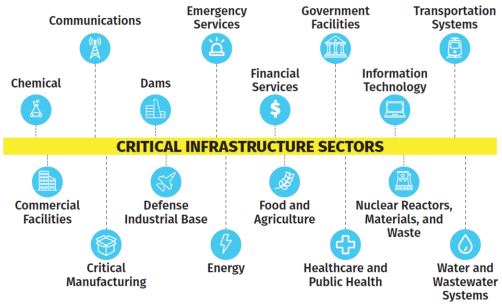
Cyber War

Le infrastrutture critiche sono quelle strutture, sistemi, siti, informazioni, persone, reti e **processi necessari al funzionamento del Paese e da cui, quindi, dipende la vita quotidiana.** Le infrastrutture critiche, comprendono anche alcune funzioni, siti e organizzazioni che non sono critici per il mantenimento dei servizi essenziali, ma che devono essere protetti a causa del potenziale pericolo per la popolazione (come per esempio: siti nucleati o siti chimici). Alcuni esempi di infrastrutture critiche sono riportati nella seguente immagine:



Da evidenziare il fatto, che per gli attacchi malware (che abbiamo visto nella prima parte del corso), il cui obiettivo era di attaccare ed infettare un sistema che fosse collegato ad una rete IT e le proprietà che volevamo garantire erano per lo più la riservatezza, l'integrità e la disponibilità. → invece, essendo che le infrastrutture critiche sono pensate per operare 24 ore su 24, gli attacchi a quest'ultime mirano principalmente (l'obiettivo primario degli attacchi) a compromettere la proprietà della disponibilità, in quanto tali strutture sono essenziali per il funzionamento del Paese. L'altra grande proprietà che si vuole preservare delle infrastrutture critiche è quella della safety, intesa come sicurezza, dato che essendo servizi essenziali alla nazione, avere un problema di sicurezza può compromettere anche la perdita di vite umane. Quindi, la cui perdita o compromissione degli elementi critici dell'infrastruttura (dove per elementi critici intendiamo: beni, strutture, sistemi o processi), potrebbe comportare:

- un grave impatto negativo sulla disponibilità, integrità ed erogazione dei servizi essenziali, compresi anche quei servizi la cui integrità, se compromessa, potrebbe comportare:
  - la perdita significativa di vite umane;
  - impatti economici e/o sociali significativi.

- impatti significativi sulla sicurezza nazionale, sulla difesa nazionale e sul funzionamento dello Stato.

Il cuore delle infrastrutture critiche è rappresentato dai **Sistemi di Controllo Industriale (ICS)**. All''interno di una infrastruttura critica vi sono molteplici processi automatizzati, di cui vogliamo garantire il funzionamento e l'operatività all'interno di determinati parametri → il compito dei ICS è di garantire, quindi, la continuità e l'operatività di tali processi automatizzati (detti anche **processi fisici**). Sorge, allora, spontanea la domanda: "Come fanno a garantire il loro funzionamento?"
Tipicamente ci sono dei parametri, che l'esecuzione di un processo deve rispettare (i cosiddetti **Set-points**) e i ICS garantiscono, che l'esecuzione del processo si mantenga sempre all'interno di tali Set-points → per riuscire a mantenere l'esecuzione del processi sempre all'interno di questi parametri, abbiamo che i ICS raccolgono e processano dati provenienti dai sensori, che sono associati ai vari dispositivi che implementano il processo fisico. Successivamente, i ICS vanno a confrontare i valori forniti da questi sensori con i Set-points ed ovviamente se:

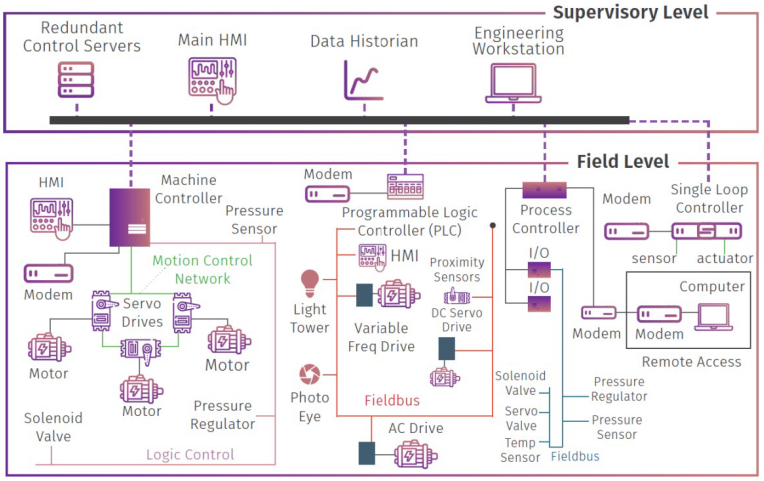
- il valore fornito dai sensori è più alto o più basso da quello dei Set-points, il ICS genera un comando (il quale poi viene eseguito), che va a far rientrare il valore nei Set-points;
- il valore fornito dai sensori è nei Set-points, allora va tutto bene.

Nella nostra vita quotidiana, troviamo i ICS praticamente ovunque. Basti pensare a:

▼ quando ci svegliamo, vi è un ICS che garantisce che arrivi la corrente a casa;

▼ vi è un ICS che garantisce che ci sia il gas a casa.

Le **principali componenti di un ICS** sono le seguenti:



- Nel livello più basso troviamo i cosiddetti **sensori attuatori**, i quali monitorano il funzionamento di dispositivi fisici (quali ad esempio: circuiti o valvole) e raccolgono dati sul loro funzionamento;
- Abbiamo, poi, il **Programmable Logic Controller (PLC)** → esso va a monitorare il corretto funzionamento dei dispositivi fisici. In particolar modo, il PLC funziona nel seguente modo:
  - processa i dati provenienti dai molteplici sensori attuatori;
  - esegue un programma, che stabilisce quale sarà la prossima azione che dovrà essere eseguita, in base ai dati forniti dai sensori;
  - genera dei comandi → per esempio, se il PLC sta monitorando una pompa dell'acqua, all'interno di un sistema di distribuzione dell'acqua, e il livello dell'acqua è troppo basso, il PLC può decidere di generare un comando per rialzare il livello dell'acqua nel sistema di distribuzione.
- I PLC vengono programmati attraverso le cosiddette **Engineering Workstation** → esse vengono generalmente utilizzate da degli operatori e la loro particolarità è che sono totalmente sconnesse (scollegate) da Internet e vengono utilizzate per implementare il codice, che deve essere eseguito dal PLC;
- Un'altra componente fondamentale degli ICS sono le **Human Machine Interfaces (HMI)** → esse raccolgono dati relativi a tutti i processi fisici monitorati dai vari PLC, che fanno parte del ICS e di conseguenza, le HMI forniscono agli operatori una visione di come stanno operando i vari processi e possono eventualmente generare comandi, che possono essere inviati direttamente ai PLC.

Una volta, **la sicurezza di tali sistemi era basata sul fatto che erano Air-gap**, ovverosia che erano completamente sconnessi da Internet. Esisteva, quindi, solamente una rete LAN che connetteva i componenti degli ICS (quindi i PLC, le HMI e i sensori attuatori). Al giorno d'oggi, però, le aziende (soprattutto quelle che operano nel settore energetico e dei trasporti) vogliono avere accesso ai dati generati all'interno del sistemi di controllo industriale, anche per garantire il monitoraggio e la manutenzione da remoto → per questi motivi, sempre di più, alcuni dei componenti dei sistemi di controllo industriale (ed in particolare i PLC e le HMI), sono esposte tramite Internet. Per proteggere tali componenti, quello che tipicamente viene fatto è di implementare un firewall tra la rete aziendale (che spesso ovviamente è collegata ad Internet e ai sistemi cloud aziendali) e la rete OT (Operational Network), ovverosia la rete che connette i dispositivi con i sistemi di controllo industriale.

Possiamo immediatamente capire, che se alcuni di questi dispositivi vengono esposti su Internet, stiamo creando una nuova superficie di attacco (nuova superficie, perchè prima non esisteva, dato che i sistemi erano isolati dalla rete Internet) → c'è anche da sottolineare il fatto, che **questi dispositivi e i protocolli di comunicazione tra dispositivi, sono progettati senza alcun livello di sicurezza**. Essi sono progettati senza alcun livello di sicurezza per molteplici motivi, tra cui:

- la necessità di re-implementare completamente la Stack di tutti i dispositivi;
- i dispositivi sono obsoleti. Per esempio, una Workstation ha un ciclo di vita di circa 20 anni.

Quello che spesso viene fatto dagli attaccanti, quindi, che hanno come obiettivo quello di compromettere e/o sabotare un'infrastruttura critica è di andare a:

- ricercare un qualche componente esposto su Internet;
- analizzare le vulnerabilità dei componenti;
- sfruttare tali vulnerabilità per ottenere l'accesso iniziale all'OT.

In particolare, i componenti più vulnerabili e che quindi vengono presi di mira dagli attaccanti, come iniziale punto d'accesso all'infrastruttura critica sono:

- Tra gli OT Devices (Operation Technologies Devices), ovverosia i dispositivi all'interno di un sistema di controllo industriale, troviamo:
  - PLC;
  - Engineering Workstation;
  - Sistemi di automazione degli edifici (per esempio i sistemi di riscaldamento degli edifici o i sistemi di controllo di apertura e chiusura delle porte);
  - Remote Terminal Unit.
- Nei sistemi medici, invece, le componenti più vulnerabili sono:
  - Computer utilizzati dai medici → basti pensare al fatto, che tali computer hanno ancora come sistema operativo Windows XP;
  - Monitor dei pazienti;
  - Monitor della glicemia;
  - Sistemi di medicina nucleare.
- Come compenti vulnerabili troviamo i dispositivi IoT, in quanto molto spesso gli attaccanti non vanno ad ottenere l'accesso diretto alla rete OT, bensì prima

ottengono l’accesso alla rete dell’organizzazione che gestisce il sistema di controllo industriale dell’infrastruttura critica. In particolare, i dispositivi IoT più compromessi troviamo:

- Stampanti;
- IP camera;
- Network Attached Storage (NAS) → dispositivi che permettono di salvare e condividere i file in rete;
- Dispositivi VoiP.

“**Quali sono le vulnerabilità in comune tra questi sistemi, che possono essere sfruttate dagli attaccanti?**” Una prima vulnerabilità è certamente il fatto, che questi sistemi sono obsoleti (o tipicamente detti dispositivi di Legacy) → tali sistemi, quindi, non vengono mantenuti e i dispositivi hanno vecchi sistemi operativi, che quindi non sono più aggiornati e non presentano nuove patch di sicurezza e questo comporta, che le nuove vulnerabilità non verranno mai patchate → **questa prima problematica, in particolare, riguarda i dispositivi che compongono il sistema di controllo industriale**.

Un’altra grande problematica riguarda il fatto, che a differenza di un computer che utilizziamo quotidianamente, dove se vi è una nuova patch siamo in grado di applicarla immediatamente, questo non possiamo farlo con i dispostivi elencati precedentemente, dato che il ciclo di vita di tali dispositivi è di anni e quindi non si può tollerare un periodo di tempo, in cui il dispositivo non sia funzionante e operativo → l’aggiornamento del sistema operativo dei componenti di un sistema di controllo industriale deve essere pianificato con largo anticipo. Questo comporta, che la maggior parte dei dispositivi di controllo industriale sono vulnerabili a molteplici vulnerabilità.

Un altro problema nasce dal software eseguito dai dispositivi, in particolare dal **Software Development Kit**, il quale è utilizzato per programmare il codice. In alcuni dispositivi del sistema di controllo industriale ed in particolare, in alcuni Software Development Kit è presente il **Broa Web Server** → tutti gli ambienti di sviluppo, che utilizzato quest’ultimo Web Server, sono vulnerabili ad uno o più tentativi di compromissione. Per esempio, il Broa Web Server ha vulnerabilità ai processi di autorizzazione e autenticazione → gli attaccanti, quindi, stanno sempre di più utilizzando questo Server vulnerabile, per ottenere accesso all’SDK che è stata utilizzata per sviluppare il codice e dopo di che sfruttare le vulnerabilità presenti nell’SDK per compromettere il dispositivo.

Infine, un altro problema riguarda il fatto, che molti dispositivi utilizzano protocolli di monitoraggio e manutenzione da remoto (per evitare, che l'operatore debba effettuare la manutenzione in loco) e tra i protocolli maggiormente utilizzati troviamo SMB (il quale è vulnerabile a diversi exploit) e Remote Desktop Protocol (con il quale basta ottenere le credenziali di tale protocollo e si ha accesso al dispositivo) → inoltre, molti dei dispositivi del sistema di controllo industriale sono esposti su Internet.

> 💡 Una o più di queste vulnerabilità, quindi, vengono adottate dagli attaccanti per ottenere l'accesso iniziale all'OT del sistema di controllo industriale.

Sorge a questo punto spontanea una domanda: "**Quali sono tipicamente le fasi di un attacco ad un sistema di controllo industriale?**" Solitamente questi attacchi sono diversi rispetto a quelli che abbiamo visto precedentemente. Abbiamo visto, che la Cyber Kill Chain di un attacco tipico inizia con la fase di Reconnaissance e termina con l'installazione di un malware, il quale può compiere diverse azioni malevoli, come ad esempio cifrare i dati. Negli attacchi ai sistemi di controllo industriale, solitamente la prima fase dell'attacco serve principalmente ad acquisire conoscenza sul design del sistema di controllo stesso, in quanto per il successo dell'attacco è fondamentale per gli attacchi conoscere esattamente la configurazione del sistema del controllo industriale (quindi, gli attaccanti devono conoscere quali protocolli e modelli di PLC vengono utilizzati all'interno del sistema di controllo industriale, quali sistemi operativi sono installati sulle HMI) → questa conoscenza può essere acquisita solamente se si ottiene un accesso iniziale alla rete dell'organizzazione che gestisce l'infrastruttura critica oppure se si ottiene direttamente l'accesso alla rete OT del sistema di controllo industriale → solitamente, quindi, la prima fase degli attacchi è finalizzata ad acquisire l'accesso alla rete dell'organizzazione che gestisce l'infrastruttura critica, oppure l'accesso ai dispositivi che sono esposti su Internet (come per esempio un HMI o ad una Engineering Workstation), i quali poi possono dare accesso alla rete OT del sistema di controllo industriale → Questa prima fase prende il nome di **fase di Planning** e possiamo dire che sia equivalente alla fase di Reconnaissance degli attacchi tipici che abbiamo visto e quindi in questa fase, si tenta di raccogliere informazioni sui dipendenti dell'azienda che gestiscono l'infrastuttura critica, cercando di ottenere le loro credenziale (attraverso, ad esempio, attacchi di phishing), ed inoltre si cerca di vedere se vi sono dei dispositivi direttamente esposti su Internet che presentano

delle vulnerabilità (come per esempio: credenziali o password deboli, che possono utilizzare per ottenere l'accesso al dispositivo).

Nella fase successiva a quella di Planning, ovverosia nella fase di **Preparation** (che equivale alle fasi di Weaponization e Targeting di un attacco normale), andiamo a creare l'allegato malevolo per compiere l'attacco di phishing, che una volta aperto da un amministratore dell'infrastruttura critica, permette di installare un malware e di conseguenza permette all'attaccante di ottenere controllo persistente sulla macchina della vittima → nella fase di Preparation, quindi, vengono sviluppate due cose:

1. l'allegato malevolo;
2. il malware.

La terza fase, ovverosia la **fase di Cyber Intrusion**, punto sul fatto che le vittima aprano l'email di phishing e conseguentemente l'allegato, in modo da installare il malware sulla loro macchina. Il malware, poi, magari creerà un canale di C&C con gli attaccanti, tramite il quale (ovverosia il canale) il malware può ricevere altri comandi (come ad esempio: installare altri tool o elevare i privilegi) → **A questo punto ho terminato lo Stage 1**, perchè ho ottenuto l'accesso direttamente alla rete OT oppure alla rete dell'organizzazione e quindi, a questo punto, posso raccogliere ulteriori informazioni sul funzionamento del sistema di controllo industriale.

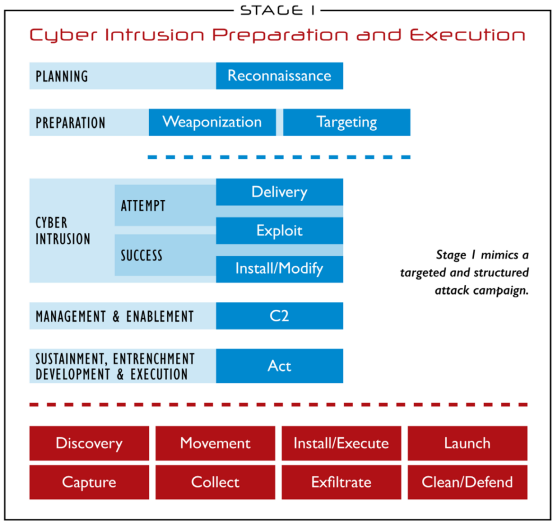
A questo punto, passo allo Stage 2 (quindi alla fase 2) dell'attacco, che è la fase più specifica dell'attacco al sistema di controllo industriale. Abbiamo detto, che questi attacchi per avere successo, hanno la necessità che gli attaccanti abbiano una conoscenza dettagliata del design del sistema di controllo industriale, che hanno acquisito nello Stage 1 (quindi nella prima fase). Lo Stage 2 si articola principalmente in tre fasi:

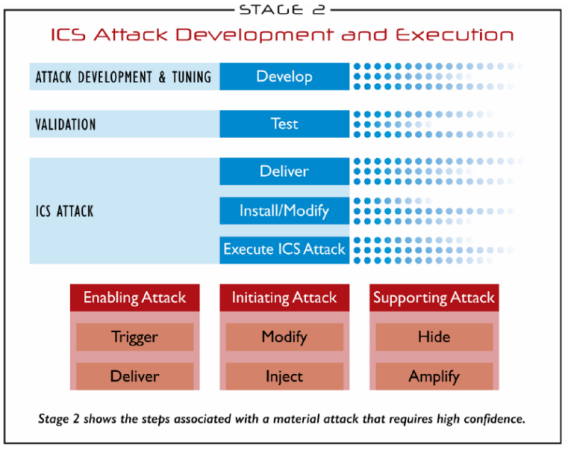
1. **Attack development & tuning** → in questa fase, gli attaccanti devono implementare gli strumenti per compromettere il sistema di controllo industriale. Naturalmente gli strumenti varieranno in base alla vulnerabilità presente nella Workstation che viene utilizzata per programmare il PLC di cui devo modificare il comportamento;
2. **Validation** → in questa fase, l'attaccante deve testare il proprio attacco e di conseguenza, va a ricreare la configurazione del PLC e della Engineering Workstation (l'attaccante, quindi, va fisicamente a comprare l'hardware per ricreare la configurazione del PLC e va a comprare lo stesso software della Workstation). In questa fase, quindi, gli attaccanti si assicurano che l'exploit che è stato sviluppato per sfruttare la vulnerabilità, funzioni effettivamente e quindi che riescano a modififcare il comportamento del PLC;

3. **ICS Attack** → in questa fase, l'attaccante deve effettivamente liberare ed eseguire l'exploit sulla Engineering Workstation.

> 💡 Quindi, possiamo affermare che gli attacchi ai sistemi di controllo industriale sono sempre multi stage.

Rivediamo le fasi dell'attacco ai sistemi di controllo industriale attraverso le seguenti immagini:





Cyber War

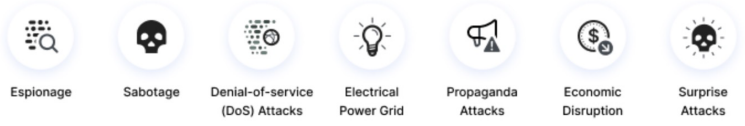
Sorge a questo punto una domanda: "**Quando gli attacchi alle infrastrutture critiche diventano attacchi di guerra verso altri Paesi?**" Un attacco informatico può essere considerato un attacco di guerra quando un gruppo affiliato ad un Governo va a condurre un attacco informatico, che va a compromettere la disponibilità di una o più infrastrutture critiche di un altro Paese, andando di conseguenza a creare dei danni paragonabili ad un normale attacco via terra → questo può essere fatto in concomitanza con una guerra in corso (come succede attualmente in Ucraina) oppure può trattarsi solamente di una guerra condotta tramite il cyber spazio.

Le principali tipologie di attacchi di Cyber War sono:

- **Spionaggio** → in questo caso, lo Stato attaccante utilizza tipicamente tattiche di ingegneria sociale, per ottenere l'accesso ad account di individui che lavorano in

ambito governativo, in modo tale da ricavare informazioni utili per condurre, ad esempio, altri attacchi nei confronti dell'altro Paese;

- **Sabotaggio** → comprende tutti questi attacchi, in cui si vanno a compromettere i servizi essenziali per i cittadini dello Stato colpito;
- **Attacchi di Denial-of-service (DoS Arracks)** → in cui sono presi di mira i siti governativi dello Stato colpito, in modo tale da compromettere l'accesa alle informazioni, per esempio, riguardanti la situazione politica e/o economica del Paese;
- **Electrical Power Grid** → comprendono tutti quegli attacchi alle infrastrutture critiche, i quali (ovverosia gli attacchi) operano nel settore energetico, quali ad esempio: centrali nucleari e centrali di produzione di energia elettrica;
- **Attacchi di propaganda** → attacchi che prevedono campagne di disinformazione o di fake news che sono condotti per discriminare (ovvero mettere in cattiva luca) il Paese attaccato alle altre nazioni e quindi prevenire che quest'ultime forniscano aiuto militare o umanitario al Paese attaccato oppure per discriminare il Paese attacco agli occhi dei propri cittadini, in modo da generare scioperi, rivolte e proteste;
- **Economic Disruption** → attacchi non molto diffusi, ma sono attacchi che impediscono ai cittadini e al Paese stesso di accedere ai servizi economici;
- **Attacchi a sorpresa (Surprise Attacks)** → attacchi non annunciati (ricordiamo, ad esempio, l'attacco di Pearl Harbor).



Il primo attacco, che può essere considerato un attacco di Cyber War contro un'altra Nazione è stato **Stuxnet** → si pensa che Stuxnet sia stato creato dalla U.S. National Security Agency in collaborazione con i Servizi Segreti Israeliani, per contrastare la campagna di generazione di armi nucleari iniziata dall'Iran. Stuxnet aveva come obiettivo i PLC, che erano responsabili dell'arricchimento dell'uranio (componente fondamentale per realizzare le armi nucleari) ed in particolare, aveva come obiettivo una delle centrali per l'arricchimento dell'uranio situata a Natarz (ovverosia una delle principali centrali iraniane). "**Come funzionava Stuxnet?**" Innanzitutto, dobbiamo

pensare che la rete all'interno della centrale nucleare di Natarz era completamente isolata da Internet, quindi si pensa che:

- o ci sia stato un operatore, che durante l'attività di manutenzione, abbia collegato il proprio PC infettato da Stuxnet alla rete interna della centrale;
- oppure qualche agente israeliano si sia mascherato da operatore e abbia introdotto, tramite una chiavetta USB, Stuxnet all'interno della centrale.

Una volta che Stuxnet infettava un computer, sfruttava diverse vulnerabilità per propagarsi ad altri computer presenti sulla rete della centrale e sui computer Windows che eseguivano un determinato software (chiamato Step 7), Stuxnet andava a modificare tale programma eseguito dal PLC, andando ad aumentale la velocità delle turbine che arricchivano l'uranio, oppure ne comportava il funzionamento → per capire la configurazione esatta del sistema, sono state utilizzate delle immagini dei video pubblicati dai telegiornali locali. Per propagarsi, Stuxnet sfruttava due vulnerabilità, che sfruttavano la connessione di rete:

1. una vulnerabilità legata allo spooler della stampante;
2. l'altra legata alla propagazione tramite chiavetta USB infetta, che sfrutta il file autorun.inf.

Inoltre, quando trovava una connessione Internet, Stuxnet cercava di scaricare da due C&C Server una versione aggiornata di se stesso ed una volta aggiornato (e anche se non era aggiornato) andava a modificare il codice del PLC nel seguente modo: abbiamo detto che l'obiettivo erano delle macchine che eseguivano il software Step 7. Quest'ultimo (ovvero Step 7) andava a modificare il codice eseguito da un PLC utilizzando una dll specifica, la quale permetteva ad un progetto Step 7 di leggere il codice eseguito dal PLC, modificarlo e caricare una nuova versione del codice → alla fine, l'effetto del codice modificato, era quello di modificare la velocità delle turbine oppure modificare la pressione registrata dalle turbine.

Attacchi russi contro l'Ucraina

Nel dicembre del 2015, vi sono stati una serie di black-out che hanno interessato la regione intorno a Kiev in Ucraina, dove per circa 3 ore i cittadini non hanno avuto alcuna fonte di energia elettrica. L'attacco russo aveva preso di mira le stazioni di distribuzione dell'energia elettrica sfruttano diverse vulnerabilità → l'attacco non ha avuto un impatto notevole sulla vita dei cittadini, ma ha destato preoccupazione per quello che ha comportato l'attacco in se, ovvero **ha dimostrato che si poteva**

attaccare un’infrastruttura critica di un altro Paese e causare potenzialmente danni notevoli. L’attacco è stato reso possibile grazie a:

- una campagna di spearphishing iniziata mesi prima contro alcuni dipendenti delle stazioni di distribuzione dell’energia elettrica, che aveva un allegato malevolo, che quando veniva aperto dalle vittime andava a scaricare il malware;
- questa campagna aveva come obiettivo quello di deliberare un malware chiamato Black energy, il quale ha permesso di rubare le credenziali di accesso, tramite VPN, alla rete OT delle varie stazioni di distribuzione dell’energia → in particolare, il malware andava a creare un canale di C&C con gli attaccanti, attraverso il quale gli attaccanti potevano installare altri tool sulle macchine degli operatori;
- è stato utilizzato anche un altro viper, il quale ha compromesso le macchine degli operatori che lavoravano nelle stazioni;
- gli attaccanti hanno, inoltre, organizzato un attacco di Denial-of-Service verso i Call-center dei fornitori dell’energia elettrica, in modo tale da impedire ai cittadini di denunciare il black-out.

L’anno successivo, quindi nel 2016, si è verificato lo stesso scenario, ma questa volta sono stati utilizzati tool diversi → questa volta il black-out è stato causato da un’altra tipologia di malware, chiamato Industroyer, che è uno dei primi malware progettati per attaccare specificatamente sistemi di controllo industriale → possiamo affermare ciò, in quanto Industroyer implementava 4 dei protocolli, che venivano utilizzati dalle HMI per comunicare con i circuiti per l’accensione e la trasmissione della corrente elettrica → si tratta di un malware modulare, dove la principale componente è un Backdoor, la quale crea un canale di C&C con gli attaccanti. Per garantire consistenza, va ad installare un Backdoor aggiuntivo e poi lancia la componente vera e propria, ossia il Launcher, il quale compie due azioni:

1. esegue i 4 payload, ognuno dei quali implementa uno dei quattro protocolli di comunicazione che l’HMI utilizzano per comunicare con i circuiti di accensione e trasmissione della corrente;
2. installa un Data Wiper, il quale rende le Workstation inutilizzabili.

Il 27 giugno 2017 un importante attacco ransomware, di nome NotPetyaha, colpito diverse organizzazioni in tutto il mondo, tra cui:

- la banca centrale ucraina, le telecomunicazioni statali, la metropolitana comunale e l'aeroporto di Kiev;

- la compagnia di navigazione danese Maersk;
- l'azienda farmaceutica statunitense Merck, un ospedale della zona di Pittsburgh e gli uffici statunitensi dello studio legale DLA Piper.

→ gli attaccanti hanno sfruttato il fatto, che le organizzazioni ucraine utilizzassero un software di dichiarazione dei redditi ed in particolare hanno sfruttato l’aggiornamento periodico di questo software.

> 💡 Si pensa che tutti questi attacchi fossero preparatori all’attacco dell’anno scorso, in cui la Russia ha deciso di invadere l’Ucraina.