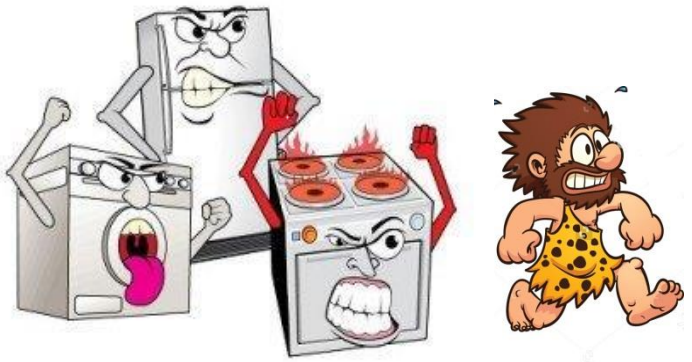
Vita poco segreta e molto pericolosa degli oggetti

Alessandro Curioni

Ieri - Oggi - Domani

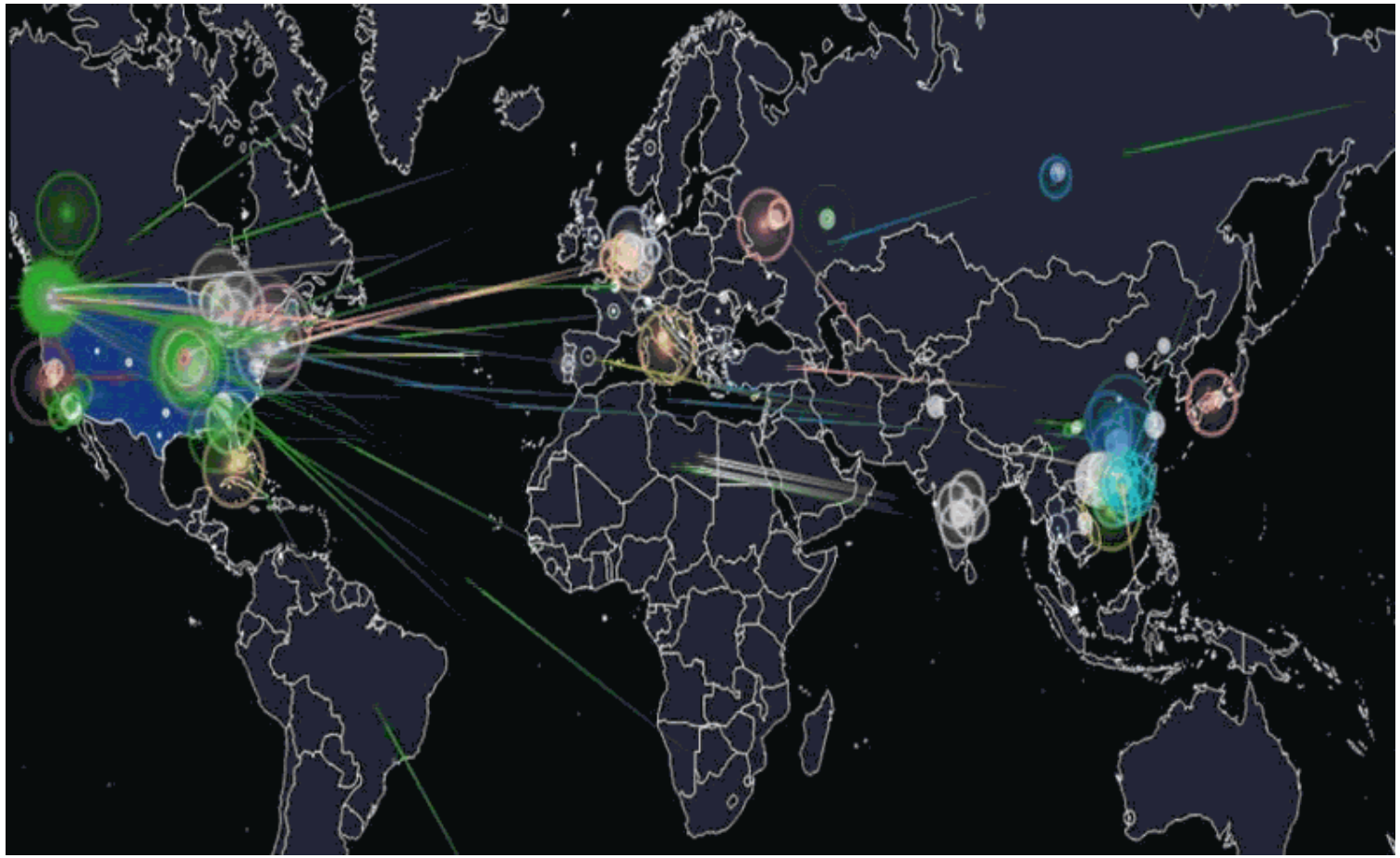


In sintesi: ogni mattina ti svegli e… Comincia a correre

Internet of Hacked Things

Il 21 ottobre 2016 si è verificato il più violento attacco DDOS della storia di Internet. Per un giorno intero Dyn (società responsabile del DNS americano) è stato bersagliato da miliardi di dispositivi compromessi, causandone di fatto il sovraccarico… **Qual è stata la novità di questo attacco?**

Il vettore dell'attacco sono stati miliardi di **dispositivi IoT** (Ip camera, Baby monitor, router di casa etc) compromessi dal malware **Mirai.**



Internet della piccole cose

Defcon 2015

66 diverse vulnerabilità scoperte in
28 dispositivi prodotti da
18 aziende diverse

Defcon 2016

47 diverse vulnerabilità scoperte in
23 dispositivi prodotti da
21 aziende diverse

Defcon 2017

?? diverse vulnerabilità scoperte in
?? dispositivi prodotti da
?? aziende diverse

Internet delle grandi cose

Aprile 2016

Ramnit e Conficker a Gundremmingen

Giugno 2017

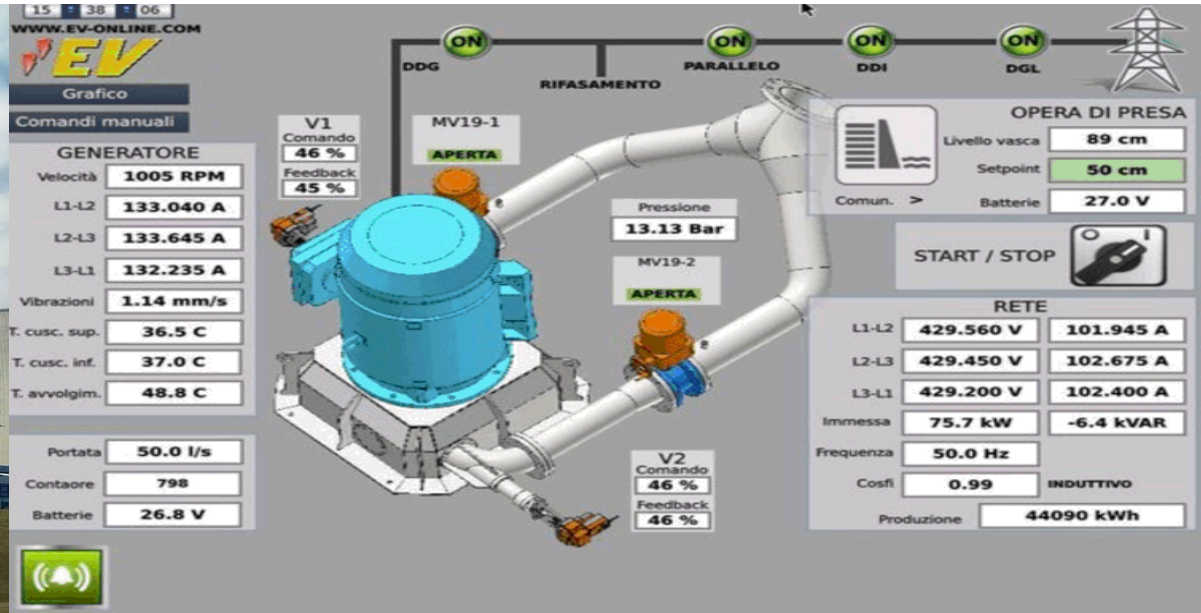
NoPetya a Chernobyl

Luglio 2017

Energetic Bear a Wolf Creek

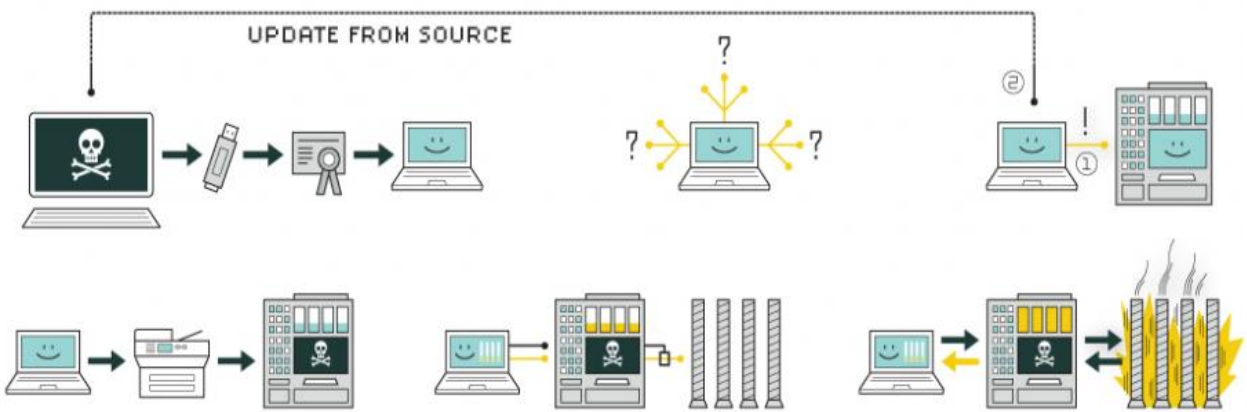
SCADA exposed

piccoli e grandi incubi

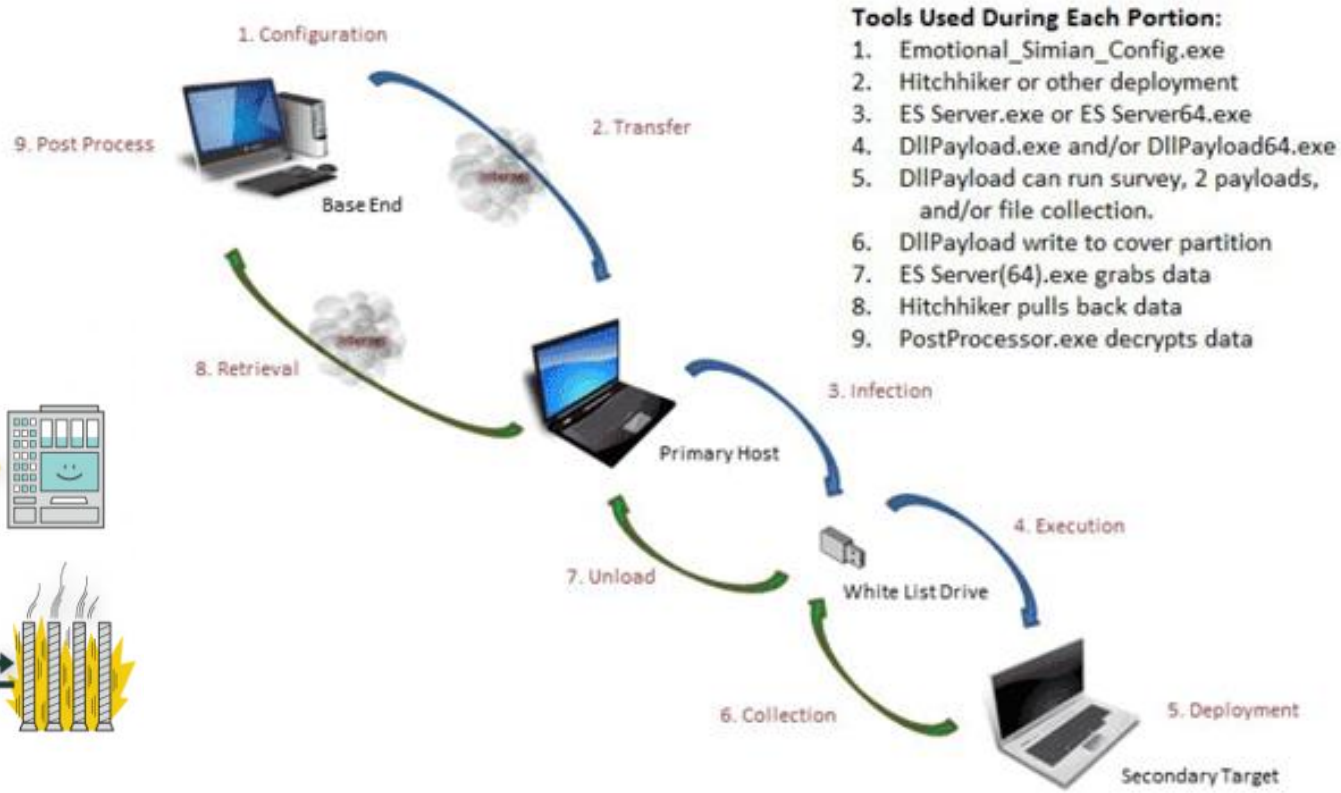


Da Stuxnet a Brutal Kangaroo – attacco alle «airgapped»

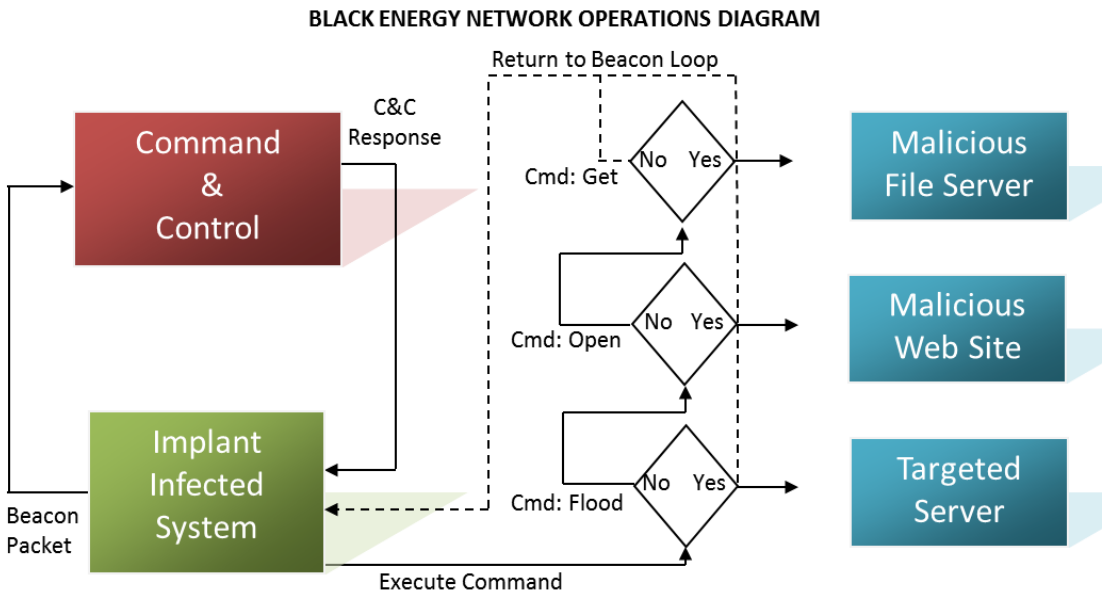
Stuxnet (dal 2009 a oggi)
Attacco a Windows
Attacco a WinCC Step 7 Siemens
Attacco alle PLC
Punti di forza: 4 vulnerabilità «zero day», certificati autentici per aggredire il kernel Win, componente worm, il rootkit che lo nascondeva



Brutal Kangaroo (dal 2016 a oggi)
Non un malware, ma un generator.
Drifting Deadline: il risultato su USB
Punti di forza: sfrutta il limite delle airgapped



Da Black Energy a Industroyer – evoluzione della specie

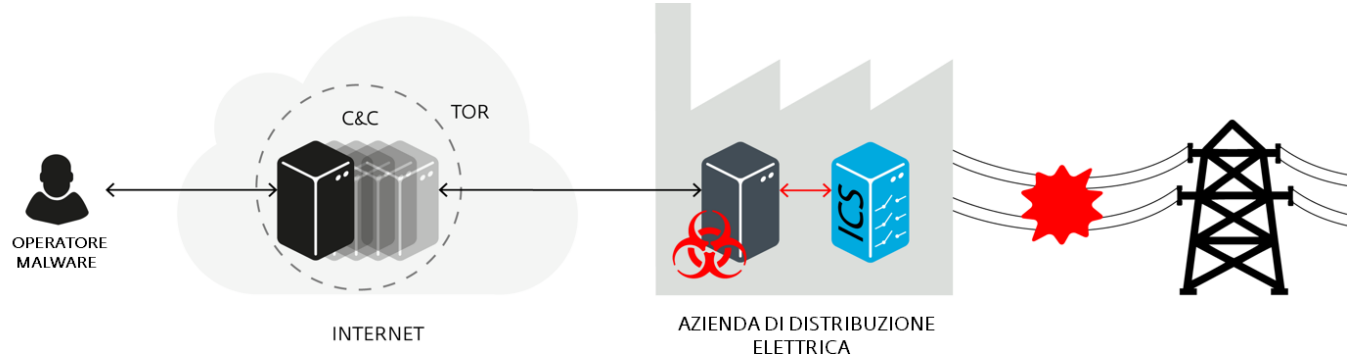


Industroyer Dal 2016 a oggi

Una backdoor (con backup nascosto in notepad)
Settaggio orario di operatività
Usato a dicembre 2016 con centrali ucraine
Dotato di port-scanner proprietario
DDoS per SiProtec
Payload per ICS personalizzabile
Dialoga direttamente con gli switch delle sotto stazioni elettriche
Tecniche di infiltrazione: spear phishing, watering hole, USB.

Black Energy Dal 2007 a oggi

Un trojan multifunzione
KillDisk il payload usato dicembre 2015 con centrali ucraine.
Tecniche di infiltrazione: spear phishing, watering hole, USB.



Visioni dal futuro

Compatibilità retroattiva e downgrade (rollback) attack

Garanzia dell'interoperabilità e comunicazione tra sistemi di diverse generazioni (un must per i sistemi SCADA ICS)
Indurre un sistema a «ridurre» il proprio livello di sicurezza per comunicare con un sistema più vecchio
Scoperto in OpenSSL con degrado della comunicazione TLS alla versione SSL 3.0. Il caso FREAK -- Factoring Attack on RSA-EXPORT Keys. Una vulnerabilità deliberata

Mega Botnet

Nuove generazione di malware per colpire IoT (dopo Mirai e Hajime) = Botnet più grandi e affidabili

ISO/IEC 15408 Evaluation criteria for IT security part 1-2-3

Certificazione di sicurezza di prodotto
Cosa (obiettivi di sicurezza)
Dove (ambiente di sicurezza)
Come (requisiti/verifiche di assurance).

Privacy e IoT

Il GDPR e il suo impatto su tutto ciò che è «smart»

Paura... Vero?

Alessandro Curioni