



INFORMATICA: Stuxnet un virus che pochi conoscono

Redazione, 26/05/2011 - 23:08



Da Wikipedia, l'enciclopedia libera.

Stuxnet è il primo worm che spia e riprogramma PC industriali. Infetta PC dotati di sistema operativo Windows e software WinCC e PCS 7. Il virus si propaga tramite penna USB o tramite rete, e si attiva alla semplice apertura in visione del dispositivo che lo contiene. È stato scoperto nel giugno del 2010 da VirusBlokAda, una società di sicurezza bielorusa. Stuxnet è in grado di riprogrammare il controllore logico e di nascondere le modifiche.

Storia

A metà giugno 2010 la società VirusBlokAda ha segnalato la sua esistenza, e l'inizio della sua progettazione è stato datato al giugno 2009. La società Symantec afferma che la maggior parte dei computer infetti siano in Iran: da qui le speculazioni in base alle quali l'obiettivo del virus potrebbero essere le centrali nucleari in costruzione nel paese asiatico.

Tale virus, definito anche arma informatica, ha già contagiato oltre a numerosi computer iraniani, anche la Cina. L'Unione europea è intenzionata a creare una normativa ad hoc per contrastare tale fenomeno.

Modalità di funzionamento

L'attacco al sistema operativo prende di mira i programmi di monitoraggio e controllo industriale SCADA/WinCC e PCS 7.

La diffusione iniziale avviene tramite penna USB infetta per poi contaminare gli altri PC collegati alla rete WinCC. Dopo aver raggiunto l'ingresso del sistema, Stuxnet utilizza parole d'ordine di default per ottenerne il controllo: per questo il produttore, Siemens, consiglia di modificare la parola d'ordine originale.

La complessità di Stuxnet è insolita per un virus informatico in quanto l'attacco richiede la conoscenza dei processi industriali e mira all'attacco a infrastrutture industriali.

Vista la complessità del virus, per la sua realizzazione si sarebbe dovuto impiegare un team di programmatori di diverse



La Talpa Online

Il Giornalino Online
Della Scuola Secondaria
Di Fontaneto d'Agogna

<http://talpaonline.altervista.org/portale/news.php?item.266>

Pagina 2/2

discipline e la verifica di sistemi reali per evitare di bloccare il funzionamento del PLC. Secondo tecnici Siemens la creazione di questo malware avrebbe richiesto mesi se non anni di lavoro se eseguita da una sola persona.

L'alias di stuxnet Ã ' Ã  : roj/Stuxnet-A, W32/Stuxnet-B, W32. Temphid, WORM_STUXNET.A, Win32/Stuxnet.B, Trojan-Dropper:W32/Stuxnet, W32/Stuxnet.A, Rootkit.Win32.Stuxnet.b, Rootkit.Win32.Stuxnet.a.

[Inviata da cicconi]