Stuxnet

Sérgio Cordeiro

Segurança Cibernética, Autose, 2015

Referências

- **Byres e Howard:** ***Analysis of the Siemens WinCC / PCS7 "Stuxnet" Malware for Industrial Control System Professionals*** **(2010)**
- **Langner:** ***To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve*** **(2013)**

  `http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf`
- **Nachenberg:** ***A Forensic Dissection of Stuxnet*** **(2012)**

  `http://www.ttivanguard.com/ttivanguard_cfmfiles/pdf/sanjose12/sanjose12session7117.pdf`

Sumário

- O Stuxnet é um programa malicioso extremamente sofisticado projetado para atacar um sistema industrial específico.
- Descoberto em 2010, vem sendo analisado até hoje. Posteriormente, descobriu-se uma versão anterior, datada de 2005.
- Provavelmente desenvolvido por um estado nacional.
- Primeiro ataque a um sistema SCADA registrado na história.

Sofisticação

- Explora 4 vulnerabilidades do Windows desconhecidas à época
- Explora características específicas da plataforma Siemens
- Explora características específicas da planta alvo
- Difícil de ser descoberto mesmo depois de executar o ataque
- Alvo: planta de enriquecimento de Urânio de Natanz (Irã)

Ciclo de vida

- inserido em PCs de empresas de engenharia no Irã por meio de drives USB
- conecta-se a um centro de controle remoto
- infecta novas máquinas pela rede Ethernet ou por meio de drives USB
- quando encontra uma estação de engenharia Siemens, infecta arquivos específicos da plataforma
- quando se encontra na planta alvo, infecta os PLCs
- periodicamente, executa a ação de ataque

Efetivamente, consiste em duas partes:

- um verme (*worm*) que propaga a infecção
- um núcleo, que executa o ataque

O verme

- Explora as vulnerabilidades do sistema para se instalar e se propagar
- Verifica se deve instalar o núcleo
- Comunica-se com o centro de controle remoto para receber atualizações e instruções e registrar suas ações

Além de verme, tem características de vírus e de *rootkit*, além de ser polimórfico.

O núcleo

- Infecta DLL da Siemens que faz interface entre o PC e o PLC
- Infecta arquivos de programa Step 7 quando o programador é executado
- Programa infectado é eventualmente copiado para o PLC pelo programador
- Após a infecção, o ataque é executado periodicamente pelo programa infectado

Destaques

O verme se comporta de forma tradicional; a única característica notável é o fato de explorar muitas vulnerabilidades inéditas à época. O núcleo é a parte que apresenta maiores novidades:

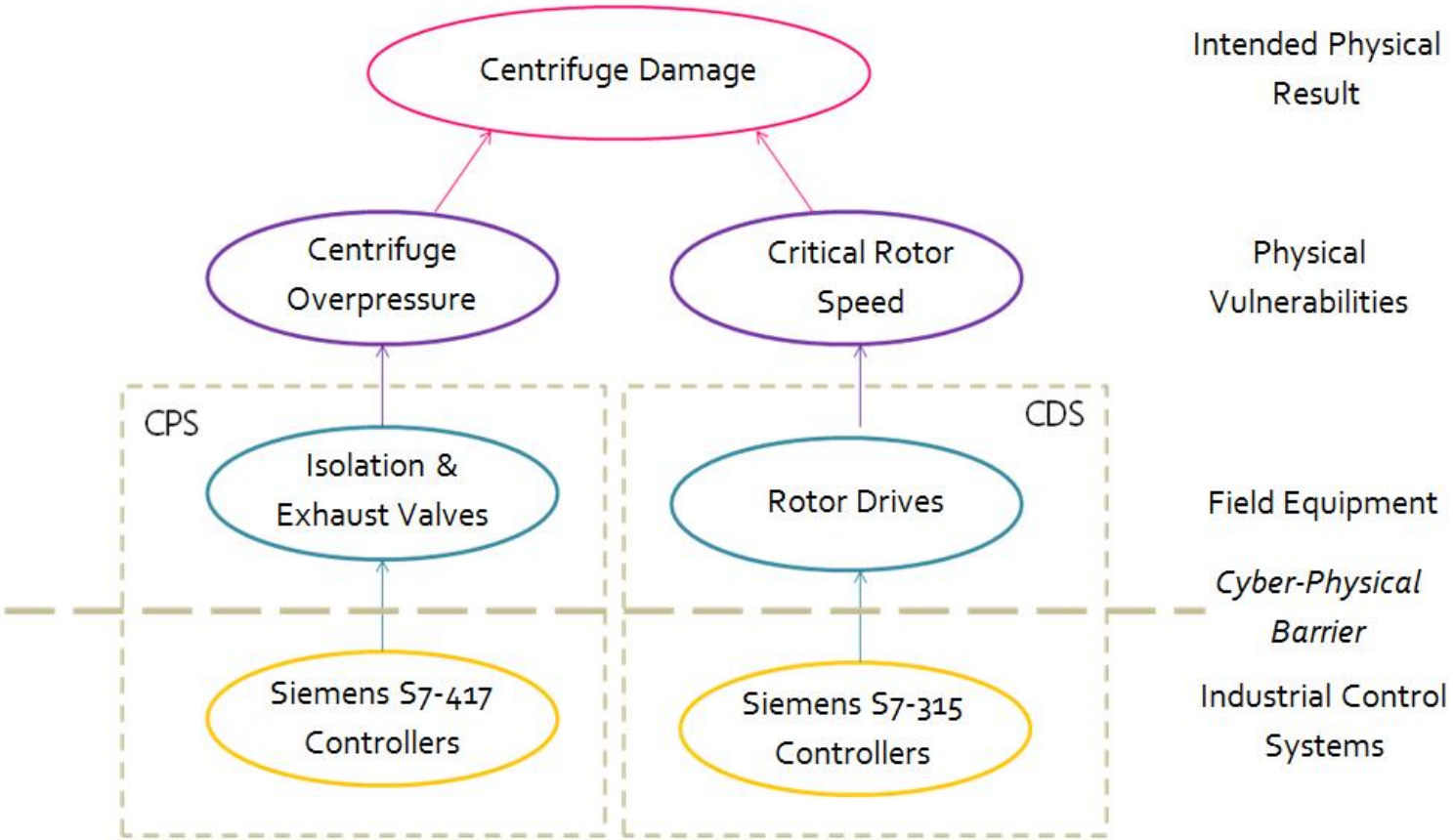
- Infecta o PLC, não apenas o PC
- Explora vulnerabilidades da plataforma Siemens:
  - senha fixa entre o WinCC e o SQLServer
  - blocos podem ser criptografados
- Explora características específicas da planta alvo:
  - Endereços de I/O determinados
  - Processo de controle de velocidade das centrífugas
  - Processo de regulação de pressão nas centrífugas (versão antiga)

O ataque

- Versão antiga:
  - Fecha determinadas válvulas de forma a fazer aumentar a pressão em algumas centrífugas
  - Impede a abertura das válvulas de alívio de pressão
  - Apresenta ao operador dados falsos sobre o processo, para evitar intervenção manual
- Versão mais recente:
  - Aumenta o setpoint do inversor em 40% ou
  - Diminui para uma velocidade muito baixa
  - Depois de alguns minutos, volta ao normal

Em ambas as versões, executa o ataque com pequenas frequência e duração, para evitar ser identificado

O ataque


Centrifuge Damage
Intended Physical Result
Centrifuge Overpressure
Critical Rotor Speed
Physical Vulnerabilities
CPS
CDS
Isolation & Exhaust Valves
Rotor Drives
Field Equipment
Cyber-Physical Barrier
Siemens S7-417 Controllers
Siemens S7-315 Controllers
Industrial Control Systems

Resultados

- O objetivo do ataque é danificar o equipamento no médio prazo.
- Não se tem confirmação do sucesso do ataque, mas aparentemente 10% das centrífugas foram danificadas.
- O ataque do Stuxnet não poderia ter sido evitado por meios tradicionais.
- Os danos (e talvez também a infecção) seriam evitados por meio de boas práticas de engenharia.

Defesas tradicionais

- *hardening*/*patching*/atualizações de software/firmware
- segregação/segmentação
- monitoramento da rede
- bloqueio de portas USB
- equipe de resposta a incidentes
- anti-virus/descobridor de *rootkits*
- AAA
- certificados digitais

Boas práticas

- Virtualização de desktops (VDI) e de servidores

  na reinicialização sempre se lê uma imagem não corrompida

- Uso de controle de versão centralizado

  controle do que foi alterado de uma versão para a outra

- Uso de relés de segurança, válvulas auto-operadas, sistemas redundantes, maior monitoramento

  robustez do projeto de automação

- Dimensionamento correto dos equipamentos

  robustez dos projetos elétrico e mecânico

- Uso de software de código aberto

  facilita a análise