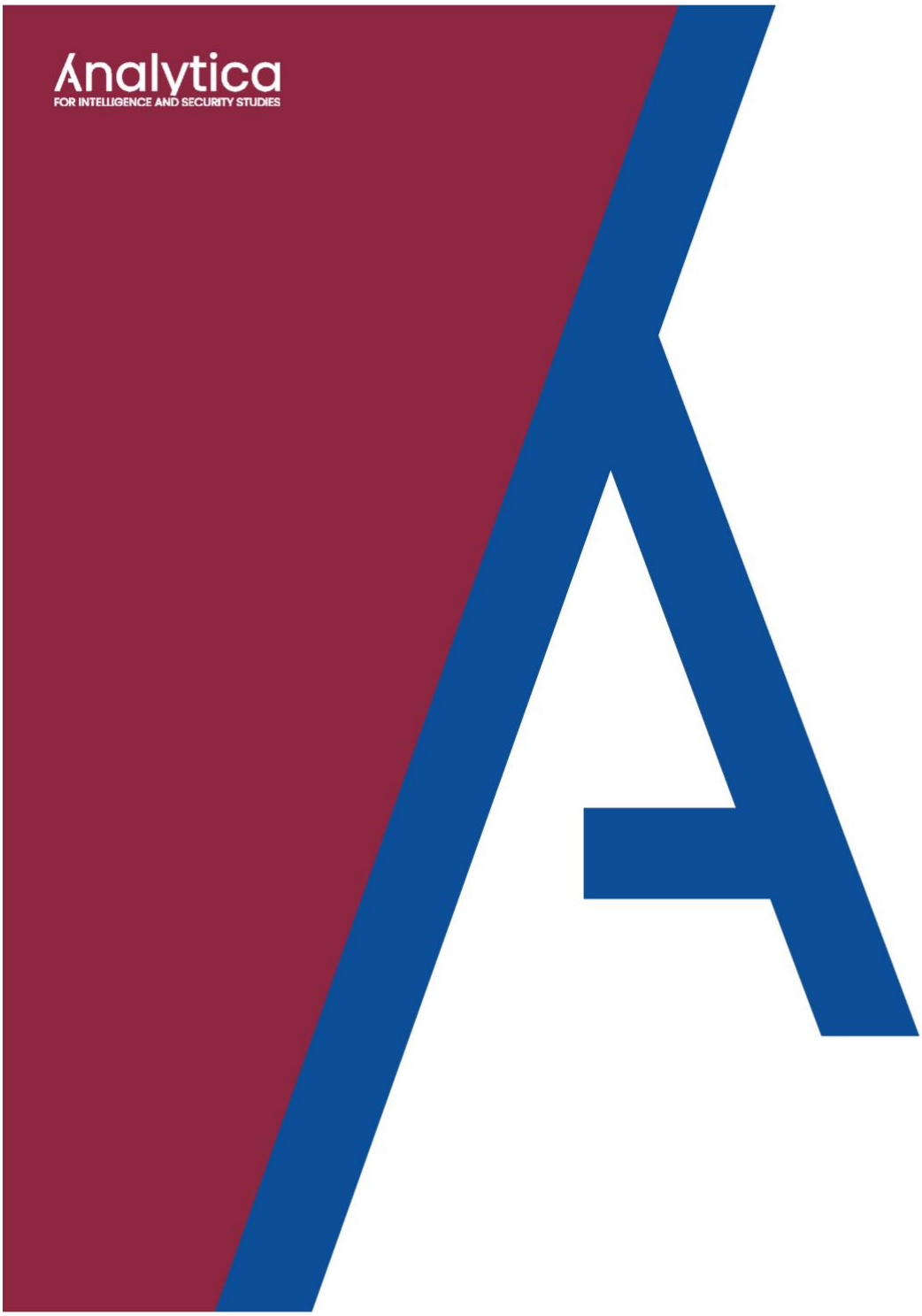

Analisi del caso BlackEnergy: tra geopolitica e cybersecurity.

Chiariello Franscesco
Chiara Aveni – Simona Bova – Noemi Capelli – Alessandro Pigoni

Analytica for intelligence and security studies

Paper Cyber-Security

Analisi del caso BlackEnergy: tra geopolitica e cybersecurity.

Francesco Chiariello
Aveni – Bova – Capelli - Pigoni

Correzioni e revisioni a cura del Dottor SPELTA Maurizio

Direttore del Dipartimento Cyber - Security

Torino, giugno 2021

Alla base di questo breve studio vi è la volontà di analizzare nel dettaglio l'attacco cyber operato dal malware BlackEnergy 3 in Ucraina il 24 dicembre 2015. In particolar modo si porrà l'accento su questioni appartenenti a diversi filoni di analisi. In primo luogo, verrà analizzata l'origine geopolitica dell'attacco partito dalla Russia. L'apparente intento di privare l'Ucraina di un bene di prima necessità, quale l'energia elettrica, cela diverse motivazioni di chiara matrice geopolitica da collegarsi a storiche tendenze dimostrate dalla Russia stessa.

In secondo luogo, si passerà a una narrazione prettamente tecnica volta prima ad analizzare i sistemi SCADA/ICS, chiarendo per quale motivo sono considerati obiettivi sensibili, e successivamente verranno trattati gli effetti della convergenza IT/OT. Seguirà, poi, una dettagliata analisi dell'attacco informatico condotto ai danni della centrale elettrica ucraina, con un particolare focus rivolto all'evoluzione del malware BlackEnergy, protagonista di tale attacco. Le conclusioni, infine, porteranno a una breve trattazione della cybersicurezza in epoca Covid-19: come convergere la protezione di infrastrutture critiche con lo smart working.

1– L'Ucraina come scacchiere geopolitico: la crisi Russo-Ucraina

L'Ucraina e la Russia hanno avuto, nei secoli, uno sviluppo storico concomitante: la stessa Ucraina è stata parte prima della *Kievskaja Rus'*[1] e poi delle Repubbliche Sovietiche, fino all'indipendenza raggiunta nel 1991. Lo stesso termine Ucraina in slavo antico significa "confine": tale denominazione sottolinea la funzione del Paese come porta di collegamento tra l'Europa Occidentale e la Russia e come terreno di incontro e di scontro di interessi economici divergenti.

Al giorno d'oggi, l'Ucraina rappresenta una sorta di zona cuscinetto tra una NATO sempre più proiettata verso Est ed una Russia che si sente sempre più minacciata e sottoposta a un tentativo di accerchiamento. In questa chiave, la Rivoluzione Ucraina del febbraio 2014 in seguito ai fatti di Euromaidan è stata letta dall'osservatore russo come una delle azioni più gravi da parte dell'Occidente nell'ambito della NATO[2].

In questa visione, l'attacco informatico operato ai danni dell'Ucraina si inserirebbe all'interno di una storica costante nella geopolitica e nella politica estera della Russia. Se, infatti, analizzassimo la lunga linea della storia di questo Paese, sarebbe possibile individuarne una ferma e valida costante: la perpetua lotta per l'espansionismo[3].

---

[1] La Rus' di Kiev fu il primo Stato russo fondato intorno alla metà del IX secolo. Esso si estendeva su parte dell'attuale territorio ucraino, bielorusso e russo e aveva come capitale Kiev.

[2] Di Rienzo E., *Il conflitto russo-ucraino. Geopolitica del nuovo (dis)ordine mondiale*, Rubettino, 2015.

[3] K.S., *Russia's Perpetual Geopolitics. Putin Returns to the Historical Pattern*, in "*Foreign Affairs*" a.MMXVI vol.95 n.3, maggio/giugno 2016, pp.2-9.

Le radici dell'espansionismo russo sono da ricercare, dunque, nell'elemento geopolitico, caratterizzato dalla volontà di difendersi e di portare le frontiere occidentali il più lontano possibile. Fondamentale, inoltre, l'elemento psicologico: a causa delle continue invasioni, la Russia si è sentita spesso vulnerabile, nascondendosi dietro a uno scudo di aggressività difensiva[4].

La sicurezza è, senza dubbio, da annoverarsi come uno dei principali cardini delle scelte geopolitiche russe: tradizionalmente, essa è basata su attacchi preventivi e ancora oggi gli Stati più deboli situati ai suoi confini sono visti più come potenziali roccaforti che come alleati politici e militari.

La contemporanea Federazione Russia guidata dal suo storico leader Vladimir Vladimirovič Putin, si è ritirata, dal lato del fronte europeo, su confini che la fanno sentire in grande pericolo. Nonostante l'attuale momento storico sia caratterizzato dall'assenza di nemici interessati all'invasione dei territori della Federazione, dal punto di vista russo la percezione del pericolo resta comunque elevata: le stesse politiche della NATO verso l'Ucraina e il Caucaso lasciano un enorme senso di insicurezza negli animi dei russi.

Il neo-realismo di tipo aggressivo operato dalla politica estera di Putin è considerato come la reazione esplicita a una politica estera condotta, secondo la Russia, dalla NATO e dall'Unione Europea in aree strategiche dello spazio post-sovietico e, in particolare, dell'Ucraina[5]. La stessa destabilizzazione del Paese operata a partire dai fatti di Euromaidan, secondo Vladimir Putin, ha afflitto l'interesse vitale della Russia.

L'attacco cibernetico nei confronti della Kyivoblenergo, un'azienda regionale di distribuzione di energia elettrica situata nella regione Ucraina di Ivano-Frankivsk, è, dunque, da analizzarsi come fisiologica risposta russa a questa spirale di insicurezza. Un attacco volto, più che alla mera privazione di energia elettrica – un bene strettamente necessario, al mantenere l'area di crisi in una situazione di continua e inaspettata instabilità e a lanciare un importante messaggio agli osservatori occidentali attraverso l'esercizio di potere e forza, in questo caso anche tecnologica.

---

[4] *Ibidem*

[5] T.D., *Why Putin Took Crimea. The Gambler in the Kremlin*, in "*Foreign Affairs*" a. MMXVI vol.95 n.3 maggio/giugno 2016.

2- Sistemi SCADA/ICS

Perché sono obiettivi sensibili?

Gli ICS (*Industrial Control Systems*) sono sistemi di controllo industriale preposti alla gestione dei processi fisici in molti settori industriali e infrastrutturali, tra cui in primo piano spicca sicuramente quello energetico. Poiché svolgono un ruolo indispensabile e strategico nella sicurezza del Sistema-Paese, le infrastrutture energetiche, come quelle ospedaliere e dei trasporti sono definite infrastrutture critiche.

Il termine SCADA (*Supervisory Control And Data Acquisition*) si riferisce ad un sistema informatico impiegato nel monitoraggio e nel controllo elettronico dei sistemi industriali (ICS). Si tratta di un'applicazione che consente all'operatore di interfacciarsi con i processi mediante sistemi di controllo e ha due obiettivi principali:

1. monitoraggio, gestione e controllo a distanza del sistema fisico e dei processi in esecuzione;
2. acquisizione dei dati per supervisionare il corretto funzionamento del sistema e intervenire in caso di criticità[6].

Sintetizzando, ogni sistema SCADA si inserisce all'interno di una architettura così composta:

- uno o più computer interconnessi tra loro preposti alla supervisione e all'interfaccia uomo-macchina;
- una serie di unità periferiche che si interfacciano con il processo tramite sensori e attuatori;
- una rete di comunicazione che garantisce il corretto scambio di informazioni tra computer di supervisione e unità periferiche[7].

Ad oggi, i rischi di un attacco ai sistemi industriali sono concreti e reali poiché si tratta di obiettivi sensibili, data l'importanza dei processi in cui sono coinvolti e dell'impatto che un disservizio può causare sulla comunità, come indicato all'interno della Direttiva NIS, che introduce il concetto di Operatori di Servizi Essenziali[8], il quale racchiude in le infrastrutture critiche.

Originariamente, per le loro caratteristiche, i sistemi industriali erano immuni dalle minacce cyber poiché non erano dotati di un indirizzo IP e si avvalevano di protocolli proprietari. Infatti, il sistema SCADA nasce negli anni '50, prima della diffusione di Internet, dunque, questo sistema era isolato ed era controllato da PLC (*Programmable Logic Controller*) privi di connessione. Nel corso del tempo, i sistemi sono diventati sempre più complessi e sono stati connessi alla rete, ma spesso senza

---

[6] Pirozzi A., Visaggio C. e Giorgione F., *SCADA (In)Security: un'analisi approfondita sulla superficie di attacco del noto sistema di controllo industriale*, https://www.ictsecuritymagazine.com/articoli/scada-insecurity-unanalisi-approfondita-sulla-superficie-di-attacco-del-noto-sistema-di-controllo-industriale/ (consultato il 18 maggio 2021).

[7] Galloway B., Hancke G. P., *Introduction to Industrial Control Networks*, 2012.

[8] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio.

un adeguato e preciso progetto di sicurezza e difesa dalle minacce derivanti da reti interne e esterne. L'attuale processo di modernizzazione delle infrastrutture mette in luce un aspetto significativo per la sicurezza delle stesse: la convergenza tra *Information Technology* (IT) e *Operational Technology* (OT). Se da un lato, tale nuovo assetto massimizza la capacità operativa di queste strutture, dall'altro comporta una maggiore vulnerabilità delle reti industriali giacché inevitabilmente più esposte ad attacchi esterni, dato dall'aumento esponenziale del perimetro d'attacco causato dall'interconnessione dei dispositivi IT con le reti di processo su cui si attestano i sistemi OT.

Natura delle principali minacce

I principali attacchi a cui possono essere esposti questi sistemi rientrano in due macro categorie: i cybercriminali accedono al sistema attraverso reti esterne collegate che gestiscono le informazioni; oppure riescono a penetrare il sistema approfittando della distrazione di un dipendente (ad esempio, attraverso spear phishing) o direttamente sfruttando la complicità dello stesso. Citiamo brevemente i possibili attacchi, attualmente noti, su un sistema SCADA/ICS: *Malware, Exploit Kits, Advanced Persistent Threats (APTs), Insider Threat, Eavesdropping, Communication System network outage, (Distributed) Denial of Service* e *Data/Sensitive information leakage*[9].

Nel nostro caso analizzato, l'attacco ha avuto inizio nella centrale di distribuzione di energia elettrica di Kyivoblenergo in Ucraina il 24 dicembre 2015. L'attacco è stato perpetrato impiegando il *malware* denominato BlackEnergy 3, contenuto in e-mail dirette ai dipendenti dell'azienda. È stato rivolto inizialmente verso i sistemi SCADA di questo impianto per poi essere rapidamente indirizzato verso altre aziende, interrompendo in tal modo il servizio di erogazione di elettricità destinato a centinaia di migliaia di utenti.

Allo stato attuale, si rileva come l'approccio con cui si progettano e si gestiscono gli ICS sia rimasto di stampo prettamente industriale e scarsamente rivolto alla sicurezza informatica, come se questi impianti fossero in funzione in una realtà quasi estranea alle minacce cyber. Dunque, urge la necessità di adottare un atteggiamento diverso che integri la sicurezza dell'impianto industriale con quella della rete informatica.

[9] Mattioli R., *Enhancing infrastructure cybersecurity in Europe*, 2016.

3- Convergenza IT/OT

Con il termine *Operational Technology* (OT) si indicano l'hardware e il software impiegati per azionare le reti di controllo industriale (ICS), come SCADA.

All'origine IT e OT erano considerati separatamente, mentre negli ultimi anni è possibile assistere ad una forte convergenza di questi due sistemi. L'integrazione di funzionalità IT nei sistemi OT ha permesso ai differenti settori industriali di migliorare la produttività e l'efficienza in modo economicamente competitivo. Si rivela di fondamentale importanza la capacità del team OT di valutare e considerare quanto questa convergenza possa influenzare l'intero sistema IT e le infrastrutture critiche, avendo presente le possibili conseguenze di un attacco informatico sul Sistema-Paese. Interessante a questo proposito risulta il report elaborato da Fortinet sull'*Operational Technology* e cybersecurity[10]. Il report ha evidenziato delle rilevanti criticità nella protezione dell'OT da parte di attacchi informatici e ha sottolineato che le realtà OT non conferiscono la giusta priorità alla cybersecurity come parte fondamentale della loro strategia di convergenza IT e OT. La maggior parte delle aziende coinvolte nel monitoraggio, condotto da Fortinet, ha affermato che il team OT si occupa delle attrezzature critiche e della sicurezza informatica afferente a questo ambito, mentre, il team IT è responsabile delle attività svolte dal proprio reparto. Sono emerse notevoli difficoltà nell'individuare chi ha la responsabilità per quanto concerne le soluzioni di sicurezza informatica come i processi e i sistemi di controllo-automazione. Quasi la totalità degli intervistati ha asserito che la sicurezza delle attrezzature e dei macchinari deve essere una responsabilità condivisa tra IT e OT. Il principale limite che si rileva è rappresentato dalle diverse tecnologie su cui si basano i due sistemi. Questo significa che vi è una comprensione limitata delle tecnologie impiegate in entrambi i settori al di fuori delle persone che lavorano in questi ambienti. È fondamentale investire nella formazione dei membri del team OT su temi della cybersecurity affinché riescano a risolvere i frequenti problemi di incomprensione, cooperazione e visibilità con il team IT.

Come può un operatore dei servizi energetici difendere la struttura IT e OT della sua infrastruttura? Adottando l'approccio SOAR (*Security Orchestration, Automation and Response*), che si focalizza sul permettere il dialogo tra le tecnologie di sicurezza tra i diversi sistemi. Gli operatori di questo settore si trovano a doversi difendere da innumerevoli attacchi informatici con un carico di lavoro notevole e con una carenza di forza lavoro qualificata per rispondere agli incidenti[11].

---

[10] Fortinet, *2020 State of Operational Technology and Cybersecurity Report*, 2020.

[11] Forte D., *Security Orchestration, Automation and Response: i benefici del modello SOAR per la sicurezza aziendale*, https://www.cybersecurity360.it/soluzioni-aziendali/security-orchestration-automation-and-response-i-benefici-del-

Gli utenti del SOAR sono 3:

- *Security Operation Center* (SOC): centro operativo che si occupa della gestione, analisi, monitoraggio e difesa della sicurezza IT di un'azienda;
- *Computer Security Incident Response Team* (CSIRT): struttura che monitora, intercetta, analizza e risponde alle minacce cyber;
- *Managed Security Service Provider* (MSSP): fornitore di servizi di sicurezza per le aziende.

Dunque, il SOAR permette di ottimizzare le operazioni, unificare e orchestrare gli strumenti di sicurezza, poiché gode di una visibilità degli eventi e può per questo automatizzare le risposte. In particolare, il SOAR aiuta i SOC a diventare più orientati all'*intelligence*, poiché contribuisce a contestualizzare gli incidenti, prendere decisioni più informate e rispondere alle minacce in tempi brevi.

4- BlackEnergy: da malware DDoS a protagonista della crisi energetica in Ucraina

Questo paragrafo si occuperà di presentare l'evoluzione del malware BlackEnergy e la timeline dell'attacco cibernetico ai danni della rete elettrica ucraina avvenuto il 24 dicembre 2015. Apparso per la prima volta nel 2007, in occasione della sua vendita da parte del rinomato hacker Cr4sh, il malware BlackEnergy è stato soggetto ad uno sviluppo esponenziale che, in un decennio, lo ha portato a venire annoverato tra gli *Advanced Persistent Threat* (APT)[12]. In particolare, del malware BlackEnergy è possibile distinguere tre versioni, la cui ultima - BlackEnergy 3 - è stata protagonista dell'attacco informatico al centro di questo report.

L'evoluzione di BlackEnergy

Nella sua versione originale emersa nel 2007 – BlackEnergy 1 - consisteva in un malware dedito alla creazione di botnets http finalizzati a condurre attacchi di tipo DDoS. Le sue componenti principali erano un intuitivo builder, avente lo scopo di generare un eseguibile da diffondere attraverso campagne di phishing e diversi scripts, da eseguire sul lato server, attraverso cui sviluppare e gestire il sistema di comando e controllo (C2) dei bot distribuiti.

---

modello-soar-per-la-sicurezza-aziendale/, (consultato il 18 maggio 2021).

[12] Ferrazza F., *BlackEnergy, il malware per colpire i sistemi industriali: dettagli ed evoluzione*, https://www.cybersecurity360.it/nuove-minacce/blackenergy-il-malware-usato-per-colpire-i-sistemi-industriale-dettagli-ed-evoluzione/, (consultato il 18 maggio 2021).

Attraverso questa natura duale, i bot, gestiti da remoto, erano in grado di causare DDoS attraverso il comando '*flood*' (ICMP, SYN, TCP/UDP, HTTP), interromperlo attraverso '*stop*' e persino cancellarsi dal computer designato attraverso il comando '*die*'[13]. Una variante successiva del malware – BlackEnergy 2 – venne rilasciata a partire dal 2010. Rispetto al predecessore, la nuova versione vanta capacità di attacco superiori e una struttura interna modulare più complessa specializzata nell'attacco di sistemi ICS. Infatti, combinando stringhe di codice della prima versione con strumenti di cifratura dei contenuti più efficaci e con una componentistica trojan più avanzata, BlackEnergy 2 rappresenta, sotto tutti i punti di vista, un passo avanti significativo rispetto alla versione precedente[14]. Con l'avvento del 2014, venne alla luce la versione definitiva del malware. A differenza dei suoi predecessori, BlackEnergy 3, presenta una configurazione innovativa adottando un componente installer più intuitivo e sostituendo le funzionalità del modulo driver legacy con la distribuzione diretta del payload – come file DLL - in seguito all'esecuzione della macro[15]. In aggiunta al perfezionamento della potenzialità di disruption, la nuova configurazione permette al malware di aumentare la sua persistenza sui sistemi infettati. Infatti, attraverso l'offuscamento del contenuto della macro, la continua cifratura e decifratura del payload e la creazione di un file LNK nella cartella di esecuzione automatica del sistema infiltrato, BlackEnergy 3 ostacola una rapida individuazione da parte di antivirus e permette l'esecuzione diretta del payload ad ogni restart del sistema[16]. Avendo presentato brevemente l'evoluzione del malware BlackEnergy, con particolare focus dedicato alla componentistica della sua versione finale, questo report andrà ora ad analizzare l'utilizzo del suddetto all'interno dell'attacco informatico alla centrale energetica in Ucraina protagonista del nostro studio.

Disamina dell'attacco

L'attacco che ha messo in ginocchio per diverse ore la rete energetica regionale di Ivano-Frankivsk rappresenta un esempio lampante di un attacco cibernetico pianificato nei minimi dettagli e condotto in maniera esemplare. Infatti, da un'analisi approfondita delle fasi di hackeraggio delle infrastrutture IT e OT della centrale elettrica si può evincere la complessità dell'attacco e la

[13] Ferrazza F., *BlackEnergy, il malware per colpire i sistemi industriali: dettagli ed evoluzione*, https://www.cybersecurity360.it/nuove-minacce/blackenergy-il-malware-usato-per-colpire-i-sistemi-industriale-dettagli-ed-evoluzione/, (consultato il 20 maggio 2021).

[14] Stewart J., *BlackEnergy version 2 threat analysis*, https://www.secureworks.com/research/blackenergy2, (consultato il 20 maggio 2021).

[15] F-Secure, *BlackEnergy and Quedagh the convergence of crimeware and APT attacks*, 2019.

[16] Ferrazza F., *BlackEnergy, il malware per colpire i sistemi industriali: dettagli ed evoluzione*, https://www.cybersecurity360.it/nuove-minacce/blackenergy-il-malware-usato-per-colpire-i-sistemi-industriale-dettagli-ed-evoluzione/, (consultato il 18 maggio 2021).

minuziosità della sua preparazione. Al fine di presentare uno studio conciso, seppure dettagliato, dell'attacco, questo report introdurrà le fasi principali attraverso cui l'hacking è stato progettato e condotto. Le fasi antecedenti all'attacco sono state caratterizzate da una minuziosa attività di information gathering e reconnaissance attraverso cui i criminali hanno individuato il personale IT e gli amministratori di sistema impiegati in più aziende del settore energetico ucraino. L'attacco è stato condotto secondo lo schema riassuntivo qui presentato:

1. I target designati sono protagonisti di una campagna di spear phishing, ricevendo un'e-mail con allegato un file dannoso in formato XLS contenente VBA macro, attraverso cui impiantare BlackEnergy 3 all'interno dei computer[17]. Le e-mail sono state forgiate utilizzando falsi mittenti riconducibili a conosciuti partiti politici come 'Pravii Sektor' (Partito politico ucraino di estrema destra) o società di finanziamento al fine di nascondere l'intento fraudolento del documento contenuto[18]. Inoltre, la scelta di utilizzare un documento XLS come principale vettore di attacco è imputabile alla scelta dei potenziali target del gruppo criminale. Infatti, all'interno di un ambiente di lavoro interconnesso e multifunzionale, file XLS scambiati per e-mail non destano sospetti in impiegati manchevoli di risk awareness nei confronti delle tecniche comuni di phishing[19].
2. Una volta infettati i computer, i criminali hanno provveduto ad attuare un intensiva network discovery e mappatura delle reti al fine di intercettare le credenziali di accesso degli utenti e così connettersi alla VPN e ai sistemi ICS e SCADA. Questa fase ha richiesto grandi capacità di permanenza nella rete aziendale. Infatti, secondo alcuni studi condotti, la fase di network discovery e credential theft ha richiesto circa sei mesi di permanenza all'interno del sistema ed è stata condotta in largo anticipo rispetto alla messa in atto dell'attacco vero e proprio[20].
3. In seguito all'infiltrazione all'interno dei sistemi ICS e SCADA, i criminali hanno provveduto ad implementare un firmware malevolo nei dispositivi serial/ethernet collegati all'*Enterprise Content Management* (ECM). L'importanza strategica di questa fase è notevole. Infatti, il caricamento di questo firmware, ha impedito che le sottostazioni potessero essere riavviate da remoto, aumentando così il tempo necessario

[17] Cappelletti, F., *Russia, Ucraina, Cyber: il ruolo del dominio del cyber spazio nel confronto russo-ucraino*, 2018.
[18] Ferrazza F., *BlackEnergy, il malware per colpire i sistemi industriali: dettagli ed evoluzione*, https://www.cybersecurity360.it/nuove-minacce/blackenergy-il-malware-usato-per-colpire-i-sistemi-industriale-dettagli-ed-evoluzione/, (consultato il 18 maggio 2021).
[19] Cappelletti, F., *Russia, Ucraina, Cyber: il ruolo del dominio del cyber spazio nel confronto russo-ucraino*, 2018.
[20] *Ibidem*

al ripristino della funzionalità della rete energetica[21].

4. Apertura da remoto degli interruttori nel sistema SCADA e disattivazione infrastruttura IT[22].
5. Utilizzo del wiper KillDisk per cancellare i dati memorizzati all'interno delle unità terminali remote e campagna TDoS per rallentare il normale ripristino delle funzionalità del sistema energetico[23].

5 - Contromisure e prevenzione

In seguito all'attacco alla Kyivoblenergo, è diventata evidente la necessità di ridurre il rischio di attacchi informatici a infrastrutture critiche. In tal senso, l'analisi verterà sui sistemi di sicurezza sviluppati dagli Stati e da aziende private.

Sistemi statali

Gli Stati hanno iniziato a sviluppare un quadro di sicurezza informatica in grado di supportare le imprese nella difesa dagli attacchi informatici, soprattutto nei settori di importanza critica per il buon funzionamento nazionale, come le infrastrutture energetiche, dei trasporti o delle comunicazioni. Un valido esempio esistente è rappresentato dal NIST (National Institute of Standards and Technology) sviluppato da stakeholders delle infrastrutture del settore privato statunitense nel 2014, che pian piano sta crescendo fino a includere diverse organizzazioni a livello globale, tra cui Microsoft, Bank of England e Nippon Telegraph[24].

Il NIST è un framework di sicurezza non obbligatorio che integra un insieme di pratiche e modelli standard per la sicurezza informatica. Tali pratiche necessitano di essere adattate alle esigenze e alle peculiarità di ogni azienda. Il NIST prende in esame l'intera organizzazione aziendale, a partire dal dipartimento IT fino ad arrivare all'OT/ICS. Su modello del framework di sicurezza statunitense, nel 2015 è stato ideato il Framework Nazionale per la Cybersecurity e la Data Protection dallo stato italiano, frutto della collaborazione tra il mondo accademico, le imprese private e il settore pubblico.

---

[21] *Ibidem*
[22] *Ibidem*
[23] *Ibidem*
[24] NIST. *Questions and Answers*, https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics, (consultato il 19 maggio 2021).

Il NIST, nella pratica, definisce un punteggio di vulnerabilità attraverso il database CVE (*Common Vulnerability and Exposures*). Questo sistema garantisce alle aziende degli elementi aggiuntivi per catalogare i rischi e una comunicazione in codice durante le discussioni su vulnerabilità e rischi.[25]

Revisione dell'architettura di sicurezza SCADA

In seguito all'attacco del malware Stuxnet i problemi di sicurezza di SCADA hanno assunto una rilevanza primaria in funzione del loro ruolo strategico.

Se da un lato l'interconnessione dei sistemi SCADA garantisce un aumento della produttività, dall'altro espone i sistemi aziendali a un maggior rischio in caso di attacco informatico. Infatti, collegandosi ad altre reti, emergono nuove vulnerabilità che comprendono quelle di tipo hardware, come la poca memoria delle RTU, e software, ad esempio l'utilizzo di sistemi operativi in tempo reale (RTOS) che rendono i sistemi SCADA maggiormente esposti agli attacchi DoS (Denial of Service).

I professionisti della sicurezza dovrebbero riesaminare regolarmente l'architettura di rete ICS, inclusi i file di configurazione VPN, il posizionamento del firewall, il monitoraggio del traffico, ecc.

Risk Assessment

La sicurezza dei sistemi SCADA è intrinsecamente collegata alle strategie di analisi del rischio.

Spesso le aziende approcciano il problema della sicurezza informatica solamente dal punto di vista tecnico, non considerando che questo tipo di approccio esclude molti altri elementi coinvolti. Il focus sulla parte hardware tralascia elementi fondamentali come il fattore umano, molto spesso prima causa di attacchi informatici, le comunicazioni e i dati.

Per ovviare a questo problema ed effettuare un'analisi del rischio completa, è necessario individuare le aree aziendali. In questa prima fase bisogna studiare come le varie aree di lavoro interagiscono, quindi le relazioni tra il capitale umano, i workflow, gli asset e anche gli elementi che risiedono al di fuori del perimetro aziendale. Anzi, secondo Paul Calatayud, chief security officer di Palo Alto Network Americas il perimetro aziendale è un concetto non più applicabile alle aziende che, visto il nuovo livello di innovazione e di creazione di dati, si trovano a dover difendere una quantità prima inimmaginabile di dati.

[25] NIST. *NVD - Vulnerabilities*. https://nvd.nist.gov/vuln, (consultato il 20 maggio 2021).

In un momento storico in cui la vera ricchezza è rappresentata dai dati, le aziende devono adottare un "approccio dato-centrico", cioè focalizzandosi sulla protezione dei dati piuttosto che dei sistemi. Inoltre, secondo la letteratura recente, un approccio rivoluzionario in materia di sicurezza aziendale sarebbe il cosiddetto *Security by Design*. In accordo a questa metodologia, la protezione dei sistemi hardware e software deve essere posta al centro sin dalla loro ideazione cercando di prevedere le potenziali vulnerabilità derivanti dalla loro implementazione.

6 - Conclusioni

L'educazione alla cyber sicurezza nel periodo del COVID-19

Come analizzato precedentemente, nel caso di infrastrutture critiche la sicurezza complessiva dei sistemi hardware/software è fondamentale. Questa necessità è diventata una priorità con l'inizio della pandemia di Covid-19, che ha generato un repentino cambio delle modalità di lavoro. Lo spostamento da una dimensione di lavoro in ufficio allo smart working, ha colto alla sprovvista la maggior parte delle aziende e i loro dipendenti con un notevole aumento dei rischi derivanti da attacchi informatici ai danni degli propri asset.

Nella buona riuscita dell'attacco BlackEnergy, condotto nei confronti della centrale elettrica ucraina, il fattore umano è stato fondamentale. Questa criticità è particolarmente osservabile nell'attuale contingenza storica. Molto spesso, i dipendenti usano i propri device elettronici e la loro rete di casa, che frequentemente mancano di sistemi di sicurezza adeguati. Per risolvere i problemi di sicurezza, le aziende dovrebbero imporre delle misure preventive, come l'utilizzo di VPN, che garantiscano la confidenzialità necessaria alle aziende per estendere pratiche di sicurezza anche ai lavoratori in remoto. In aggiunta a ciò, l'utilizzo di *multi-factor authentication* (MFA) per accedere alla rete aziendale sta diventando la nuova normalità.

Tuttavia, anche i lavoratori in smart working dovrebbero osservare qualche accortezza, come ad esempio assicurarsi che i device aziendali non vengano utilizzati da altri membri della famiglia, inserire un blocco schermo, o effettuare il logout da questi a fine giornata lavorativa.

In particolare, gli hacker, attraverso la struttura aziendale pubblicata online da tutte le organizzazioni, sono in grado di selezionare dei target specifici per le e-mail di phishing attraverso cui spedire dei malware per attaccare le aziende. Specialmente nell'era dei social media, i criminali informatici hanno sviluppato diversi metodologie per individuare i loro bersagli e strutturare accuratamente le e-mail da inviare. Gli utenti dei social non sempre rispettano le buone pratiche per la protezione della privacy, a volte condividendo eccessive informazioni. Inoltre, attraverso lo

studio dei cookies, gli hacker possono risalire alle ultime azioni online della carta di credito, o visualizzare gli ultimi siti visitati. Secondo uno studio di F-Secure[26], la mail di spam sono la maniera più usata per la diffusione di malware, spesso nascosti in file zippati. Le e-mail di phishing hanno avuto un tasso di successo del 30% o maggiore in questo ultimo anno, con un aumento del 600% nel primo quadrimestre del 2020[27]. È quindi necessario che gli utenti utilizzino la massima cautela. Secondo uno studio condotto dal governo bretone, nel 2020 solamente l'11% delle aziende nazionali conducevano regolarmente dei corsi di formazione alla sicurezza informatica per i dipendenti[28].

Dalla nostra breve, e non esaustiva, analisi, si evince che al fine di garantire la cybersecurity in epoca Covid-19 è necessario da un lato garantire una regolare formazione dei dipendenti sulle *best practice* da adottare online e dall'altro attuare strategie di protezione aziendale che siano in grado di far fronte alle minacce legate all'attuale contingenza storica.

[26]Sattler J., *COVID-19 scams — how to spot and stop coronavirus email attacks*, https://blog.f-secure.com/re-covid-19-scams-how-to-spotand-stop-coronavirus-email-attacks/, (consultato il 18 maggio 2021).

[27]Sjouwerman S., *Q1 2020 coronavirus-related phishing email attacks are up 600%*, https://blog.knowbe4.com/q1-2020-coronavirus-relatedphishing-email-attacks-are-up-600, (consultato il 18 maggio 2021).

[28] Pedley D., Borges T., Bollen A., et al. *Cyber security skills in the UK labour market 2020*–Findings report. Department for Digital, Culture, Media and Sport. 2020, https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cybersecurity-skills-in-the-uk-labour-market-2020 (consultato il 19 maggio 2021).

Bibliografia

Cappelletti, F., *Russia, Ucraina, Cyber: il ruolo del dominio del cyber spazio nel confronto russo-ucraino*, 2018.

Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio.

Di Rienzo E., *Il conflitto russo-ucraino. Geopolitica del nuovo (dis)ordine mondiale*, Rubettino, 2015.

Fortinet, *2020 State of Operational Technology and Cybersecurity Report*, 2020.

F-Secure, *BlackEnergy and Quedagh the convergence of crimeware and APT attacks*, 2019.

Galloway B., Hancke G. P., *Introduction to Industrial Control Networks*, 2012.

K.S., *Russia's Perpetual Geopolitics. Putin Returns to the Historical Pattern*, in "*Foreign Affairs*" a.MMXVI vol.95 n.3, maggio/giugno 2016.

Mattioli R., *Enhancing infrastructure cybersecurity in Europe*, 2016.

T.D., *Why Putin Took Crimea. The Gambler in the Kremlin*, in "*Foreign Affairs*" a. MMXVI vol.95 n.3 maggio/giugno 2016.

Sitografia

Ferrazza F., *BlackEnergy, il malware per colpire i sistemi industriali: dettagli ed evoluzione*, https://www.cybersecurity360.it/nuove-minacce/blackenergy-il-malware-usato-per-colpire-i-sistemi-industriale-dettagli-ed-evoluzione/, (consultato il 18 maggio 2021).

Forte D., *Security Orchestration, Automation and Response: i benefici del modello SOAR per la sicurezza aziendale*, https://www.cybersecurity360.it/soluzioni-aziendali/security-orchestration-automation-and-response-i-benefici-del-modello-soar-per-la-sicurezza-aziendale/, (consultato il 18 maggio 2021).

NIST. *Questions and Answers*, https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics, (consultato il 19 maggio 2021).

NIST. *NVD - Vulnerabilities*. https://nvd.nist.gov/vuln, (consultato il 20 maggio 2021).

Pirozzi A., Visaggio C. e Giorgione F., *SCADA (In)Security: un'analisi approfondita sulla superficie di attacco del noto sistema di controllo industriale*, https://www.ictsecuritymagazine.com/articoli/scada-insecurity-unanalisi-approfondita-sulla-superficie-di-attacco-del-noto-sistema-di-controllo-industriale/ (consultato il 18 maggio 2021).

Stewart J., *BlackEnergy version 2 threat analysis*, https://www.secureworks.com/research/blackenergy2, (consultato il 20 maggio 2021).