



Relazione Sicurezza Informatica

01/06

STUXNET

L'INIZIO DELLA CYBERWAR

Arianna Cipolla

Università degli studi di Parma
arianna.cipolla@studenti.unipr.it





CINQUE DOMANDE

- 1. Quando : 2010
- 2. Chi : Israele + USA
- 3. Dove : Iran, Natanz
- 4. Perché : Armi Nucleari
- 5. Come : Worm





3 SOFTWARE ATTACCATI

01

Windows

Sfruttarono le vulnerabilità di Windows XP/7 nel 2010:

- CPLINK
- Windows Print Spooler
- Conficker
- Driver

02

Siemens S7

- Libreria `s7otbxdx.dll` di Siemens WinCC
- Man In The Middle
- Replay
- NO Autenticazione e Crittografia

03

PLC

- Solo i PLC con determinate caratteristiche
- Blocco di memoria delle macchine
- Modifica delle frequenze di velocità delle centrifughe





ELIMINARE LA MINACCIA



Come ha agito Siemens:

- ha messo a disposizione uno strumento in grado di rilevare e rimuovere gli Stuxnet
- ha sviluppato S7 Plus, un nuovo protocollo che risolveva i problemi principali che aveva S7

Consigli che le aziende possono attuare per proteggersi dalle minacce informatiche:

- Isolamento delle reti industriali
- Lista di permessi per le applicazioni
- Gestione rigorosa dei supporti rimovibili
- Hardening dell'host
- Utilizzo di comunicazioni criptate





DANNI|DENARO



Stuxnet ha sabotato circa 1.000 centrifughe, danneggiandone il 10-20%. Il danno stimato è di 2-3 miliardi di dollari tra attrezzature distrutte e ritardi nel programma nucleare iraniano.

Riporto il numero di computer trovati infetti alla data del 6 agosto 2010:

- Iran: 62.867
- Indonesia: 13.336
- India: 6.552
- Stati Uniti: 2.913
- Australia: 2.436
- Regno Unito: 1.038
- Malesia: 1.013
- Pakistan: 993
- Finlandia: 7
- Germania: 5





Per redigere al meglio questa relazione ho dovuto fare riferimento ad alcuni link informativi trovati in rete, che cito d seguito:

- [Wikipedia](#)
- [StormShield](#)
- [MalwareBytes](#)
- [NordVPN](#)

BIBBLIOGRAFIA

