TD SYNNEX

Nella mente di un Hacker: Stuxnet

Il primo caso di guerra digitale

21 Marzo 2025

Webinar

Andrea Pezzoni – Security Presales Specialist – TD SYNNEX

7 tipi di Threat Actor

Cyber Crime Organizations

Hacktivists

Insider Threats

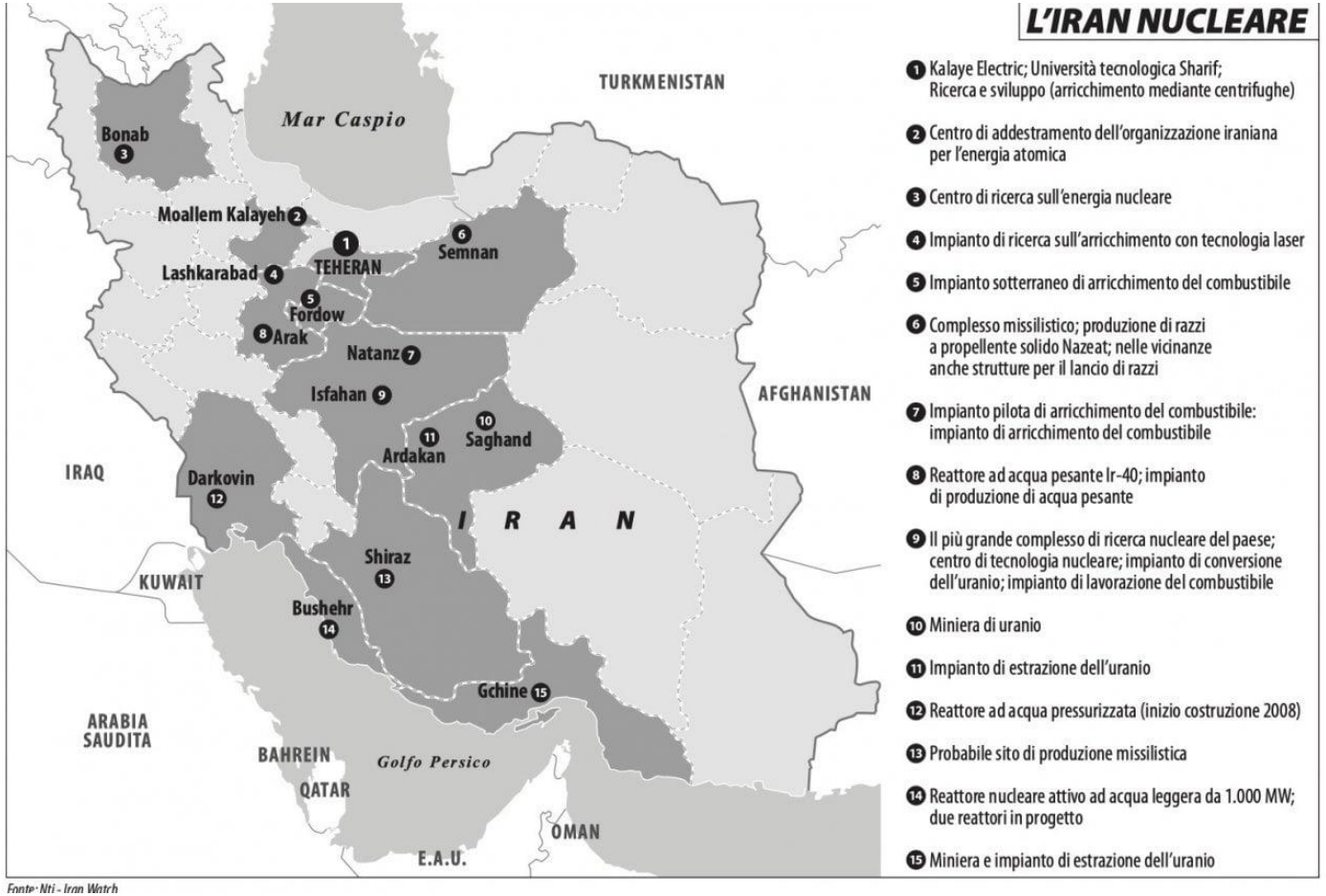
Cyber Extorsionist

Script Kiddies

State Sponsored Hackers

Cyberterrorists

Situazione Geopolitica



Fonte: Nti - Iran Watch

- Ahmadinejad presidente Iran (2005-2013)
  - Riavvio programma nucleare
  - Costruzione centrale di Natanz
- George W. Bush e Barack Obama presidenti USA
  - Sanzioni verso Iran (2010)
- Benjamin Netanyahu primo ministro israeliano

La centrale di Natanz

- 2002 tramite immagini satellitari, i ricercatori di Institute for Science and International Security (ISIS) scoprono la costruzione di un impianto sotterraneo a Natanz.
- Programma nucleare iraniano è sotto monitoraggio da parte di International Atomic Energy Agency (IAEA)
- A Natanz 8.700 centrifughe per arricchimento dell'Uranio
  - 10% di sostituzione per anno
  - Dicembre 2009 – Gennaio 2010 tra le 800 e le 1.000 sostituzioni, forse 2.000

Le 7 fasi di attacco

Reconnaissance

Weaponisation

Delivery

Exploitation

Installation

Command and control

Actions on objectives

Un nuovo attacco in the wild

- Nel Giugno 2010 un reseller iraniano del software bielorusso VirusBlokAda apre un ticket al supporto per segnalare un comportamento anomalo su alcuni client, alcuni dei quali, anche dopo la formattazione, andavano incontro a continuo riavvio.
- In breve tempo si trovò la causa in un driver di sistema modificato a livello di sistema operativo
- La fonte dell'infezione sembrava essere la combinazione di 4 file derivanti da una periferica USB.
- I Sistemi di sicurezza venivano bypassati a causa di una rootkit di offuscamento e della vulnerabilità di Windows legata ai processi .LNK, necessari per l'inventory delle cartelle. Al contrario dei classici virus derivanti dal processo autorun, non si era mai visto nessun attacco provenire dai processi .LNK.

Mascheramento degli attacchi

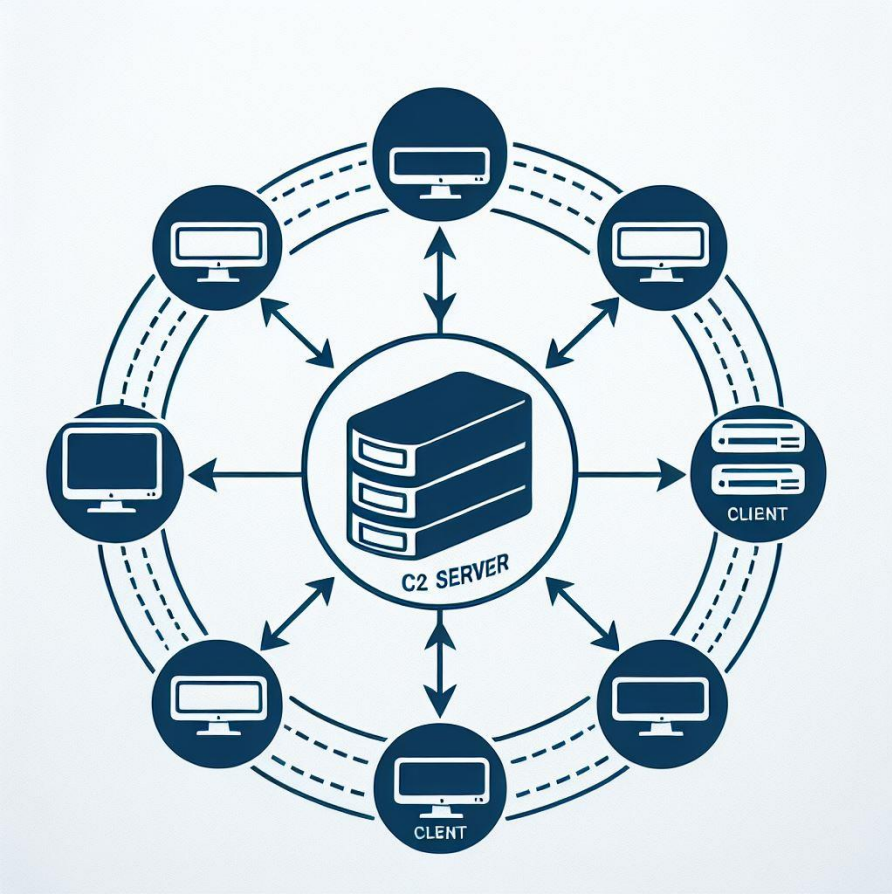
- Per falsificare la sua identità, il malware si installa sfruttando dei driver di sistema firmati digitalmente da due aziende verificate: Realtek e JMicron, passando quindi inosservate a livello di sistema operativo

- I driver riportano la data di firma del 25 Gennaio 2010, uno dei due è stato compilato il 1 Gennaio 2009 mentre il secondo pochi minuti prima della firma digitale.

- La vulnerabilità non sembra essere mai stata individuata, VirusBlokAda, il 12 Giugno 2010, pubblica tutte le informazioni tecniche e rilascia le firme per il proprio motore di rilevamento per bloccare il comportamento malevolo, inoltre comunica a Microsoft la vulnerabilità Zero Day per le patch dei sistemi operativi.

- Tutti i produttori di sistemi di sicurezza si mobilitarono. Il 16 Giugno 2010 venne creata una squadra ad hoc di Symantec, trovarono che il malware andava a creare delle librerie .DLL e interagiva con Windows API per risultare un processo autorizzato di Windows in caso di scansione anti-virus

La fase C&C



- Una volta installato, il malware andava a contattare due server C&C mascherati come siti sportivi mypremierfutbal.com e todaysfutbol.com ubicati in Danimarca e Malesia, registrati con nomi e carte di credito false.

- La connessione, criptata, comunicava diverse informazioni riguardo il target infettato:
  - Indirizzo IP interno ed esterno
  - Versione del sistema operativo Windows
  - Presenza di software Siemens installato

- Senza software Siemens installato, il malware si disattivava tentando di eliminare le proprie tracce

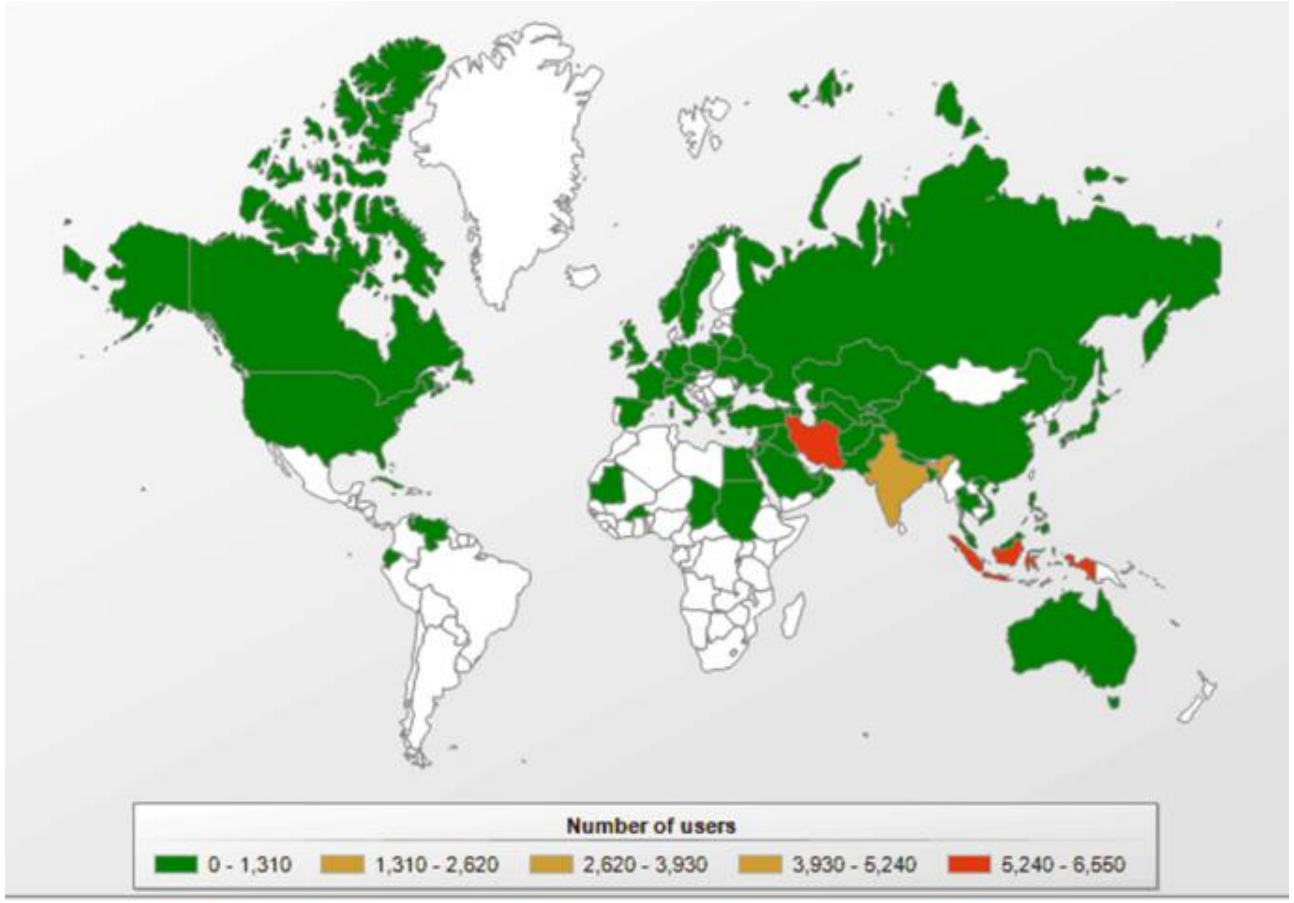
Analisi delle infezioni a livello mondiale

- Symantec contattò i provider DNS per creare un reindirizzamento dei siti C&C verso un sinkhole e quindi analizzare le connessioni in entrata per tracciare la diffusione delle infezioni

- In una settimana di monitoraggio:
  - 38.000 infezioni, 9.000 nuove al giorno, provenienti da dozzine di stati
  - 22.000 in Iran, 6.700 in Indonesia, 3.700 in India, 400 in USA

- DI queste solo alcune con software Siemens installato:
  - 217 in Iran
  - 16 in USA

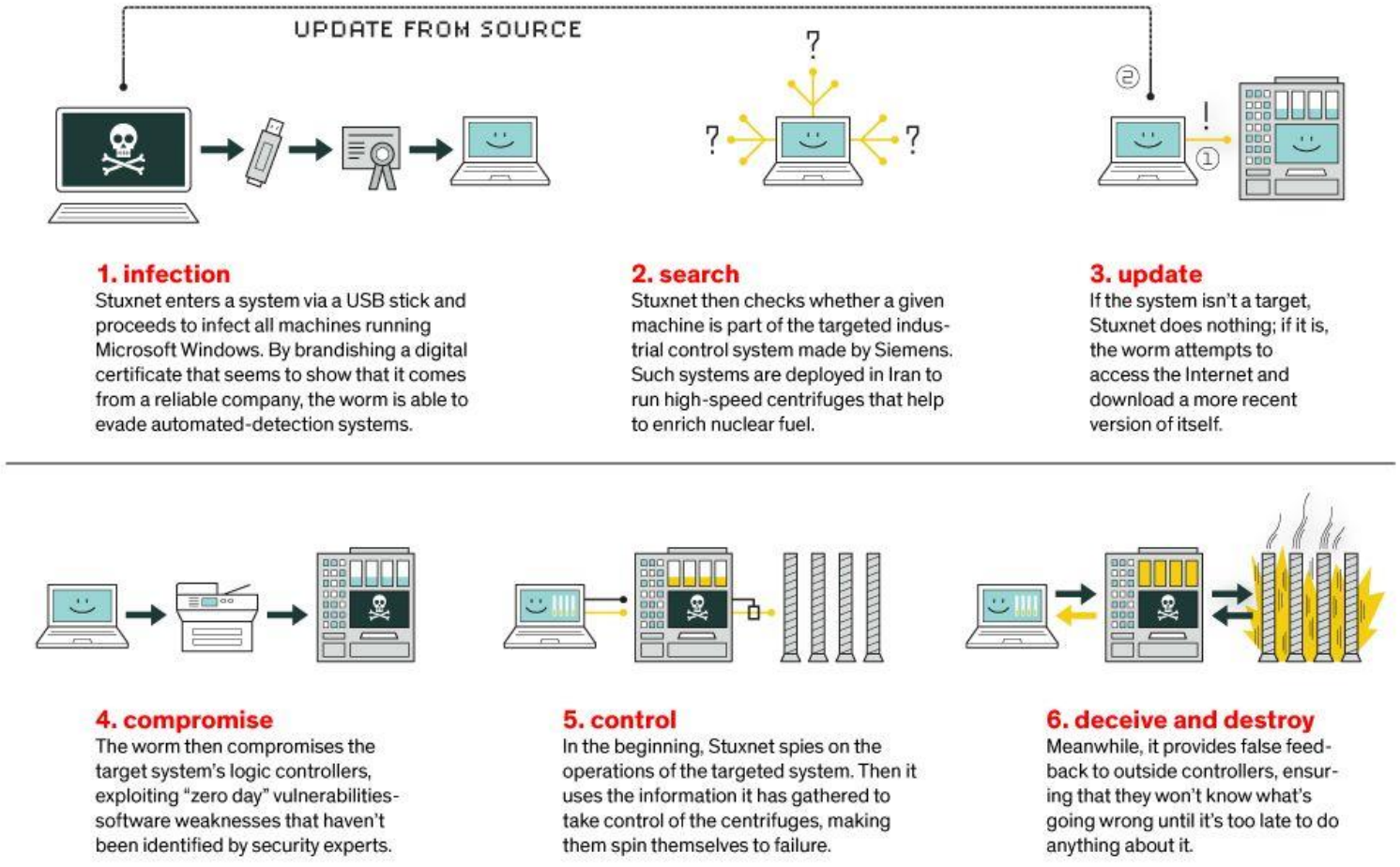
Chi c'era dietro gli attacchi? Competenze alte nella compilazione del virus, richieste specifiche, certificati rubati, aree geografiche ben identificabili.



Reverse Engineering

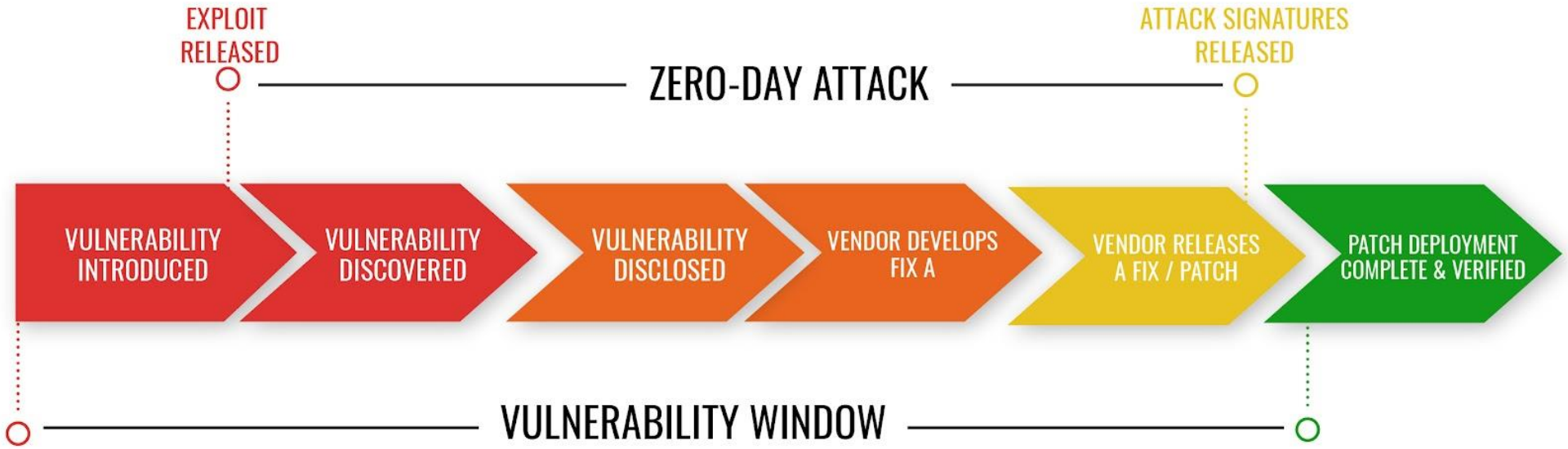
- Il team di ricerca divenne globale e tutti i maggiori brand di Cyber Security iniziarono a verificare il codice

- Il Malware è composto di 4 diversi moduli
  - Dropper: Infetta il sistema e si autoestrae
  - Rootkit: Nasconde la sua presenza
  - Moduli PLC: Modifica dei protocolli industriali
  - Propagazione: Tramite USB e lateral movement



Zero Day Vulnerabilities

- CVE-2010-2568: Vulnerabilità nel driver di stampa di Windows.
- CVE-2010-2732: Vulnerabilità nel servizio di Windows Server.
- CVE-2010-2743: Vulnerabilità nel servizio di gestione dei dispositivi.
- CVE-2010-2772: Vulnerabilità nel software di Siemens.



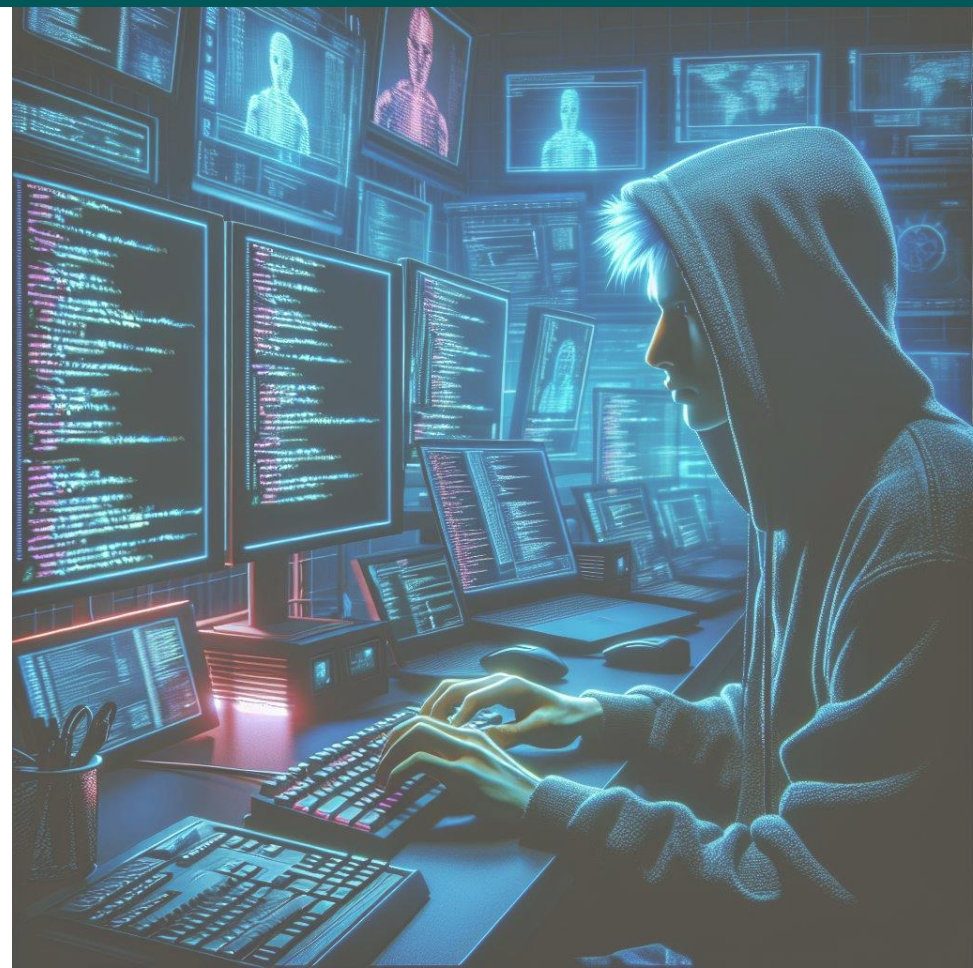
Il vero obiettivo

- Aziende fornitrici di sistemi industriali iraniani
- Pc con software Siemens Step-7 e i file di progetto .s7p
- PLC S7-300 e S7-400 Siemens
- Invio di codice ai controller industriali simulando letture corrette dell’attività delle centrifughe
- Sistemi Airgapped

Funzionamento del codice

Il codice è programmato per avere diversi cicli di funzionamento:

- 13 giorni di Reconnaissance delle normali attività dei PLC
- Lettura di 1.1 Milioni di operazioni
- Due ore di countdown
- 15 minuti di modifica delle attività sulle centrifughe da 1064 Hz a 1410 Hz
- Ritorno alla normalità
- 26 giorni di Reconnaissance e lettura del doppio delle operazioni
- Nuovo countdown
- 50 minuti di modifiche sulle centrifughe da 1064 Hz a 2 Hz
- Ritorno alla normalità
- Ripartenza del ciclo



I progetti paralleli

Duqu

Nel 2011, CrySyS lab in Ungheria, intercettano una campagna di Phishing contenente un malware con le stesse caratteristiche di Stuxnet.
Con Reverse Engineering risalgono all'anno di creazione, il 2007.
Il malware contiene Keylogger.
Sembra essere un'operazione di spionaggio.
Attacco ad obiettivi mirati in ambito militare.

Flame

Nel 2012 un altro rilevamento ha scosso il mondo della cyber security, il malware Flame è stato scoperto dai ricercatori Kaspersky, rivelandosi un malware a vasta scala per ottenere informazioni sui pc target tramite una rete di server di Command and Control. Si troveranno le informazioni di una cooperazione tra NSA, CIA e Esercito Israeliano risalente al 2007.
Grande diffusione in Iran.

Stuxnet 0.5

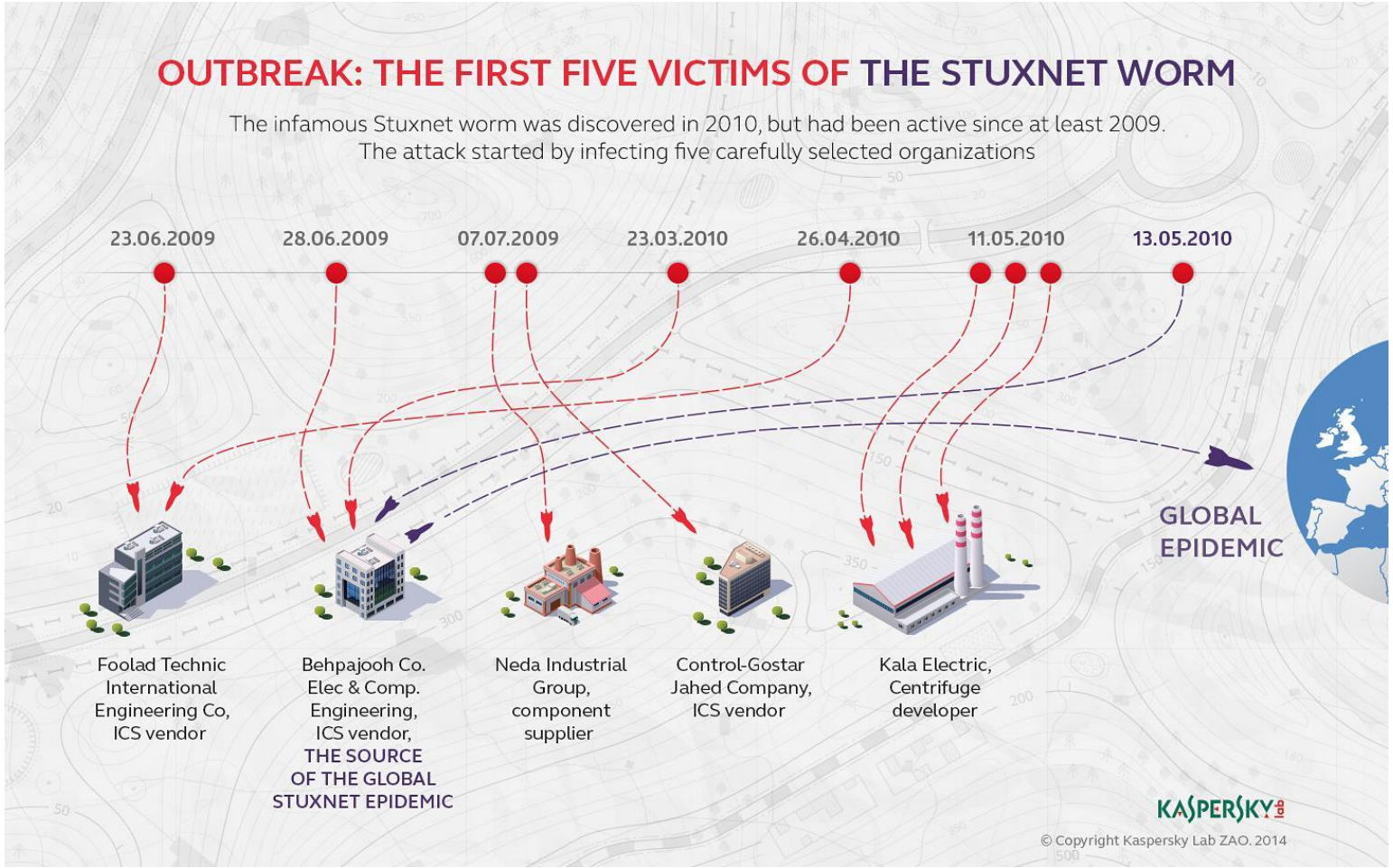
Stuxnet 0.5, caricato sul portale Virus Total il 15/11/2007, è il primo rilevamento del virus, differentemente da quelli successivi andava a modificare pressione del gas nelle centrifughe. Si pensa che sia stato abbandonato perché poco efficiente. Non attaccava i PLC ma solo i file di configurazione Step7.

Il progetto Olympic Games

Operazione approvata da George W. Bush nel 2006 e continuata sotto l'amministrazione Obama per colpire la centrale di Natanz con un'arma cyber.

Successivi lanci di campagne di protezione da cyber warfare con stanziamenti ingenti da parte degli stati

Timeline in grafica



TD SYNNEX

“You couldn't bomb a plant you didn't know about, but you could possibly cyberbomb it”

Kim Zetter

https://www.limesonline.com/rivista/storia-del-nucleare-iraniano-16174207/
https://maps.google.com
https://spectrum.ieee.org/the-real-story-of-stuxnet
https://mixmode.ai/blog/zero-day-attack-strategy/
https://www.cve.org/
https://link.springer.com/article/10.1007/s10708-023-10929-z
https://www.giorgiosbaraglia.it/la-guerra-cibernetica-caso-piu-famoso/
https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en
https://securityanddefence.pl/Operation-Olympic-Games-nCyber-sabotage.html
https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet
https://www.kaspersky.it/blog/stuxnet-le-sue-prime-vittime/5266/
https://www.anti-virus.by/

Zetter Kim, Countdown to Zero Day, Broadway Books, 2014

Q&A

PROSSIMI APPUNTAMENTI

21 MARZO: Stuxnet e gli attacchi iOT
28 MARZO: Il rapporto Clusit 2025
4 APRILE: Cisco Security

https://events.tdsynnex.it/cyber-unit-missione-protezione/

TEAM SECURITY: security.it@tdsynnex.com
SPEAKER: andrea.pezzoni@tdsynnex.com