels
  - Industriels / Technologique
  - etc.
- Leurs impacts sont majeurs
  - Financier
  - Réputation
  - Crédibilité
  - Voire vitaux (nucléaires, énergies, etc.)
- Elles sont sophistiquées et suscitent parfois une sorte d'admiration
  - Compétences techniques évoluées (ex. Stuxnet, RSA, etc.)
  - Pas à la portée de tout le monde
- Les auteurs présumés sont souvent sujet a des tensions géopolitique majeure
  - Crime organisé, Etats, etc.
  - La Chine est souvent montrée du doigt.
- Mais aussi parce que celles qui sont découvertes, sont fortement médiatisées !

Quelques exemples

- 2000 : Attaques massives contre les infrastructures militaires américaines
  - Principales cibles l'US Air force, etc.
  - Vol de plans aéronautiques

- 2003 : Enquête de l'attaque « Titan Rain » par le FBI
  - Attaques massives des systèmes informatiques gouvernementaux américains.
  - Utilisation de techniques très variées proxy, PC zombies computer, spyware, virus

- 2008 : DoD (Department of Defense) américain
  - Operation Buckshot Yankee

- 2009 : Night Dragon
  - Découvert par McAfee
  - Cibles : compagnies pétrolières et énergétiques
  - Objectif : vol d'informations dans les technologies de l'énergie (email, documents, etc.)
- 2009 : Stuxnet
  - Découvert par McAfee
  - Cibles : centrifugeuses nucléaires iraniennes
  - Objectif : saboter le programme de nucléarisation de l'Iran

- Fin 2009 : Opération Aurora (Google, Adobe et bien d'autres)

Google™ Adobe™

- 2011 : RSA (SecurID)
  - Cibles : vol d'informations concernant le système de cryptographie two-factors de RSA
  - Objectif : incertain, a priori compromettre les clients exploitant cette solution.

RSA® The Security Division of EMC

- 2011 : Bercy
  - Cibles : systèmes internes (a priori + de 150 systèmes infectés)
  - Objectif : incertain

MINISTÈRE DE L'ÉCONOMIE DES FINANCES ET DE L'INDUSTRIE

Industrie Services Tertiaire

Computer Emergency Response Team
Industrie Services Tertiaire

Mesures de protection contre les APT

Protections en profondeur

A défaut de pouvoir bloquer les APT, il faut pouvoir freiner les attaquants

- Maintenir à jour ses systèmes
  - Systèmes et applications (Java, IE, etc.)
  - Protection périmétriques (Firewall, IDS, IPS, DLP, etc.)
  - Solutions antivirales

    L'attaque Aurora aurait pu être stoppée, ou ralentie si des utilisateurs n'utilisaient pas IE6.
    Stuxnet exploitent de nombreuses vulnérabilités connues depuis très longtemps.

- Sensibiliser les utilisateurs
  - A être vigilent
  - A remonter toutes anomalies
    - Compte bloqué
    - Problème à l'ouverture d'un fichier (PDF ou autres)
  - Aux bonnes pratiques de sécurité.

- Sensibiliser les HelpDesks
  - Anomalies récurrentes
    - Ex. comptes bloqués chez un ou plusieurs utilisateurs (cas de Night dragon)

- Préparer les administrateurs et les équipes sécurité
  - A collecter des informations (les logs)
  - A remonter aussi toutes anomalies
    - Connexion depuis des zones inhabituelles (pays)
    - Connexion à des heures inhabituelles
    - Etc.
  - Surveiller périodiquement les systèmes d'information

Computer Emergency Response Team
Industrie Services Tertiaire

Une attaque APT hors-norme : Stuxnet !

Stuxnet : quelques rappels

- Stuxnet est un ver informatique utilisé dans le cadre d'une attaque APT visant à compromettre des systèmes de contrôle industriels.

- Le code malveillant a pour objectif (semblerait-il) d'endommager les centrifugeuses nucléaires de Natanz (notamment entre autre, en changeant sa vitesse de rotation).

- Découvert le 17 juin 2010 par une société biélorusse développant des produits antivirus (VirusBlokAda).
- Des traces montreraient que Stuxnet officiait déjà en 2009 (probablement des tests de la part des concepteurs).

Stuxnet : quelques rappels (suite)

- Stuxnet est capable d'infecter des infrastructures de supervision SCADA insuffisamment sécurisées
- Initialement Stuxnet n'était pas identifié comme un malware s'attaquant aux systèmes SCADA (Supervisory Control and Data Acquisition)

- 1er ver (connu) à s'attaquer à des systèmes de contrôles industriels (ICS). Dans le cas présent les systèmes d'automates Siemens PCS7

- Le code a pour objectif d'attaquer les applications de supervision WinCC de Siemens fonctionnant sous Windows et permettant de piloter les équipements.

- Le facteur humain a été privilégié pour conduire l'attaque, par l'intermédiaire de clés USB

- Des vulnérabilités jusque là inconnues ont été utilisées.

Industrie Services Tertiaire

Stuxnet : quelques rappels (suite)

- En effet, 4 failles 0day exploitées composent l'arsenal d'attaque du ver Stuxnet
  - Vulnérabilité (CVE-2010-2568) dite « LNK » dans Windows (faille corrigée par un bulletin hors cycle de Microsoft MS10-046)
  - Vulnérabilité RPC dans le service Server (CVE-2008-4250). Notoirement connue pour être la 1ère vulnérabilité exploitée par le ver Conficker (MS08-067)
  - Vulnérabilité (CVE-2010-2729) dans le spooleur d'impression (MS10-061)
  - Vulnérabilité (CVE-2010-3338) dans le Task scheduler (MS10-092) de Microsoft Windows

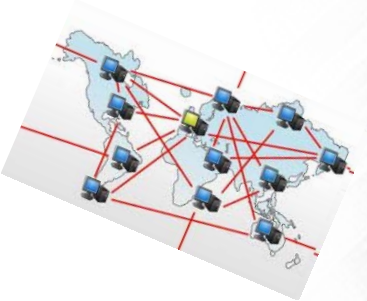
- Le rootkit exploité par Stuxnet utilise des drivers signés (légitimes) !

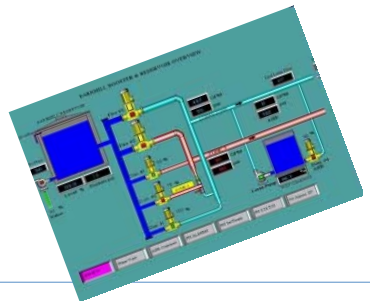
Industrie Services Tertiaire

Stuxnet : quelques rappels (suite et fin)

- Mais aussi, les mots de passe des applications Siemens étaient codés en dur !

- Les techniques d'attaque utilisées par Stuxnet sont courantes dans l'IT conventionnelle :
  - Rootkits (qui plus est signé)
  - Protocole d'échanges P2P (dialogue avec les machines infectées, et le C&C)
  - Failles 0-days (vulnérabilités non-patchées),
  - Faiblesse des mots de passe
  - Etc.





- C'est moins le cas dans le monde SCADA. Un rootkit affectant le PLC (Programmable Logic Controller) est une première.

Industrie Services Tertiaire

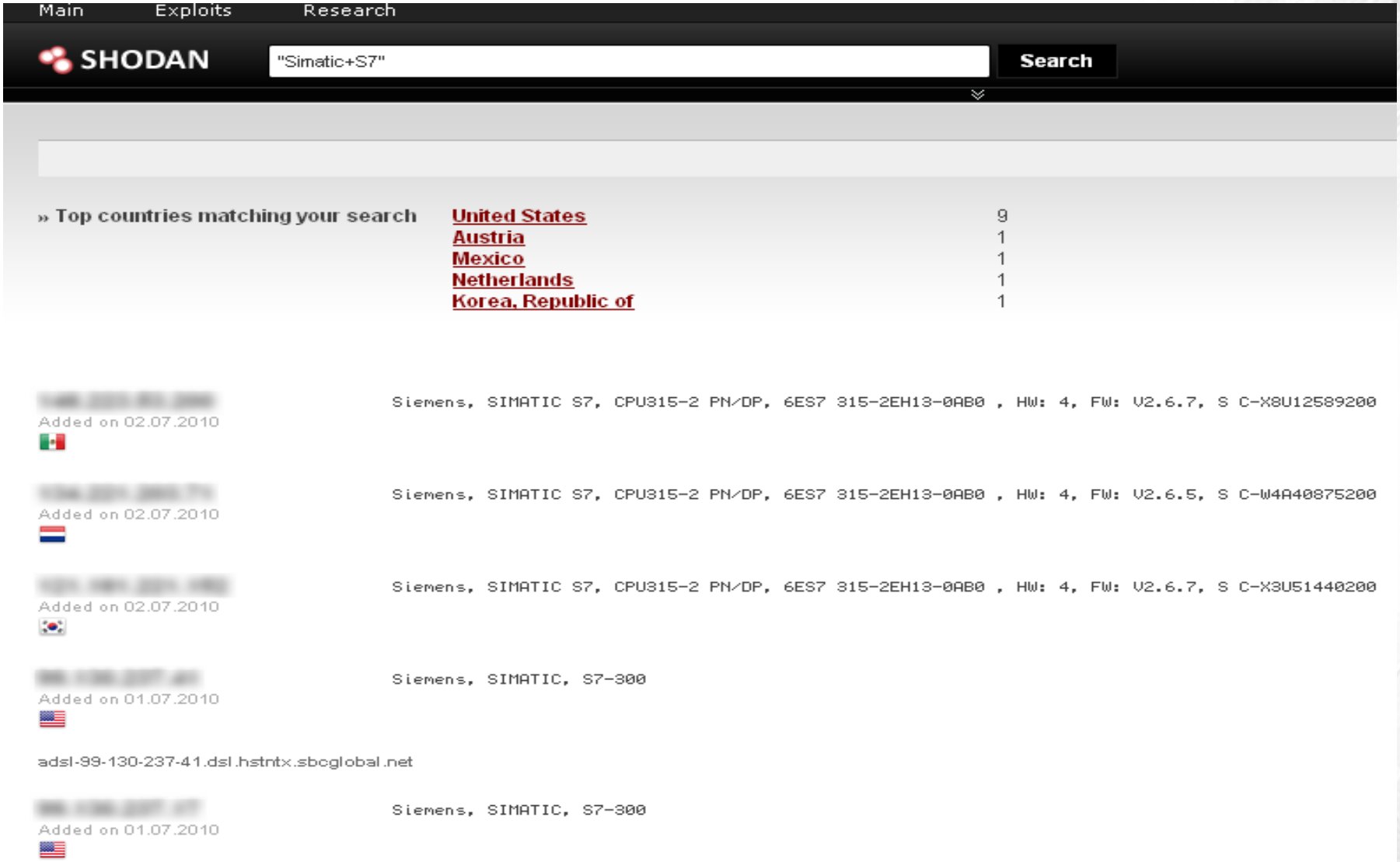
Quid de la sécurité dans l'informatique industrielle

- Stuxnet est l'APT qui a changé la vision de la sécurité non seulement dans le monde de l'informatique des systèmes de contrôle industriels (ICS), mais aussi dans l'informatique IT tout court.

- Le SCADA doit tirer les leçons apprises de la sécurité du monde IT, car les enjeux ne sont plus les mêmes !

- Les bonnes pratiques de sécurité restent à être mises en œuvre.
  - Ne plus coder en dur les mots de passe codés par exemple (ex. Siemens),
  - Développer/renforcer le patch management,
  - Sensibiliser les utilisateurs et les industriels du SCADA,
  - Etc.

- Cependant le chemin sera long, … Le monde SCADA n'est pas préparé à ces types de menaces comme le montre l'illustration suivante !!!
  - Des aberrations subsistent !


Main
Exploits
Research
SHODAN
"Simatic+S7"
Search
» Top countries matching your search
United States 9
Austria 1
Mexico 1
Netherlands 1
Korea, Republic of 1
Siemens, SIMATIC S7, CPU315-2 PN/DP, 6ES7 315-2EH13-0AB0 , HW: 4, FW: V2.6.7, S C-X8U12589200
Added on 02.07.2010
Siemens, SIMATIC S7, CPU315-2 PN/DP, 6ES7 315-2EH13-0AB0 , HW: 4, FW: V2.6.5, S C-W4A40875200
Added on 02.07.2010
Siemens, SIMATIC S7, CPU315-2 PN/DP, 6ES7 315-2EH13-0AB0 , HW: 4, FW: V2.6.7, S C-X3U51440200
Added on 02.07.2010
Siemens, SIMATIC, S7-300
Added on 01.07.2010
adsl-99-130-237-41.dsl.hstntx.sbcglobal.net
Siemens, SIMATIC, S7-300
Added on 01.07.2010

Des questions ?

Fin de la présentation

Merci