09-NOV-2026
da pag. 8 / foglio 1 / 3

La Verità
Quotidiano - Dir. Resp.: Maurizio Belpietro
Tiratura: 51920 Diffusione: 21261 Lettori: N.D. (Data Stampa 0006901)

DATA STAMPA
45° Anniversario

Data Stampa 6901-Data Stampa 6901

DIEGO MARSON

# «Gli attacchi ai frigoriferi potrebbero essere un test»

**Il manager di Yarix, azienda di cybersecurity: «Azioni replicabili in più Paesi perché i big della Gdo usano le stesse tecnologie. A rischio ospedali, reti idriche e traffico stradale»**

*Un hacker può usare pure un nostro elettrodomestico per colpire altri obiettivi Con gli allarmi via email si interrompe un servizio con un minimo sforzo*



di **LAURA DELLA PASQUA**

■ Frigoriferi che vanno in tilt mandando al macero tonnellate di cibo, voli presi di mira con minacce di bombe. Improvvisamente gli attacchi hacker si sono moltiplicati colpendo in maniera imprevedibile. Difficile decifrare la strategia che muove le fila di questa vera e propria guerra cibernetica e altrettanto oscura la matrice. Ma come difendersi? Abbiamo girato questa domanda a Diego Marson, chief security officer di Yarix (Var Group) azienda italiana specializzata in cybersecurity e digital security.

**Come è stato possibile far saltare il sistema di refrigerazione dei supermercati?**

«Non parliamo di normali frigoriferi domestici, ma di impianti di refrigerazione industriale gestiti da architetture Ot (Operational technology), cioè le tecnologie utilizzate per controllare e gestire macchinari e infrastrutture fisiche. Il funzionamento di questi impianti è regolato da centraline e dispositivi elettronici connessi a piattaforme di monitoraggio e gestione che permettono di controllarli anche a distanza. Per consentire il monitoraggio delle temperature e l'efficienza energetica, spesso questi impianti sono connessi a Internet attraverso reti di manutenzione da remoto di fornitori terzi. Si tratta di criticità già emerse in occasione dei primi incidenti registrati in Francia, dove sono state rilevate problematiche legate all'esposizione dei sistemi di controllo su Internet, all'obsolescenza di alcune installazioni e all'utilizzo di credenziali di accesso deboli. Anche in Italia sembra che siano state sfruttate vulnerabilità note e non corrette, interfacce di gestione accessibili dall'esterno senza opportuni livelli di autenticazione forte o nessuna separazione tra le reti aziendali, in modo da impedire che un problema in una di esse si propaghi alle altre. Una volta ottenuto l'accesso ai sistemi di controllo remoto, gli attaccanti hanno potuto agire direttamente sui parametri di funzionamento degli impianti, come quelli che regolano la temperatura, provocando un danno senza bisogno di sviluppare malware».

**E come possibile farlo contemporaneamente in più Paesi?**

«La spiegazione risiede nella standardizzazione della supply chain. Le grandi catene della Gdo o le organizzazioni con sedi distribuite utilizzano gli stessi fornitori di tecnologia, le stesse piattaforme di gestione cloud/IoT e i medesimi apparati hardware a livello internazionale. Se un attaccante individua un difetto sistemico o un'interfaccia esposta su una specifica piattaforma di telegestione usata su scala globale, l'attacco diventa replicabile. La diffusione delle stesse tecnologie presso più operatori rende particolarmente importante un approccio condiviso alla sicurezza: una vulnerabilità che interessa un apparato utilizzato su larga scala può esporre contemporaneamente realtà diverse, anche appartenenti a Paesi differenti».

**È un gruppo internazionale organizzato o piccole cellule che agiscono per emulazione?**

«In un contesto geopolitico teso, organizzazioni che agiscono con il sostegno o sotto la direzione di governi o attivisti informatici che utilizzano attacchi digitali per sostenere interessi politici o nazionali, utilizzano tecniche di cyber-sabotaggio a bassa intensità per testare la resilienza delle infrastrutture civili e generare instabilità. Una volta che il vettore di attacco o la configurazione vulnerabile vengono diffusi nei forum e canali frequentati dalla comunità del cybercrime, la tecnica viene replicata rapidamente da gruppi minori ("script kiddies" o gang cybercriminali). La combinazione tra la semplicità dell'exploit e l'elevato impatto mediatico/economico rende questo tipo di azioni estremamente attraente per una platea molto ampia. Un ulteriore elemento da considerare è il possibile ruolo dell'Intelligenza artificiale, che può facilitare l'individuazione di potenziali bersagli e automatizzare alcune attività ostili. Non ci sono tuttavia elementi per affermare che sia stata impiegata negli episodi in questione».

**Si è fatto un'idea sulle finalità?**

«Le finalità variano a seconda delle motivazioni e degli interessi che guidano gli hacker. Nel caso di operazioni riconducibili a una matrice geopolitica, una delle principali finalità è la guerra ibrida. Dimostrare che è possibile impattare la catena di approvvigionamento alimentare o la logistica di un Paese crea allarme sociale e mina la fiducia delle persone e dei mercati. Colpire servizi essenziali, come la distribuzione degli alimenti, può quindi diventare uno strumento di pressione e destabilizzazione anche senza ricorrere a un conflitto militare tradizionale. Una seconda finalità è provocare un dan-



ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1737 - T.1737

La Verità
Quotidiano - Dir. Resp.: Maurizio Belpietro
Tiratura: 51920 Diffusione: 21261 Lettori: N.D. (Data Stampa 0006901)

DATA STAMPA
45° Anniversario

no economico diretto: interrompere la catena del freddo significa costringere le aziende a gettare tonnellate di merci, causando perdite milionarie. In alcuni casi, si tratta di test: l'attaccante vuole misurare i tempi di risposta della difesa cibernetica per valutare come potrebbe reagire di fronte a crisi più ampie».

**I frigoriferi di casa possono essere manomessi a distanza?**

«Teoricamente, qualsiasi dispositivo "smart" o IoT connesso al wifi domestico ha una superficie d'attacco e presenta punti deboli che un hacker potrebbe sfruttare per accedervi. Tuttavia, il rischio e la finalità sono totalmente diversi da quelli di questo specifico caso. Compromettere un singolo frigorifero di casa richiede uno sforzo mirato che non offre alcun ritorno strategico a un attaccante. Il rischio reale a livello domestico è usare questi dispositivi come botnet, rendendolo parte di una rete di altri device informatici infettati e controllati da remoto dagli hacker, che li usano per sferrare attacchi informatici verso terzi».

**Quali altri sistemi rischiano?**

«Una vecchia battuta dice che un computer sicuro è un computer spento. La realtà è che qualsiasi servizio connesso a Internet comporta un rischio che va adeguatamente previsto e valutato. Nello specifico meritano particolare attenzione tutti i sistemi Ot (Operational Technology) e IoT industriali, ovvero le tecnologie connesse utilizzate per monitorare e controllare macchinari e infrastrutture fisiche».

**Quali sono questi sistemi?**

«Impianti Hvac (sistemi di riscaldamento, ventilazione e condizionamento dell'aria) in ospedali, data center ed edifici direzionali; piattaforme che regolano e controllano la distribuzione dell'acqua e il trattamento delle acque reflue; sistemi di gestione del traffico e segnaletica stradale; inverter fotovoltaici, colonnine di ricarica per veicoli elettrici e contatori intelligenti. La loro protezione richiede un coinvolgimento non soltanto dei responsabili It, ma anche di chi gestisce gli impianti, della direzione aziendale e dei fornitori esterni incaricati della manutenzione».

**C'è un modo per proteggersi e quanto costerebbe?**

«Sì, esiste un modo per proteggersi, ma richiede anzitutto un cambio di passo culturale. Non si tratta tanto di investire in software costosi, quanto di adottare un approccio corretto alla sicurezza e alla gestione del rischio. In concreto, questo significa innanzitutto superare la logica della "conformità cartacea"; rispettare normative europee come la Nis 2 Cyber Resilience Act, che introducono obblighi di sicurezza informatica e gestione del rischio; mappare tutti i dispositivi, i software e i sistemi presenti nell'organizzazione; verificare regolarmente la presenza di vulnerabilità più rischiose e intervenire rapidamente con aggiornamenti e correzioni di sicurezza; separare la rete It (aziendale) dalla rete Ot (gli impianti fisici) affinché i sistemi critici non siano raggiungibili direttamente da Internet; cambiare le credenziali e rafforzare la sicurezza degli accessi remoti. Adeguare l'infrastruttura ha un costo ampiamente inferiore al danno economico».

**Quindi meno siamo tecnologici e meno siamo vulnerabili?**

«Tornare indietro non è praticabile né auspicabile. La digitalizzazione è ciò che garantisce l'efficienza energetica, il tracciamento dei prodotti e la riduzione degli sprechi nella catena del freddo. Essere vulnerabili non è una conseguenza inevitabile dell'essere tecnologici, ma l'effetto dell'aver connesso apparati operativi a reti pubbliche senza la necessaria architettura di sicurezza. La risposta non è la rinuncia all'innovazione, ma la digitalizzazione consapevole».

**E i falsi allarmi bombe sugli aerei?**

«Al momento non esistono elementi che suggeriscano una matrice comune o un'unica regia tra la compromissione dei sistemi di refrigerazione e le minacce di bombe sui voli di linea in Europa. C'è un parallelismo che chi si occupa di cybersecurity nota: la somiglianza tra questi falsi allarmi bomba sugli aerei e le campagne di Denial of Service (DoS), comunemente condotte da hacktivisti. In entrambi i casi le azioni non mirano a distruggere il bersaglio, ma a interromperne temporaneamente il funzionamento per generare disservizi. Nel caso del trasporto aereo, un falso allarme può avere effetti concreti sulla continuità del servizio anche senza compromettere i sistemi informatici. Gli autori non hanno bisogno di violare sistemi avionici o varchi fisici aeroportuali: è sufficiente utilizzare canali di comunicazione standard, quali email anonimizzate, servizi VoIP flessibili o piattaforme di messaggistica, per segnalare una presunta minaccia. I protocolli di sicurezza previsti per la tutela della sicurezza dei passeggeri impongono di trattarla come potenzialmente reale fino alla smentita formale. Questo automatismo procedurale determina un'asimmetria operativa: chi genera l'allarme sostiene costi minimi e impiega strumenti facilmente accessibili, mentre il sistema di risposta composto da compagnie aeree, aeroporti e autorità è costretto a mobilitare risorse significative e a sostenere costi operativi, logistici ed economici dovuti all'applicazione dei protocolli. Dal punto di vista della sicurezza, un aspetto centrale è quindi la capacità di analizzare e contestualizzare rapidamente le informazioni ricevute».

**È possibile individuare queste organizzazioni malavitose?**

«Il processo di identificazione dei responsabili di un attacco informatico è molto complesso poiché gli attaccanti utilizzano diversi sistemi per mascherare la propria identità e origine: server proxy, che permettono di nascondere l'indirizzo Ip di provenienza, reti cifrate (connessioni protette attraverso sistemi di crittografia) e assenza di confini fisici. Tuttavia, le agenzie di cybersecurity internazionali e le forze dell'ordine collaborano incrociando dati di intelligence, analisi forensi ed analisi del traffico di rete. Mentre l'individuazione e la risposta giudiziaria richiedono tempo, la vera chiave rimane la prevenzione».

© RIPRODUZIONE RISERVATA

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1737 - T.1737

LaVerità
Quotidiano - Dir. Resp.: Maurizio Belpietro
Tiratura: 51920 Diffusione: 21261 Lettori: N.D. (Data Stampa 0006901)

DATA STAMPA
45° Anniversario



**ESPERTO** Diego Marson, chief security officer di Yarix [Imagoeconomica]

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1737 - T.1737