REPORT

Report Fortinet: Tendenze nella sicurezza delle tecnologie operative 2019

Un aggiornamento sul panorama delle minacce per i sistemi ICS e SCADA

Sommario

Sintesi preliminare

Nelle organizzazioni è in corso una trasformazione verso una maggiore agilità, in risposta alla rapida evoluzione del mercato. In questo contesto, molti sistemi OT (Operational Technology) vengono collegati per la prima volta al mondo esterno. Questa tendenza promette importanti vantaggi per le organizzazioni, ma espone anche i sistemi OT a minacce avanzate persistenti. La separazione dal sistemi IT, che proteggeva i sistemi OT dagli hacker e dal malware, non esiste più in molte organizzazioni, e gli aggressori, di conseguenza, stanno prendendo sempre più di mira i sistemi OT.

Il report 2019 Operational Technology Security Trend di Fortinet analizza i dati aggregati dei FortiGuard Labs per raccogliere informazioni sullo stato della sicurezza dei sistemi SCADA (Supervisory Control And Data Acquisition) e di altri sistemi di controllo industriale (Industrial Control System, ICS). L'analisi rileva che i sistemi OT sono sempre più spesso bersaglio di attacchi basati sulle tecnologie dell'informazione (IT), spesso tipi di attacco legacy che non interessano più i sistemi IT, così come di attacchi concepiti specificamente per i sistemi OT. Logicamente, questi attacchi tendono a colpire le parti più deboli delle reti OT e sfruttano la complessità causata dalla mancanza di standardizzazione dei protocolli. Gli autori delle minacce non sembrano fare distinzioni di settore industriale o posizione geografica: ogni settore e ogni area hanno subito attacchi significativi.

Con l'aumentare delle connessioni dei sistemi OT, la tendenza all'aumento degli attacchi sembra destinata a continuare. Questa nuova esposizione richiede alle organizzazioni di adottare best practice di gestione del ciclo di vita e delle operazioni di sicurezza più rigorose, per proteggere le loro organizzazioni dalle principali minacce al cuore della loro attività. Di conseguenza, i team OT e IT devono fare fronte comune per rispondere in modo completo a minacce crescenti.

Infografica: risultati in evidenza

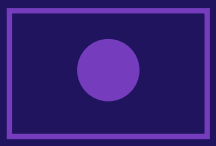
Gli exploit **sono aumentati in volume e prevalenza** nel 2018 per quasi tutti i fornitori ICS/SCADA.

Gli aggressori **riciclano regolarmente le minacce IT** per colpire i sistemi OT.

L'85%

delle minacce uniche rilevate ha colpito macchine con protocolli:
OPC Classic
BACnet
Modbus

Gli attacchi BACnet hanno raggiunto il picco **tra gennaio e aprile 2018**, in corrispondenza con la botnet Mirai.



La vulnerabilità **Moxa 313** si è concentrata particolarmente sul Giappone.

Introduzione

Storicamente isolati da "air gap", i sistemi OT sono ora sempre più connessi, a volte più di quanto ritengano i responsabili degli impianti e i tecnici dei controlli industriali. Secondo uno studio recente, quasi due terzi dei dispositivi OT sono connessi: il 32% direttamente a Internet e un altro 32% attraverso un gateway aziendale.[1] Questo gateway è a volte un elemento innocuo, ad esempio un singolo PC collegato separatamente sia al sistema OT che a Internet.

L'integrazione dei sistemi IT e OT è una decisione aziendale sensata per molte organizzazioni, con vantaggi quali:

- **Monitoraggio più efficace ed efficiente dei processi**, con la possibilità di apportare cambiamenti importanti in modo immediato
- **Possibilità di utilizzare i dati dei dispositivi IoT** per informare i processi decisionali, con l'aggiunta di un livello molto dettagliato di informazioni su clienti, prodotti e processi
- **Accesso a dati di mercato in tempo reale** per una tempistica ottimale di consegna dei prodotti e un'interazione più efficiente con la catena di fornitura
- **Risparmi significativi sui costi** grazie al controllo dei consumi energetici, alla riduzione degli sprechi di materie prime e a una migliore efficienza dei dipendenti

L'integrazione dei sistemi OT solleva problemi di sicurezza.

Nonostante questi evidenti vantaggi, l'eliminazione dell'"air gap" che separava i sistemi OT da quelli IT espone i primi agli stessi rischi per la sicurezza che impattano i secondi e rende più facile la diffusione di exploit specifici per i sistemi OT. A complicare il problema, i sistemi ICS e SCADA hanno storicamente funzionato con cicli di aggiornamento e sostituzione molto più lunghi rispetto ai sistemi IT, il che significa che molti sistemi tecnologici ormai datati sono ora esposti per la prima volta alle attuali minacce avanzate persistenti. Un'altra sfida è costituita dalla mancanza di visibilità: l'82% degli intervistati in un sondaggio ha ammesso di non essere in grado di identificare tutti i dispositivi collegati alle proprie reti OT e IT.[2]

In molte organizzazioni, queste sfide hanno portato a un tasso inaccettabilmente elevato di incidenti di sicurezza. In un recente sondaggio condotto tra organizzazioni leader del settore OT, il 77% degli intervistati ha dichiarato di aver subito un'intrusione di malware nell'ultimo anno e la metà di questi ne ha subite da tre a 10.[3] La natura di queste intrusioni è preoccupante: gli intervistati riferiscono eventi con un impatto sulla produttività (43%), sui ricavi (36%), sull'immagine del marchio (30%), su perdite di dati (28%) e persino sulla sicurezza fisica (23%).

La sicurezza OT comporta un rischio significativo.

Gli aggressori hanno infatti molti incentivi ad attaccare i sistemi ICS e SCADA. I criminali possono richiedere un riscatto dopo aver bloccato le operazioni di una fabbrica, disabilitato un sistema di accesso tramite badge o preso il controllo di una parte di un'infrastruttura critica. Entità concorrenti (spesso nazioni-stati che agiscono per conto di imprese di proprietà dello stato) possono infiltrarsi nei sistemi a scopo di spionaggio industriale. E gli aggressori con scopi politici possono colpire le organizzazioni percepite come ostacoli ai loro obiettivi, seminando caos e disordine.

I responsabili della sicurezza dei sistemi OT si trovano ad affrontare sfide significative quando i sistemi vengono connessi:

- **Superficie di attacco ampliata** a causa dell'eliminazione dell'"air gap"
- **Sistemi legacy** con caratteristiche di sicurezza progettate per un'infrastruttura non connessa
- **Scarsa visibilità** dei sistemi, spesso con dispositivi IoT connessi in modo frammentario
- **Dispositivi di telemetria legacy** la cui manipolazione potrebbe essere catastrofica
- **Scarsa segmentazione della rete**, con il 45% degli utenti ICS/SCADA che non ricorrono alla gestione delle identità privilegiate[4]

Il Report Fortinet 2019 Operational Technology Security Trend analizza i dati raccolti da milioni di dispositivi Fortinet per fotografare lo stato della sicurezza informatica per i sistemi ICS e SCADA. Le informazioni strategiche ricavate possono aiutare i responsabili della sicurezza di questi sistemi a comprendere i rischi e a definire la priorità delle misure da adottare.

Tendenze nel panorama delle minacce dei sistemi OT

Tendenza: gli attacchi basati sull'IT hanno un impatto crescente sui sistemi OT

Quando i sistemi OT vengono connessi alle reti IT, diventano spesso l'anello più debole della catena della sicurezza. I dati dei FortiGuard Labs indicano che gli aggressori utilizzano le minacce dei sistemi IT per attaccare i sistemi OT. In uno scenario tipico, gli autori delle minacce prendono di mira i sistemi IT e OT di un'organizzazione simultaneamente con lo stesso malware. Poiché i sistemi OT utilizzano spesso tecnologie più datate e le operazioni di sicurezza sono spesso meno sviluppate, gli attacchi a questi sistemi hanno un tasso di successo più elevato.

Gli autori delle minacce "riciclano" il malware per i sistemi OT.

Un altro scenario vede gli aggressori riutilizzare pacchetti malware legacy utilizzati in passato per attacchi IT, ma che ora vengono bloccati da tutte le soluzioni di sicurezza IT basate sulle signature. La Figura 1 mostra la percentuale di minacce esistenti rilevate da Fortinet durante ogni mese dell'anno, nonché il numero di dispositivi con protocolli OT colpiti da una delle minacce ogni mese. Come si può vedere, l'andamento è nettamente ciclico: quando vengono utilizzate più minacce, vengono colpiti meno dispositivi e viceversa.

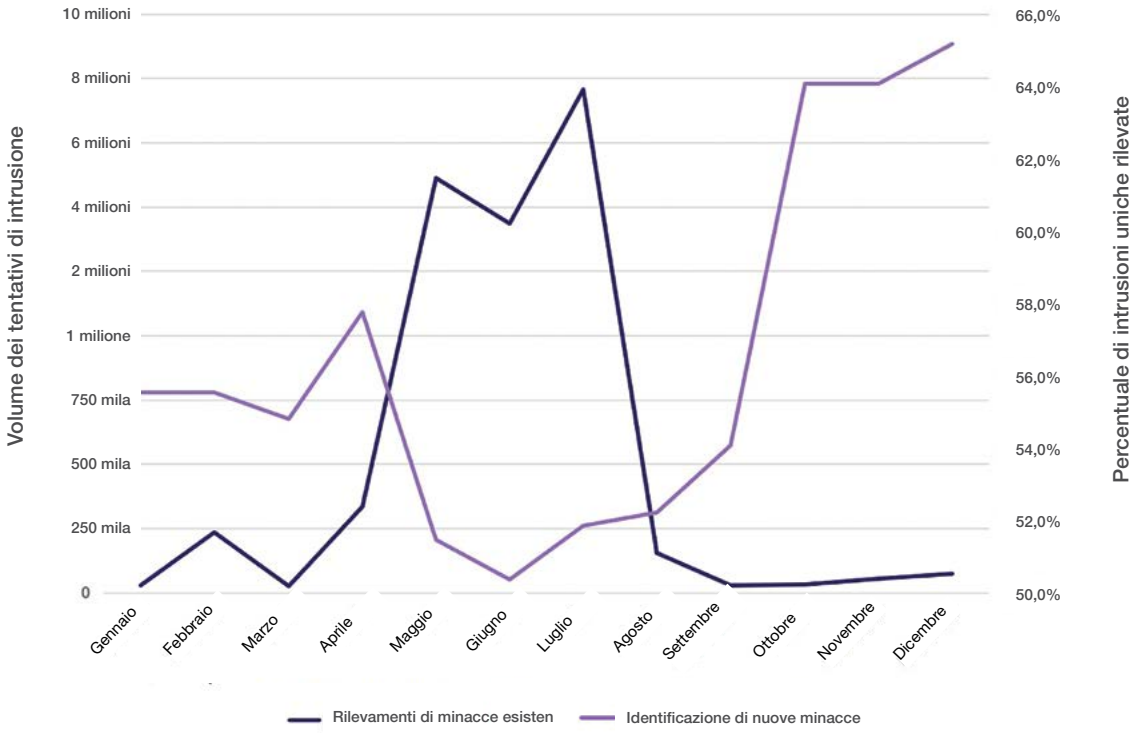


Figura 1: volume dei rilevamenti di intrusioni rispetto alle intrusioni uniche rilevate, 2018

Questo ciclo suggerisce che gli aggressori fanno tentativi per individuare nuove vulnerabilità nei sistemi OT appena connessi. Nella fase di "ricognizione", testano una gamma più ampia di vecchi malware su un numero relativamente piccolo di macchine. Una volta identificate le minacce che hanno successo, passano alla fase di "attacco" su un maggior numero di macchine, utilizzando gli attacchi che si sono dimostrati efficaci. Il loro obiettivo è ottenere il massimo valore dal malware esistente prima di investire nella creazione di nuovi attacchi più mirati.

Vi è un altro fattore che può contribuire a questa variazione stagionale nell'uso di minacce nuove rispetto a quelle vecchie. In particolare, sembrerebbe che gli attacchi ai sistemi HVAC e alle reti elettriche siano più probabili quando questi sistemi lavorano al massimo, generalmente durante i mesi estivi nell'emisfero settentrionale. Conta anche l'età dei sistemi OT: gli aggressori tendono a colpire più spesso le tecnologie più vecchie rispetto a quelle più recenti e più sicure.

Gli autori delle minacce attaccano dispositivi che utilizzano vari protocolli OT.

Mentre i sistemi IT hanno adottato da molti anni il protocollo TCP/IP come standard, i sistemi OT utilizzano una vasta gamma di protocolli, molti dei quali sono specifici per funzioni, settori e aree geografiche. La Fondazione OPC è stata fondata negli anni '90 come tentativo di condurre il settore verso la standardizzazione dei protocolli. La nuova architettura unificata di OPC (OPC UA) è potenzialmente in grado di unificare i protocolli per tutti i sistemi industriali, ma questa unificazione richiederà ancora molti anni, a causa della prevalenza di protocolli legacy e del lento ciclo di sostituzione dei sistemi OT.

I cybercriminali hanno cercato attivamente di sfruttare questa mancanza di standardizzazione puntando agli anelli deboli di ciascun protocollo. Questi problemi strutturali sono acuiti dalla mancanza di protezioni standard e dalle pratiche di sicurezza insufficienti adottate in molti sistemi OT, un'eredità degli anni in cui erano isolati dai sistemi IT.

Tre protocolli dominano in termini di volume.

Due fattori sembrano governare quali protocolli subiscono più attacchi in termini di volume di traffico: la loro diffusione e la loro vulnerabilità. Insieme, i protocolli OPC Classic, BACnet e Modbus rappresentano l'85% delle signature di Application Control che vediamo in esecuzione sui controlli OT.

Il protocollo di gran lunga più attaccato in termini di traffico è **OPC Classic**, il predecessore di OPC UA ma attualmente molto più diffuso. Rispetto ad altri, questo protocollo utilizza una tecnologia più recente (sviluppata per la maggior parte alla fine degli anni '90 e negli anni 2000), ma la sua prevalenza e l'isolamento in cui sono stati sviluppati i vari elementi lo rende un bersaglio allettante per i cybercriminali.

La domotica è un'area dell'OT che ha maggiormente adottato un unico protocollo come standard. **BACnet** è in uso in quasi tutte le organizzazioni di grandi dimensioni, indipendentemente dal settore, in parte perché è utilizzato da grandi fornitori di sistemi HVAC come Johnson Controls e Carrier. Come risultato, BACnet è il secondo protocollo più utilizzato. Un altro fattore: BACnet si basa su una tecnologia molto vecchia, che risale al 1987. Tre delle quattro minacce principali nel 2018 in termini di numero di dispositivi sono state di tipo BACnet (Figura 2). Il volume di rilevamenti di attacchi a macchine con protocollo BACnet ha registrato un picco nella prima metà dell'anno (Figura 3), corrispondente alla botnet Mirai che ha preso di mira i sistemi BACnet. Mirai ha causato eventi DDoS (Distributed Denial of Service) in tutto il mondo.[5] Il fatto che Mirai è presente da ottobre a dicembre 2018 ma BACnet è assente indica che Mirai, che è una botnet "noleggiabile", non è stata più utilizzata per attaccare BACnet ma altri sistemi OT.

Figura 2: primi 4 protocolli con rilevamenti per numero di dispositivi, 2018.

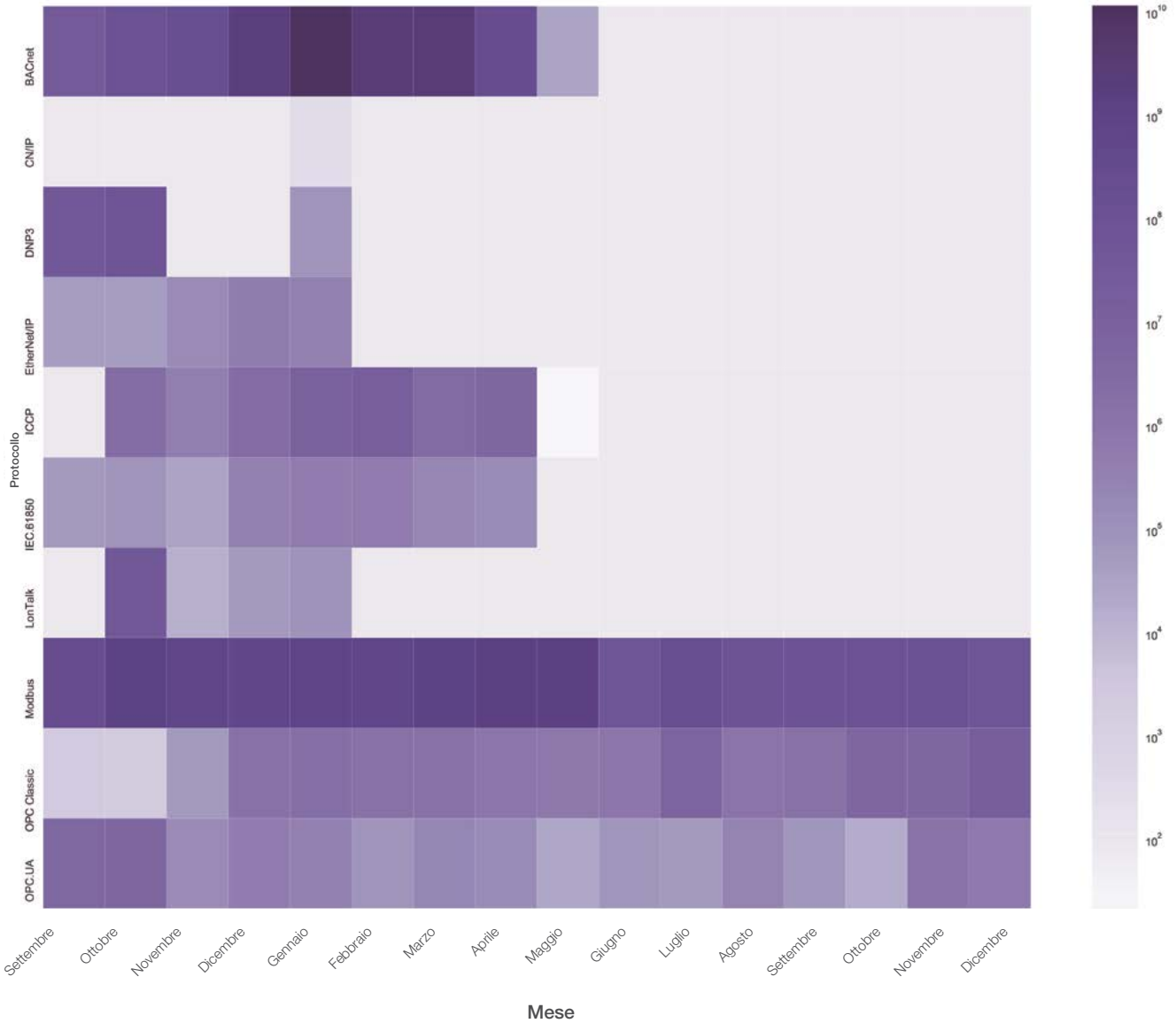


Figura 3: Volume di rilevamenti per protocollo, settembre 2017–dicembre 2018.

Il terzo protocollo più attaccato, **Modbus**, è un protocollo di comunicazione che facilita un'interazione efficace di diversi componenti dei sistemi OT. Questa tecnologia è stata sviluppata nel 1979 ed è stata progettata per un sistema chiuso (isolato con "air gap"). Modbus si presenta con decine di iterazioni diverse create da diversi fornitori, rendendo difficile per i team OT tenere traccia delle sue vulnerabilità.

Nessun fornitore ICS/SCADA è immune.

Nel 2018 sono stati rilevati attacchi mirati a ciascuno dei 70 fornitori OT che monitoriamo e, a parte pochi attacchi specifici (come quelli a Schneider e Moxa), queste minacce sono state costanti durante tutto l'anno (Figura 4). Detto questo, i fornitori più attaccati da minacce uniche sono tra i più grandi: Advantech, Schneider, Moxa e Siemens (Figura 5). Come regola generale, le soluzioni più datate e complesse presentano maggiori vulnerabilità rispetto ai prodotti più recenti e più efficienti.

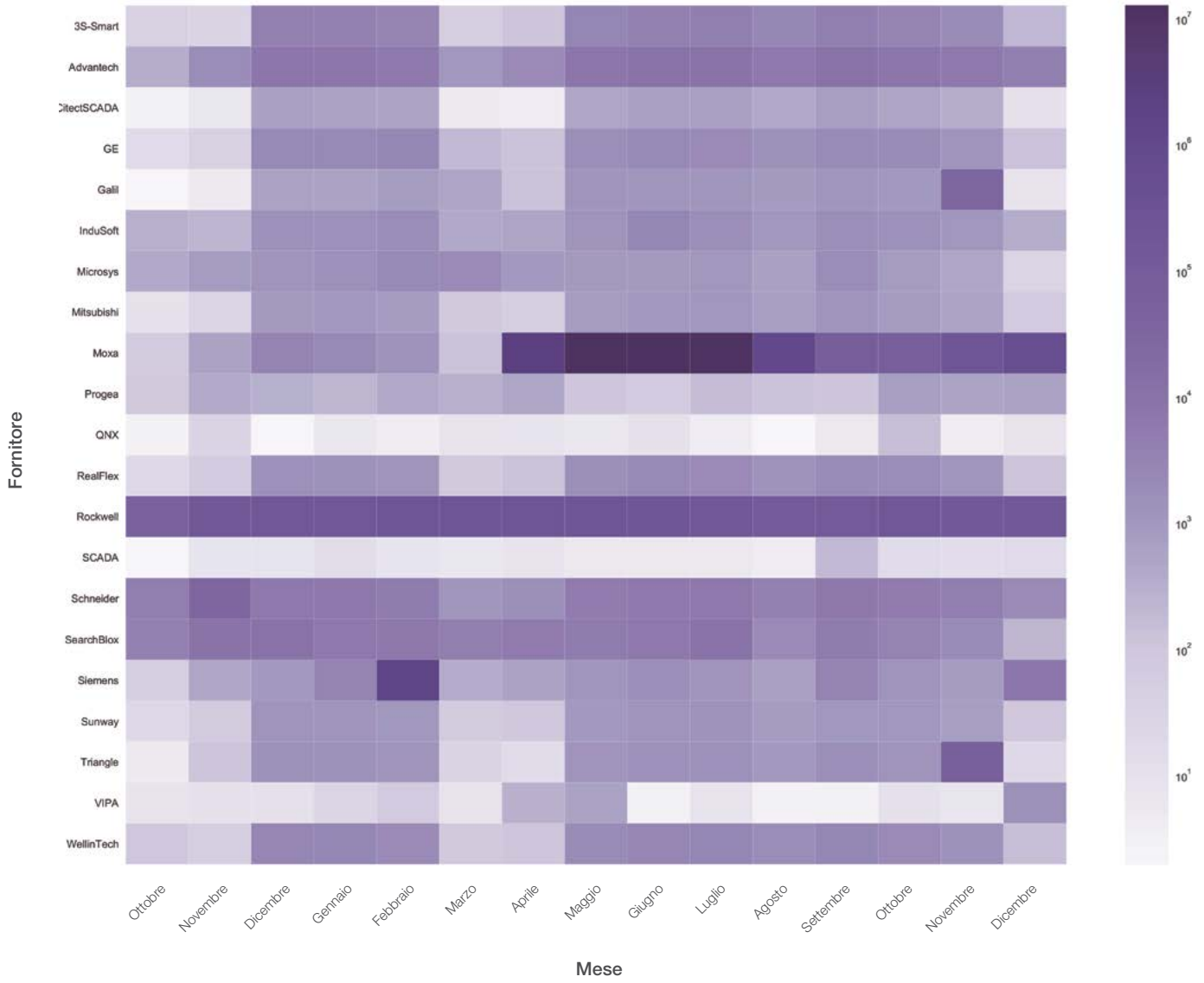


Figura 4: Volume dei rilevamenti di minacce mirate ai fornitori ICS/SCADA, ottobre 2017–dicembre 2018.

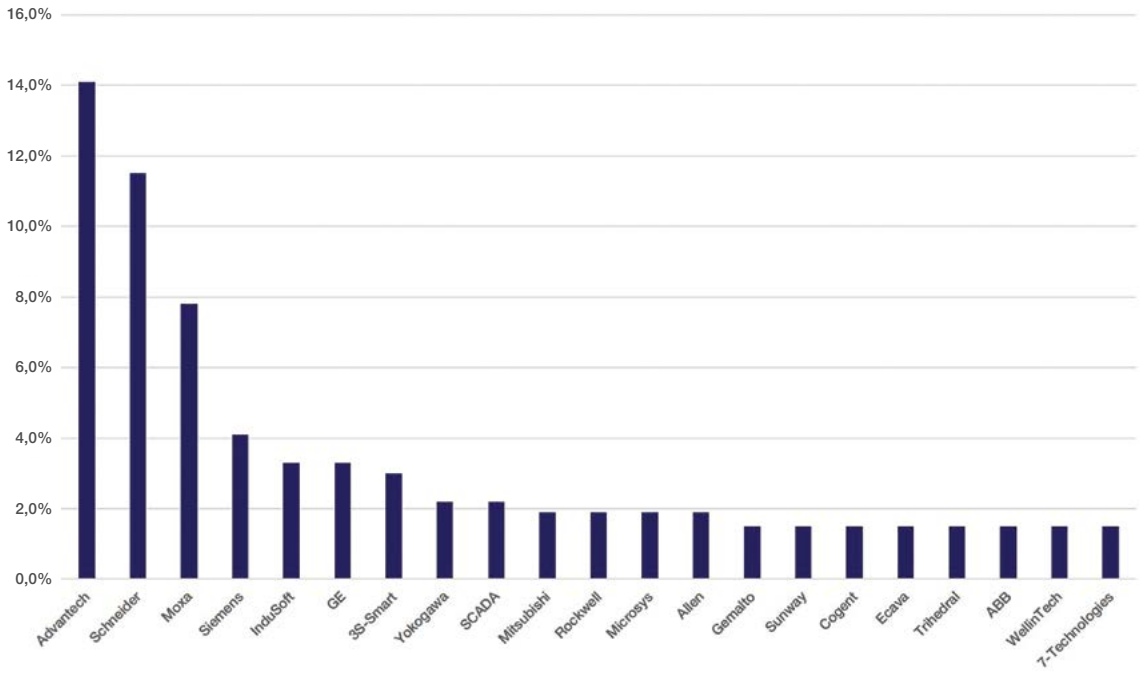


Figura 5: principali fornitori ICS/SCADA, classificati in base al numero di minacce uniche rilevate.

Complessivamente, gli attacchi informatici sono in aumento.

Nonostante le fluttuazioni stagionali e l'ampia varietà di obiettivi, su una cosa i dati sono chiari: gli attacchi informatici ai sistemi OT sono in aumento. Ad esempio, la Figura 1 mostra che il picco delle nuove minacce rilevate è molto più elevato alla fine dell'anno rispetto al picco di inizio anno. La Figura 6 illustra che nel corso del 2018 sono aumentati, sia in volume che in prevalenza, gli exploit mirati a quasi tutti i fornitori di ICS. Nulla fa prevedere un cambiamento di questa tendenza nel 2019. Il volume è la misura della frequenza o proporzione complessiva e rappresenta il numero totale o percentuale di osservazioni di un evento di minaccia. La prevalenza è la misura della diffusione o della pervasività tra i gruppi, con la percentuale di organizzazioni che hanno osservato l'evento di minaccia almeno una volta.

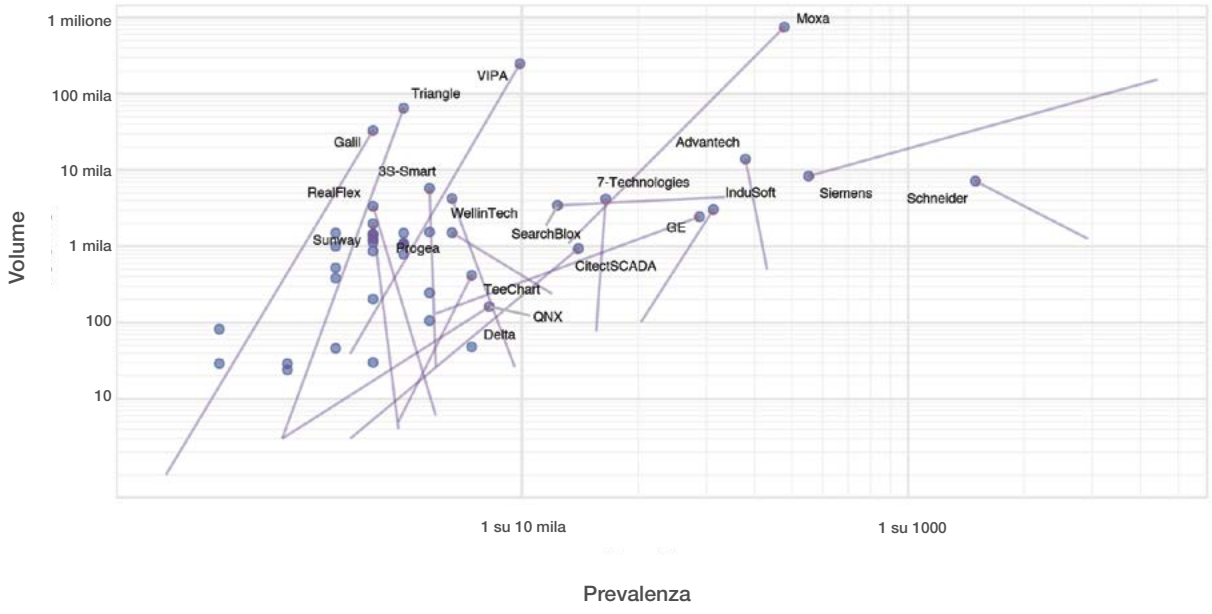


Figura 6: variazione della prevalenza e del volume degli exploit mirati ai principali fornitori ICS, T1-T4 2018.

Tendenza: continuano ad apparire attacchi mirati ai sistemi OT e i sistemi di sicurezza sono ora un obiettivo

Il malware specifico per i sistemi ICS e SCADA viene sviluppato da oltre un decennio, ma gli esempi non sono numerosi. Gli exploit specifici per OT includono **Stuxnet, Havex, Industroyer** e, più recentemente, **Triton/Trisis**.

Si ritiene che Industroyer e Havex siano stati inizialmente utilizzati dalle forze militari russe come armi cibernetiche contro la rete elettrica dell'Ucraina durante l'occupazione del paese nel 2016. Da allora il malware è trapelato ed è stato riutilizzato contro varie altre reti basate sulla stessa infrastruttura Schneider Electric.[11]

Un nuovo e pericoloso attacco prende di mira i sistemi di sicurezza.

Triton/Trisis prende di mira i controllori dei sistemi di sicurezza strumentati (SIS) Triconex, anch'essi venduti da Schneider Electric e diffusi nel settore energetico. Il suo primo bersaglio, un impianto petrolifero e di gas in Arabia Saudita, ha subito un arresto completo nel 2017.[12] Considerato che il malware ha come obiettivo il sistema di sicurezza, le conseguenze sarebbero potute essere peggiori, con la distruzione di macchinari e la messa a repentaglio di vite umane.[13] Nell'aprile 2019 è stata annunciata una seconda vittima di Triton/Trisis, un'anonima società in Medio Oriente.[14] Gli esperti sono allarmati da Triton/Trisis, che per molti aspetti è il primo vero attacco cyber-fisico ai sistemi OT.

Il ransomware continua ad attaccare i sistemi OT

All'inizio del 2018, i FortiGuard Labs hanno assistito a un forte aumento dei ransomware e dei ransom worm negli ambienti IT.[6] Questo aumento ha seguito a ruota l'attacco ransomware NotPetya del 2017, un evento massiccio che ha colto il segno, mettendo in ginocchio sistemi IT e OT in tutto il mondo. Tra i sistemi OT colpiti:

- **Merck:** NotPetya ha causato l'arresto dei sistemi OT nella maggior parte degli impianti del gigante farmaceutico, interrompendo la produzione e costringendo l'azienda a prendere in prestito 240 milioni di dollari di dosi di Gardasil dalle scorte gestite dai centri CDC statunitensi.[7] Nel complesso, l'attacco è costato all'azienda quasi un miliardo di dollari.
- **A.P. Møller – Maersk:** la più grande compagnia di trasporto di container del mondo ha subito un calo del volume di affari del 20% a causa di NotPetya, una cifra che sarebbe stata molto superiore se i dipendenti dell'azienda non si fossero prodigati a gestire manualmente l'enorme volume di attività globali e a ricostruire l'intera infrastruttura elettronica in 10 giorni.[8] Si stima che l'azienda abbia perso almeno 200 milioni di dollari a causa dell'attacco.

A partire dalla fine del 2018, gli attacchi di ransomware ai sistemi IT sono diminuiti e molti autori di minacce sembrano essere passati ad altri tipi di attacchi, come il cryptojacking.[9] Tuttavia i cybercriminali tendono a riciclare il malware esistente per attaccare i sistemi OT, molti dei quali non sono ben protetti come i sistemi informatici. Ciò può suggerire che il ransomware sarà presto una minaccia maggiore per i sistemi OT rispetto a quelli IT. Poiché gli SCADA Masters sono spesso basati su hardware con sistemi Microsoft Windows e Linux, le minacce ransomware possono avere un impatto su queste macchine, se non adeguatamente protette.

Questo scenario è stato confermato dall'attacco del marzo 2019 al gigante dell'alluminio **Norsk Hydro**, che ha causato la chiusura di diversi impianti ed è costato alla società 40 milioni di dollari nella prima settimana. Anche se sembra che il malware **LockerGoga** utilizzato per questo attacco sia stato perfezionato e migliorato, la sua prima manifestazione è stata relativamente semplice e modellata sul malware precedente.[10]

Gli attacchi con le vecchie minacce OT continuano.

I dati dei FortiGuard Labs indicano che il malware specifico per OT continua a colpire dispositivi in tutto il mondo. Ad esempio, la Figura 7 indica tentativi di intrusione con Industroyer significativi nel 2018, specialmente nella prima metà dell'anno. I malware complessi come Industroyer hanno in genere una lunga durata, anche dopo la distribuzione di informazioni sulle rilevazioni e signature.

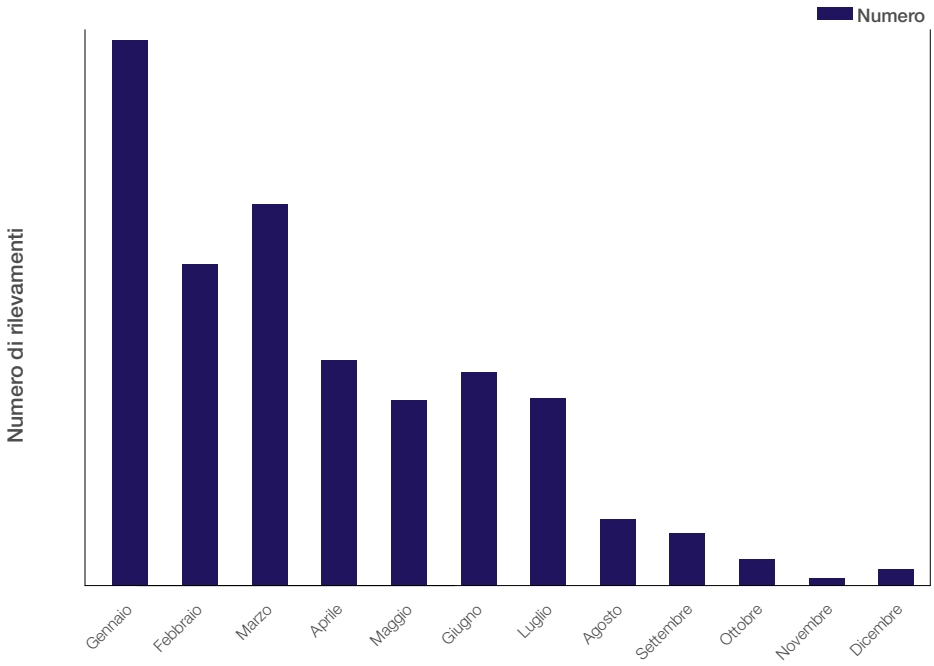


Figura 7: Rilevamenti del malware Industroyer, 2018.

EternalBlue: una minaccia per i sistemi Windows legacy

EternalBlue è stato sviluppato dalla National Security Agency (NSA) statunitense, secondo le testimonianze di ex dipendenti. Il 24 aprile 2017 è stato diffuso dal gruppo di hacker Shadow Brokers ed è stato utilizzato negli attacchi ransomware WannaCry e NotPetya nel corso dello stesso anno. Si ritiene inoltre che faccia parte del trojan dei sistemi bancari Retefe. Sfrutta una vulnerabilità del protocollo Microsoft SMB (Server Message Block).

Microsoft ha aggiornato il protocollo SMB a un nuovo protocollo chiamato Common Internet File Sharing (CIFS), pertanto i sistemi IT con infrastruttura Microsoft Windows aggiornata devono semplicemente configurare il protocollo CIFS per non accettare richieste che utilizzano il vecchio protocollo SMB. Purtroppo, molti sistemi ICS/SCADA sono basati su vecchie versioni di Windows che non supportano CIFS. È quindi necessario aggiungere al firewall NGFW un controllo esterno, che consente alcuni tipi di traffico SMB ma ne rifiuta altri.

Tendenza: gli attacchi ai sistemi OT vanno oltre i confini geografici

In un'economia globale dominata in molti settori da attori globali e caratterizzata da una connettività estrema, i confini geografici sono facili da attraversare sia per gli attori legittimi che per i criminali. La Figura 8 indica che, mentre gli attacchi contro la maggior parte dei fornitori sono stati relativamente uniformi da regione a regione, gli exploit contro Rockwell e Schneider hanno colpito in modo sproporzionato le Americhe (Nord e Sud America), dove la loro quota di mercato è più forte. D'altra parte, i sistemi Moxa sono diffusi ovunque e soggetti a molti attacchi mirati in tutto il mondo, nonostante l'origine giapponese del più grande attacco ai suoi utenti, la vulnerabilità Moxa 313 (vedere "La vulnerabilità Moxa 313: un exploit intenso e localizzato" a pagina 13).

Figura 8: distribuzione geografica dei rilevamenti di minacce esistenti mirate a specifici fornitori ICS/SCADA, 2018.

La Figura 9 mostra che, mentre i protocolli BACnet e Modbus sono stati ampiamente colpiti in tutto il mondo, l'area EMEA ha registrato il livello di rilevamento più elevato. Il volume degli attacchi ai protocolli è stato piuttosto uniforme in tutte le aree geografiche oppure più focalizzato nelle aree in cui i protocolli sono più comunemente utilizzati. Ad esempio, il protocollo ICCP è utilizzato principalmente da fornitori come Siemens e Honeywell, che hanno una presenza limitata in Asia.

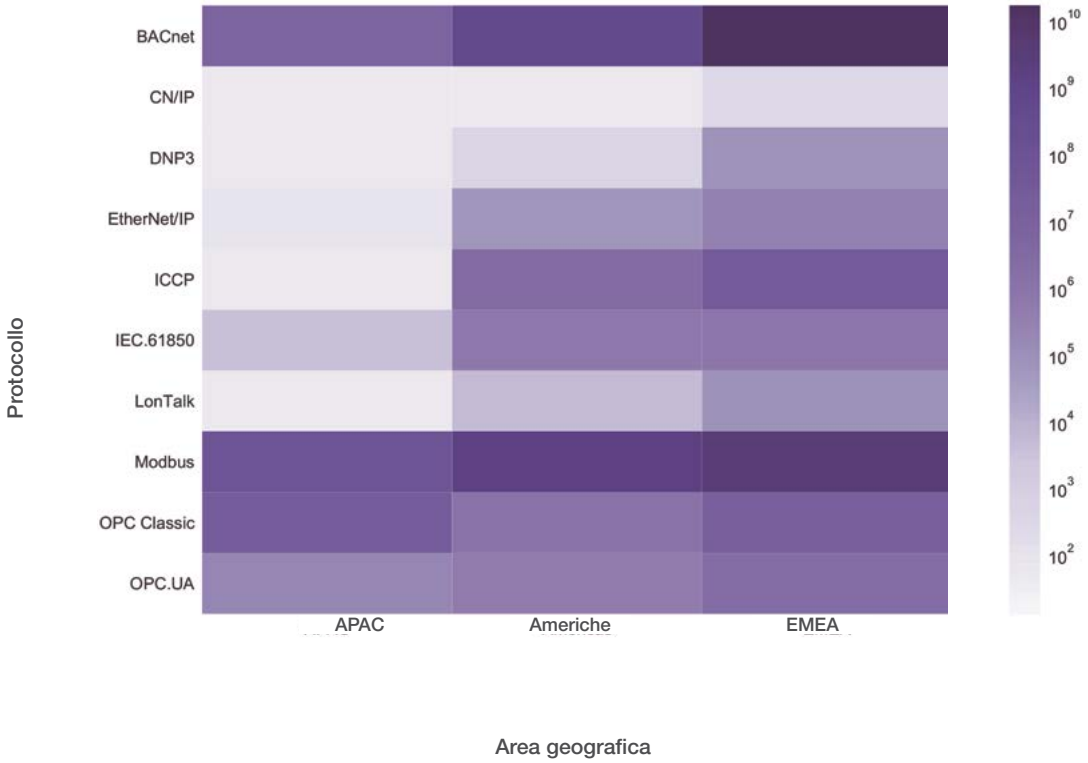


Figura 9: distribuzione geografica dei rilevamenti globali di minacce esistenti per protocollo, 2018.

La vulnerabilità Moxa 313: un exploit intenso e localizzato

Questo attacco, che si è manifestato nell'aprile 2018, ha riguardato una vulnerabilità di esecuzione dei comandi del sistema operativo nei dispositivi Moxa, in cui il sistema non convalidava l'input durante l'elaborazione di una richiesta Telnet dannosa. Ha colpito migliaia di NGFW in rapida successione durante i mesi di aprile, maggio e giugno, prima di scomparire quasi completamente a settembre (Figura 10), presumibilmente grazie alle patch applicate ai sistemi contro la minaccia.

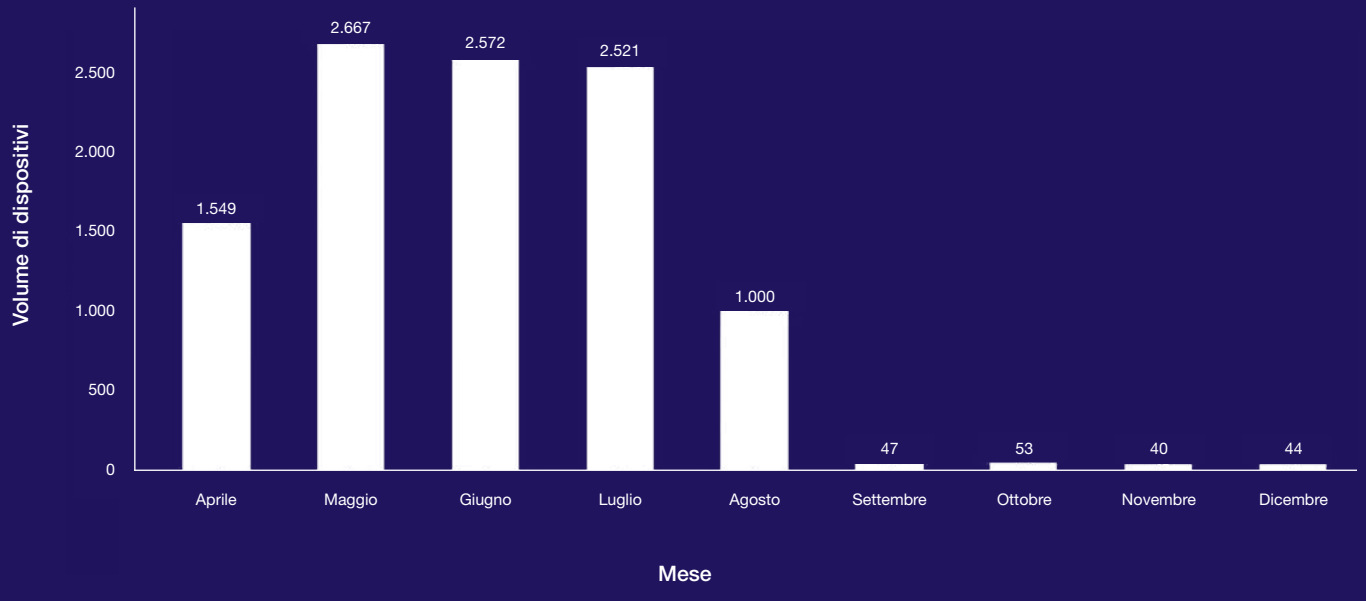


Figura 10: rilevamenti di Moxa 313 per mese, 2018.

L'analisi geografica di questo exploit rivela che l'attacco è quasi completamente limitato al Giappone (Figura 11), dove la tecnologia Moxa è ampiamente utilizzata nei prodotti di automazione domestica e aziendale. Tuttavia, i sistemi Moxa sono comunemente utilizzati in altri paesi del mondo. Il fatto che questo attacco abbia avuto un picco così rapido, anche se in un ambito geografico limitato, mette in evidenza il fatto che gli autori delle minacce tendono a colpire le parti più piccole e semplici di un'infrastruttura OT: i bridge e i convertitori seriali.

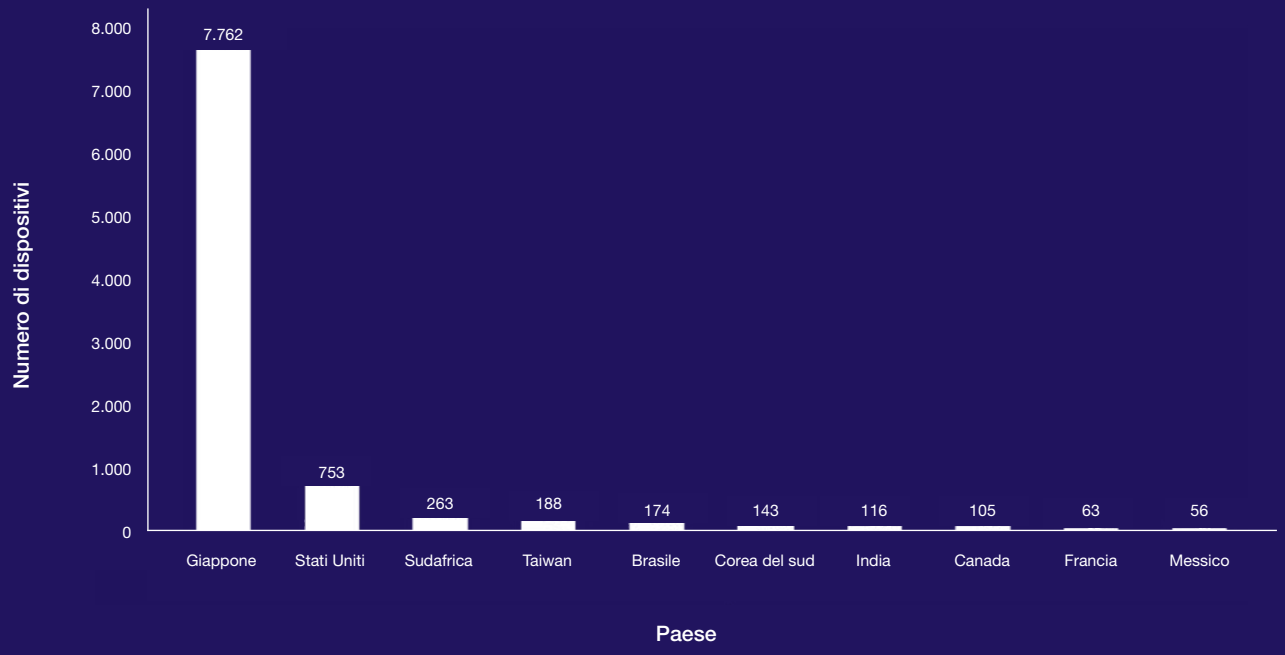


Figura 11: rilevamenti di Moxa 313 per paese, 2018.

Conclusioni

Il report Fortinet sulle tendenze nella sicurezza delle tecnologie operative 2019 dipinge un panorama di minacce che dovrebbe essere preso sul serio da qualsiasi organizzazione che abbia sistemi ICS/SCADA connessi. Gli aggressori elaborano le loro strategie estraendo il più possibile informazioni preziose da ogni nuova minaccia che sviluppano, colpendo vulnerabilità e sistemi non protetti nelle tecnologie vecchie e nuove. Le particolari sfide poste dalla lentezza dei cicli di sostituzione e dalla conseguente presenza di tecnologia legacy non scompariranno prima di diversi anni.

I governi di tutto il mondo stanno prendendo misure contro queste nuove minacce, soprattutto per quanto riguarda le infrastrutture critiche. I rischi sono grandi, fino a un collasso economico globale. In risposta, i governi hanno sviluppato linee guida per aiutare le imprese a proteggere le loro risorse critiche. Ad esempio, la North American Electric Reliability Corporation (NERC) ha definito standard in risposta al blackout del 2003 negli Stati Uniti nordorientali. Il fatto che standard come quelli del NERC e del NIST (National Institute of Standards and Technology) stiano diventando sempre più severi è un'ulteriore indicazione che la minaccia è reale.

I sistemi ICS e SCADA sono stati storicamente i cavalli da tiro tecnologici di molte organizzazioni e sono durati per decenni senza grandi aggiornamenti. La realtà delle minacce avanzate persistenti richiede un approccio più strategico, che include patch, segmentazione e controllo degli accessi. È inderogabile che tali sistemi siano soggetti allo stesso livello di protezione, agli stessi standard di sicurezza e agli stessi processi di monitoraggio e di reporting della rete IT. In caso contrario, la rete OT sarà l'anello debole attraverso il quale gli aggressori potranno infiltrarsi e accedere a sistemi e dati critici, sia in ambito OT che IT.

Per conseguire l'obiettivo desiderato, le funzioni IT e OT di ogni organizzazione devono superare le contrapposizioni culturali causate dal loro passato isolamento. I diversi team devono comprendere i reciproci valori, in modo che per il futuro possa essere costruita una relazione reciprocamente vantaggiosa. Le minacce sono reali e non faranno che aumentare. Il modo migliore per contrastarle è attraverso un approccio strategico completo, che coinvolga l'intera organizzazione.

Riferimenti

[1] Barbara Filkins, "The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns," SANS Analyst Program, luglio 2018.

[2] Jeff Goldman, "IoT Security Fail: 82 Percent of Companies Can't Identify All Network-Connected Devices," eSecurity Planet, 8 novembre 2017.

[3] "Report sullo stato della tecnologia operativa e della sicurezza informatica", Fortinet, marzo 2019.

[4] "Studi indipendenti individuano notevoli rischi per la sicurezza dei sistemi SCADA/ICS ", Fortinet, 7 maggio 2018.

[5] Oliver Gasser, et al., "Security Implications of Publicly Reachable Building Automation Systems," Technical University of Munich, consultato il 18 aprile 2019.

[6] "Quarterly Threat Landscape Report, Q4 2018," Fortinet, consultato il 9 aprile 2019.

[7] Eric Palmer, "Merck has hardened its defenses against cyberattacks like the one last year that cost it nearly $1B," FiercePharma, 28 giugno 2018.

[8] Richard Chirgwin, "IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz," The Register, 25 gennaio 2018.

[9] "Quarterly Threat Landscape Report, Q4 2018," Fortinet, consultato il 9 aprile 2019.

[10] Lindsey O'Donnell, "Ransomware Behind Norsk Hydro Attack Takes On Wiper-Like Capabilities," Threatpost, 27 marzo 2019.

[11] Charlie Osborne, "Industroyer: An in-depth look at the culprit behind Ukraine's power grid blackout," ZDNet, 30 aprile 2018.

[12] Lily Hay Newman, "Menacing Malware Shows the Dangers of Industrial System Sabotage," WIRED, 18 gennaio 2018.

[13] "FortiGuard Threat Intelligence Brief," Fortinet, 2 febbraio 2018.

[14] Tara Seals, "SAS 2019: Triton ICS Malware Hits A Second Victim," Threatpost, 10 aprile 2019.

FORTINET

www.fortinet.com

luglio 10, 2019 10:09 AM

D:\ARGOS\2019\07_2019\Assignment A-344888-924146\Work\PAKIET\OT\General\Report-security trends-A4_it_IT\Report-security trends-A4_it_IT

352048-0-1-IT