



COVER STORY

Sicurezza e performance
con le workstation CELSIUS
di Fujitsu

pag. 4-7

IN QUESTO NUMERO:

CYBER ATTACK

pag. 8

Attacchi sempre più mirati e guidati dall'artificial intelligence

pag. 11

I principali fattori di rischio per la sicurezza e cosa fare

SOLUZIONI

pag. 14

- Micro Focus rafforza la security intelligence con Intersect

pag. 16

- Un report Fortinet analizza il problema della cybersecurity in ambito OT

pag. 18

- FireEye acquisisce il Leader nella Security Instrumentation Verodin

pag. 19

- Con Trend Micro Apex One la sicurezza endpoint è definitiva

pag. 21

- L'abbraccio mortale per la sicurezza dei rootkit Scranos

Fujitsu consiglia Windows 10 Pro.

FUJITSU

shaping tomorrow with you

Affidabile,
potente
e leggero

FUJITSU Notebook
LIFEBOOK U938



Sottile e ultra-mobile.
Il notebook Fujitsu LIFEBOOK U938 è per i
professionisti che desiderano il meglio, ovunque.

Windows 10 Pro | Intel® Core™ i7-8650U | 20 GB RAM

Info: www.fujitsu.com/it/ultrabook | Numero verde: 800 466 820
customerinfo.point@ts.fujitsu.com | blog.it.fujitsu.com

© Copyright 2019 Fujitsu Technology Solutions GmbH

Fujitsu, il logo Fujitsu e i marchi Fujitsu sono marchi di fabbrica o marchi registrati di Fujitsu Limited in Giappone e in altri paesi. Altri nomi di società, prodotti e servizi possono essere marchi di fabbrica o marchi registrati dei rispettivi proprietari e il loro uso da parte di terzi per scopi propri può violare i diritti di detti proprietari. I dati tecnici sono soggetti a modifica e la consegna è soggetta a disponibilità. Si esclude qualsiasi responsabilità sulla completezza, l'attualità o la correttezza di dati e illustrazioni. Le denominazioni possono essere marchi e / o diritti d'autore del rispettivo produttore, e il loro utilizzo da parte di terzi per scopi propri può violare i diritti di detto proprietario. Schermate simulate, soggette a modifica. App Windows Store vendute separatamente. La disponibilità di app e l'esperienza possono variare in base al mercato.

 Windows 10

Windows 10 Pro è sinonimo di business.

Security & Business n.48
anno 2019

Direttore responsabile:
Gaetano Di Blasio

In redazione:
Giuseppe Saccardi, Paola
Saccardi

Hanno collaborato:
Riccardo Florio

Grafica: Aimone Bolliger
Immagini: dreamstime.com
www.securitybusiness.it

Editore: Reportec srl
Via Marco Aurelio 8
20127 Milano
tel. 02.36580441
Fax 02.36580444
www.reportec.it

Registrazione al tribunale
n.585 del 5/11/2010

Tutti i marchi sono
registrati e di proprietà
delle relative società

La sicurezza non è solo quella delle minacce dirette ai sistemi informatici, ma anche la capacità di realizzare innovazione per sistemi complessi che devono garantire fiducia nei dati. Questi ultimi in particolare, sono i protagonisti di un caso studio realizzato da Fujitsu, relativo a Luna Rossa. Il team, infatti, che sta organizzandosi per la prossima America Cup, sta progettando e preparando, muovendosi nei limiti del regolamento. Per raggiungere i massimi livelli occorre fare molta sperimentazione, ma questa sarebbe troppo costosa e meno precisa se basata su una prototipizzazione fisica, rispetto, invece a uno studio digitale basato sui dati storici.

Le workstation Celsiis di Fujitsu sono state scelte da Luna Rossa per ottimizzare le analisi e garantire la sicurezza del progetto, come racconteremo nella cover story di questo numero.

Visto il valore dei dati usati e quello dei dati che in Luna Rossa stanno accumulando, considerando gli interessi in gioco, è facile comprendere l'importanza della sicurezza. Le simulazioni e, più in generale l'utilizzo dei dati per l'automazione in fabbrica come in qualsiasi altro settore è un tema attualissimo, collegato all'Artificial Intelligence. Un tema che riguarda la sicurezza sotto diversi aspetti, sia sul fronte dei potenziali attacchi a sistemi di AI, sia riguardo i principi etici e politici che devono essere regolamentati, dato l'impatto sulle vite delle persone. Inquietanti anche gli scenari legati alla intelligenza artificiale.

Non si deve pensare al robot antropomorfo, ma ai dispositivi come quelli per la domotica, a cominciare dai sistemi di Amazon o Google, per continuare con gli smart watch e così via: progettati per aiutarci, potrebbero diventare uno strumento per controllarci.

Alcune valutazioni sulle minacce nella rubrica Cyber Attack, che contiene anche le riflessioni del Clusit sulle dinamiche di attacco, che è sempre più mirato e pericoloso. e le soluzioni proposte da alcuni dei vendor specializzati nel settore.

SICUREZZA E PERFORMANCE CON LE WORKSTATION CELSIUS DI FUJITSU

Nuovi modelli alzano il livello delle prestazioni per lo sviluppo di soluzioni avanzate, come quelle realizzate per Luna Rossa

di Gaetano Di Blasio

Le applicazioni software, che siano in cloud o meno, as a service oppure on premise, acquistano un'importanza crescente nell'era dell'automazione, del machine learning e dei big data.

Non va, però, dimenticato che le applicazioni, soprattutto quelle più esigenti in termini di prestazioni o quelle più direttamente collegate al business hanno bisogno di sistemi hardware di alto livello per essere efficaci. Lo sanno bene gli appartenenti all'equipaggio del team Luna Rossa che parteciperà come sfidante alla 36esima America's Cup.

Per progettare e costruire l'imbarcazione che parteciperà all'America's come approfondiremo più avanti, il suddetto team ha scelto le workstation di Fujitsu.

Le nuove CELSIUS C780 Rack Workstation

Indirizzate proprio alle applicazioni più esigenti, le nuove FUJITSU CELSIUS C780 Rack Workstation supportano i bisogni di accesso flessibile e sicuro per i processi con elevate esigenze delle GPU avanzate.

Un singolo rack con le più recenti tecnologie Intel in termini di processori, posizionato all'interno del data center, rappresenta la soluzione

Massimiliano Ferrini, Presidente e Amministratore Delegato di Fujitsu Italia



più sicura, sottolineano gli esperti di Fujitsu, per la realizzazione di progetti CAD o di applicazioni per il mondo dei media e dell'intrattenimento.

Un altro impiego ideale per le nuove workstation, evidenziano sempre presso Fujitsu, è la gestione del backend in sistemi video wall per i centri di controllo, tipicamente in ambito di sorveglianza o sale trading. Più in generale, come accennato, le nuove workstation sono apprezzate in comparti dove si utilizzano applicazioni che usano pesantemente le GPU, quali automobile, aeronautica, broadcasting, energia, sanità.

Fornendo un accesso flessibile alle applicazioni via rete attraverso pc portatili, thin client o desktop, CELSIUS C780 permette agli utilizzatori di lavorare



pressoché in ogni luogo, mettendo a disposizione le prestazioni di una workstation, senza richiedere spazio disco e capacità elaborativa al client.

La workstation è dotata di sistema operativo Windows 10 Pro pre-installato e supporta due schede grafiche singole "height high-end" oppure con una doppia scheda grafica "height ultra-high-end".

Ciò conferisce alla workstation capacità specifiche per l'impiego in contesti come il video editing, le simulazioni in progetti ingegneristici o l'animazione. Come accennato, i sistemi sono equipaggiati con processori di ultima generazione, quali gli Intel Core i e gli Intel Xeon E-2100, lasciando la scelta al cliente. A questo si aggiunge lo storage, che garantisce ulteriore flessibilità di scelta: sono disponibili soluzioni on-board (M.2) o periferiche SSD (per un maggior rapporto input/output in termini di prestazioni), inoltre, chi cerca una maggiore affidabilità può sfruttare le due espansioni M.2 per alloggiare NVMe RAID 0, 1, 5, e 10.

Fujitsu Server View embedded Lifecycle Management e Fujitsu Integrated Remote Management Controller semplificano la gestione dell'intero sistema, grazie al monitoraggio continuo e all'automazione di alcuni task.

A questo si aggiunge la tecnologia Fujitsu Cool safe Advanced Thermal Design, che consente alla workstation di operare nell'intervallo di temperatura tra 5°C e 40°C, con un conseguente efficientamento del consumo energetico.

Gilberto Nobili, Operations Manager e membro dell'equipaggio di Luna Rossa



Luna Rossa ci parla di Fujitsu

Luna Rossa è il nome scelto per il team nautico Prada, fondato nel 1997 da Patrizio

Bertelli, ispirato all'omonima e celeberrima canzone scritta da Vincenzo De Crescenzo e Antonio Vian nel 1950 e interpretata da decine di artisti di tutto il mondo.

Il regolamento della 36esima edizione della competizione velistica più prestigiosa del mondo è stato pubblicato e i team hanno accelerato gli sforzi per arrivare preparati e non lasciare niente al caso.

Restando ovviamente entro i limiti del regolamento, che definisce i parametri per l'ammissione alla gara, coprendo tutti gli aspetti legati alle barche classe



AC75 i team si stanno preparando anche utilizzando strumenti digitali avanzati per preparare al meglio equipaggi e imbarcazioni.

Il concetto progettuale della classe AC75 prevede due foil che consentono di sollevare completamente lo scafo al di fuori dell'acqua così da minimizzare la resistenza e raggiungere velocità estremamente elevate. Ogni foil può essere gestito indipendentemente con angoli differenti per ottimizzare l'equilibrio tra velocità e stabilità, una caratteristica di design che spiana la strada a significative opportunità competitive, ma che impone anche notevoli sfide ai progettisti.

Per questo sono necessarie continue simulazioni, che il team di Luna Rossa realizza grazie alle potenti workstation CELSIUS. Fujitsu fornisce anche i display.

Tali simulazioni sono altamente interattive e devono prevedere le molteplici possibilità, in modo da accelerare significativamente la fase di design e test, prima di arrivare alla creazione dei prototipi.

La sfida adesso è interamente digitale e

particolarmente importante. In passato si realizzavano modelli in scala che consentivano di realizzare misure approssimative in gallerie del vento e vasche navali, con processi costosi e lunghi. Grazie alle simulazioni digitali, che partono dai dati misurati su imbarcazioni reali e poi sui modelli digitali.

La tecnologia fornita dalle workstation Fujitsu CELSIUS permette di creare un prototipo completamente digitale che sarà sottoposto a simulazioni complete per tutti i calcoli necessari, dalla fluidodinamica computazionale (CFD), fino all'interazione fluido-struttura (FSI) e così via.

In questo modo il team Luna Rossa può confrontare l'efficacia delle diverse opzioni progettuali e di testare varie ipotesi, combinando tecnologie inge-

gneristiche basate su meccanica ed elettronica, fino ad arrivare a un prototipo fisico dettagliato e avanzato.

Fujitsu mette a disposizione anche display e

pc ESPRIMO a fianco dei notebook LIFEBOOK per consentire al Team Luna Rossa di collaborare in maniera efficace. Inoltre fornirà una rete storage per poter gestire i dati. La dotazione dei LIFEBOOK, dotati della protezione basata sui dati biometrici del palmo della mano, costituisce un ulteriore sistema di protezione dei preziosi dati.





Una sfida nautica e digitale

Massimiliano Ferrini, Presidente e Amministratore Delegato di Fujitsu Italia, ha dichiarato: «Le imbarcazioni che si sfidano nell'America's Cup hanno un livello di tecnologia velica all'avanguardia, che permette loro di spingersi oltre i propri limiti. Siamo orgogliosi che la tecnologia Fujitsu sia stata scelta dal Team Luna Rossa per testare un nuovo approccio digitale alla progettazione».

Ferrini aggiunge anche: «Le simulazioni complesse che le nostre workstation Fujitsu CELSIUS sono in grado di effettuare permetteranno di collaudare il prototipo dell'imbarcazione ancora prima che questo venga messo in acqua e, di conseguenza, di intervenire in una fase iniziale per applicare eventuali miglioramenti. Un vantaggio competitivo, non solo economico, fondamentale in una competizione come quella di Auckland».

Gilberto Nobili, Operations Manager e membro dell'equipaggio di Luna Rossa, evidenzia: «Anche se il regolamento della classe AC75 porterà le imbarcazioni in gara ad assomigliarsi molto, ognuna di loro sarà caratterizzata da sottili differenze che

giocheranno un ruolo importante tanto quanto l'equipaggio nel corso della regata, per la vittoria. Lavorare con i foil è particolarmente complesso, dato che bisogna bilanciare costantemente resistenza e spinta di sollevamento. La possibilità di verificare le idee progettuali per mezzo di simulazioni continue e rifinire i dettagli accelererà la nostra capacità di collaudare nuovi approcci e garantirci la miglior imbarcazione possibile per la sfida della America's Cup nelle acque di Auckland».

Una volta completate le simulazioni iniziali, il Team Luna Rossa costruirà e metterà in acqua un prototipo di imbarcazione. Il passo successivo sarà quello di verificare ogni aspetto delle sue performance, raccogliendo in tempo reale informazioni relative a fattori come la resistenza al vento, oltre ad acquisire dati dai dispositivi di bordo e dall'equipaggio per perfezionare ogni dettaglio del progetto. Una combinazione tra dati sperimentali e ulteriori test al simulatore porteranno a miglioramenti supplementari del design che saranno incorporati nell'imbarcazione che sarà costruita per la sfida. ❁

ATTACCHI SEMPRE PIÙ MIRATI E GUIDATI DALL'ARTIFICIAL INTELLIGENCE

Aumento del 57% Phishing e Social Engineering. Cresce lo spionaggio e la guerra sommersa tra nazioni. Intanto avanzano i rischi legati all'AI

di Gaetano Di Blasio

La cultura della sicurezza è ancora troppo poco diffusa, nonostante si senta parlare di attacchi informatici in televisione e sui media con regolare frequenza.

Il trend registrato dagli esperti del Clusit che, con l'annuale Rapporto analizzano dal 2011 lo stato della sicurezza a livello mondiale, mostra una curva di crescita senza sosta degli attacchi considerati significativi (tra quelli noti). Nel 2018, in particolare, si è manifestato un picco di attacchi con un più 38%. Addirittura gli attacchi considerati gravi sono saliti del 99%. Tra i settori più colpiti la sanità, dove criminali senza scrupoli bloccano le risorse e le reti per poi chiedere un riscatto. Il fattore gravità è ovviamente elevato per i potenziali rischi alla salute dei pazienti, ancor più che per le possibili violazioni a dati riservati e sensibili quali quelli trattati in questo settore.

Più precisamente, nel 96% dei casi gli attacchi a questo settore hanno avuto finalità cybercriminali e di furto di dati personali.

La crescita dell'IoT e, più in generale il diffondersi di

sistemi connessi in ogni ambito, dalle imprese alle case e così via, solleva il timore di poter arrivare a causare incidenti che passano dal piano virtuale del dark Web a quello fisico della vita reale in cui si espande l'uso del digitale.

Il Cybercrime resta la principale causa di attacchi gravi: il 79% di questi è stato infatti compiuto allo estorcere denaro alle vittime, o per sottrarre informazioni da rivendere e ricavarne denaro (+44% rispetto ai dodici mesi precedenti).

Aumenta l'attività di spionaggio cyber, comprese azioni di spionaggio indirizzate alla politica o all'industria, che hanno registrato un più 57% nel loro complesso, comprendendo anche il furto di proprietà intellettuale.

Dal Phishing e Social Engineering alla Cyber warfare

Grande ritorno del Phishing e Social Engineering, che per gli attacchi mirati, sono preferiti alle vulnerabilità (per quanto queste ultime siano comunque sfruttate massicciamente). L'obiettivo sono in buona parte le credenziali di accesso. A tal proposito si segnala anche un incremento del 7,7% di attacchi basati su tecniche di "Account Cracking", il che accentua l'importanza del sistema di Identity e Access Management. Hacktivism e Cyber warfare (la guerra delle informazioni, come viene chiamata dagli esperti del Clusit) sono invece in calo rispettivamente del 23% e del 10%. È altresì vero, che gli attacchi degli attivisti



Andrea Zapparoli Manzoni, membro del consiglio direttivo del Clusit



Stefano Quintarelli, membro del team di esperti della commissione dell'Unione Europea sull'artificial intelligence

informatici sono stati più gravi di quelli degli anni precedenti.

Specificano, infatti, gli autori del rapporto che occorre analizzare i livelli d'impatto per ogni attacco dal punto di vista geopolitico, sociale, economico e di immagine. Così facendo si riscontra un generale aumento della gravità media degli attacchi rispetto al 2017.

Più in dettaglio, sono stati classificati nel 2018 di livello "critico" l'80% di quelli realizzati con finalità di spionaggio, mentre oltre il 70% di quelli imputabili all'Information Warfare sono stati classificati di livello "critico".

Dopo la Sanità, la maggioranza degli attacchi è stata registrata nella Pubblica Amministrazione, che ha subito un 41% di attacchi in più rispetto all'anno precedente e gli attacchi multipli, indirizzati a più settori e caratterizzati principalmente dall'ottenere denaro, sono stati il 37% in più dei dodici mesi precedenti.

Siamo sempre più tutti quanti dei bersagli, sostengono gli esperti del Clusit, che ribadiscono ancora una volta quanto grande sia la disparità di forze e risorse in campo: «gli attaccanti sono diventati sempre più aggressivi e sono in grado di condurre operazioni su scala sempre maggiore, con una logica "industriale", che prescinde sia da vincoli territoriali sia dalla tipologia delle vittime», afferma Andrea

Zapparoli Manzoni, membro del consiglio direttivo del Clusit e uno degli autori del Clusit.

Nel 2018 sono stati presi di mira anche i settori della ricerca e formazione, dove c'è stato un aumento degli attacchi pari al 55%, mentre rispettivamente, sono cresciuti gli attacchi nei servizi online del 36% e quelli verso il cloud delle banche del 33%.

Le tecniche d'attacco

Spostando lo sguardo più direttamente sulle tecniche di attacco si osserva, con sconforto, che il principale vettore d'attacco è il semplice malware, prodotto "su base industriale e a basso costo. Ciò pone un vero e proprio esame di coscienza sull'attenzione alla formazione delle persone.

In questa categoria, peraltro, gli autori del rapporto Clusit hanno inserito anche i Cryptominers, pressoché inesistenti in passato (7% nel rapporto 2018), che oggi raddoppiano arrivando al 14%. Pressoché stabile il malware per il mobile al 12%:

Come accennato, Phishing e Social Engineering sono stati utilizzati in maniera crescente e con tecniche sfruttate su larga scala il che, sostengono gli esperti del Clusit è una riprova della logica "industriale" degli attaccanti, i quali realizzano costantemente codici malevoli nuovi, facendo registrare agli autori del rapporto un più 47% di tecniche sconosciute.

Quindi un impegno costante nel cercare nuove modalità di attacco.

I DDoS rimangono sostanzialmente invariati rispetto al 2017, lo sfruttamento di vulnerabilità note invece è ancora in crescita (+39,4%), così come l'utilizzo di vulnerabilità "0-day", (+66,7%). Gli autori, però, evidenziano che questo dato sia ricavato da un numero di incidenti noti limitato, quindi è presumibilmente sottostimato.

Unici attacchi in calo sono quelli basati su SQL injection, quasi spariti (meno 85%).

Cyber guerriglia

Secondo gli esperti Clusit, spiega, Zapparoli «siamo entrati in una fase di "cyber guerriglia" permanente, che rischia di minacciare la nostra stessa società digitale».

È una fase in cui evolvono rapidamente attori, modalità e finalità degli attacchi.

«È apparso evidente nel corso degli ultimi dodici mesi il graduale trasferimento dei conflitti sul fronte "cyber" da parte dei singoli Stati, con un innalzamento continuo del livello di scontro in una superficie di attacco di fatto illimitata».

Più precisamente, sottolinea l'esperto: «La crescita di cyber spionaggio e sabotaggio aggrava la cosiddetta "guerra della percezione" basata sulla creazione di fake news e sulla loro amplificazione attraverso i social media, cui si unisce il furto di informazioni per finalità geo-politiche, così da alzare il livello di rischio e quello degli attacchi.

A tutto ciò si aggiungono i rischi legati all'intelligenza

artificiale, che si presentano sia sotto forma di attacchi portati con sistemi di machine learning con automatismi a basso costo, sia per le vulnerabilità delle soluzioni AI.

A questo riguardo c'è una forte spinta da parte della comunità di scienziati e dei governi, per arrivare a una regolamentazione delle soluzioni e finalità dell'intelligenza artificiale. In particolare, la Commissione Europea ha affidato a un gruppo di esperti la realizzazione di linee guida che potrebbero diventare il seme per definire almeno una parte dei tanti aspetti che devono essere presi in considerazione, anche e soprattutto sul piano etico.

Il concetto base su cui si stanno ispirando tali esperti è quello del trustworthy, cioè "degnò di fiducia". Occorre che la AI sia accettata dalla popolazione, ma a molti fa paura, come ha spiegato Stefano Quintarelli, che fa parte dei suddetti esperti.

Come già in passato, le innovazioni sono piegate scopi riprovevoli e il risultato è che: «L'evoluzione rapidissima degli attori, delle modalità e delle finalità degli attacchi amplificano notevolmente i livelli di rischio, consentendo ai cybercriminali di finanziarsi per poter compiere poi crimini più importanti».

Tornando in particolare all'AI va osservato che da una parte tecniche di machine learning sono utilizzate dai cybercriminali per compiere attacchi in maniera molto efficace e sempre meno costosa; dall'altra, questi sistemi risultano oggi ancora piuttosto vulnerabili, e quindi facilmente attaccabili, anche a causa delle attuali difficoltà di monitoraggio e gestione dei sistemi. ❁

I PRINCIPALI FATTORI DI RISCHIO PER LA SICUREZZA E COSA FARE

Qualys ha analizzato il report di Verizon sulle Investigazioni di Data Breach (DBIR), i principali fattori di rischio per la sicurezza e che contromisure adottare

di Giuseppe Saccardi

Come ogni anno Verizon ha con il suo il nuovo Data Breach Investigations Report (DBIR) ha messo in luce gli ultimi trend delle minacce globali subite a livello internazionale.

I risultati della relazione di quest'anno, osserva Marco Rottigni, Chief Technical Security Officer EMEA di Qualys, si basano sui dati forniti da oltre 70 fonti (tra cui Quali stessa) riguardanti più di 41.000 incidenti di sicurezza, tra cui circa 2.000 violazioni dei dati, con ripercussioni in oltre 80 paesi e in tutti i settori industriali.

Tre sono in particolare i temi che l'esperto nella security evidenzia come particolarmente rilevanti:

- Chi sono gli obiettivi preferiti degli hacker, e perché
- L'importanza di ridurre il tempo impiegato per individuare i problemi di sicurezza, come le vulnerabilità o le violazioni, ed il tempo necessario per porre rimedio
- In che modo la mancanza di visibilità, gli errori umani e le configurazioni errate aumentano i rischi per la sicurezza delle organizzazioni



Le vittime

Quasi la metà delle violazioni ha coinvolto piccole imprese, e questo per svariate ragioni. Le piccole imprese hanno in genere un approccio più leggero alla sicurezza, spesso a causa di risorse scarse e competenze tecniche scarse. Sono anche un obiettivo attraente come parte della catena del valore, agevolando gli hacker ad arrivare alle reti informatiche delle aziende più grandi.

Analizzando i settori verticali si evidenzia come Government, Healthcare e Finance siano stati quelli colpiti più duramente.

Ciò conferma l'interesse di hacker nell'entrare in possesso di dati sensibili gestiti da queste organizzazioni, per procedere con la vendita o lo sviluppo di attacchi di scala superiore.

Tempistica nella reazione

Un aspetto preoccupante, nota Rottigni, è che oltre la metà delle violazioni hanno richiesto mesi per essere scoperte. Questo è un segnale negativo della scarsa visibilità che i team IT e di sicurezza hanno sulla infrastruttura informatica, sempre più ibrida e distribuita a causa della trasformazione digitale che complica monitorare, valutare, difendere e proteggere i vari ambienti.

Le tempistiche di una violazione evidenziano come la compromissione dei dati e l'azione di exfiltration avvengano in pochi minuti o giorni, mentre la scoperta degli attacchi può richiedere giorni se non settimane, mesi o anni. Senza considerare che quando si realizza di essere sotto attacco, serve spendere tempo, fatica e risorse per contenere i danni.

Per quanto riguarda le vulnerabilità, il 50% di queste vengono risolte entro 90 giorni dalla scoperta, mentre per il 25% sono necessari almeno 30 giorni. La tempistica può risultare efficace per molti, ma Rottigni ritiene, e di certo non a torto, che sia possibile fare molto meglio tramite l'integrazione tra programma di rilevamento e di rimedio.

Prodotti eterogenei e scarsamente interoperanti causano poi ritardi e punti ciechi soprattutto per la prevenzione delle violazioni, area in cui una piattaforma integrata che includa asset inventory, la gestione delle vulnerabilità, la prioritizzazione delle minacce e la gestione delle patch si rivela molto più efficace.



Marco Rottigni, Chief Technical Security Officer EMEA di Qualys

Le tattiche di un attacco

Nel report sono state rilevate tecniche di hacking nel 52% delle violazioni, mentre le infezioni da malware rappresentano il 28% dei casi e l'uso improprio dei dati dagli utenti autorizzati arriva al 15%.

Oltre alla mancanza di visibilità, queste situazioni evidenziano la necessità di rafforzare la compliance e ridurre gli errori di configurazione nei nuovi ambienti digitali fatti di istanze cloud, container, data center tradizionali, e collaboratori che operano in mobilità. Secondo Verizon è più comune la minaccia di errore non malevolo di un dipendente, piuttosto che parlare di sabotaggio premeditato. I problemi nascono sia per una configurazione errata dei server che consente l'accesso indesiderato oppure per la pubblicazione dei dati su un server che non dovrebbe essere accessibile da tutti. Serve definire correttamente gli accessi, sottolinea il report.

Un'altra tendenza preoccupante è il dominio delle minacce esterne che rappresentano il 69% delle violazioni, con il ransomware che rimane tra le minacce più diffuse (rilevato nel 24% degli incidenti). Tutto questo evidenzia l'importanza di applicare un

adeguato programma di gestione delle vulnerabilità e dei rimedi, per ridurre la superficie vulnerabile esposta agli attaccanti.

Per aumentare sicurezza e velocità di risposta, appare quindi consigliabile:



- La prioritizzazione del processo di rimedio, in modo da identificare e risolvere immediatamente le minacce più critiche per la propria organizzazione
- La distribuzione di dashboard dinamiche nei vari reparti dell'organizzazione, per potenziare la consapevolezza della situazione
- Una automazione trasparente di tutte le piattaforme che coinvolgono i processi IT e Security

Un altro elemento che sottolinea l'importanza di avvalersi di un valido programma di gestione delle vulnerabilità è che queste si classificano al terzo posto tra le tecniche di compromissione più diffuse e spesso il vettore delle violazioni è legato proprio alle web application.

Aspetto chiave per una prioritizzazione efficace è la capacità di consumare dati di cyber threat intelligence; utilizzare criteri come quanto una vulnerabilità sia sfruttabile tramite exploit, disponibilità di patch ed altri indicatori di minacce da mettere in correlazione con le informazioni sulle vulnerabilità. Il report evidenzia anche l'importanza di conformità ai regolamenti: abuso dei privilegi, gestione errata dei dati e processi temporanei non approvati sono infatti tra le prime cause di violazioni rilevate e sono sinonimi di mancata compliance.

Come comportarsi

È il momento per le organizzazioni, suggerisce Rottigni, di ripristinare fondamenta solide per sicurezza e conformità. Tutto deve partire dall'inventario delle risorse IT che deve essere continuamente aggiornato, assicurando poi una rilevazione efficace ed accurata delle vulnerabilità e delle configurazioni errate.

Ma non basta. Subito dopo, è necessario assegnare le giuste priorità alle attività di rimedio correlando gli indicatori di minaccia informatica con le risorse e le loro vulnerabilità.

È fondamentale avere un programma di gestione delle patch integrato per correggere rapidamente gli asset interessati.

E' indispensabile assicurarsi che tutti gli apparati, non solo i sistemi locali, siano inclusi nei processi di controllo e rilevamento: dispositivi mobili, cloud workload, applicazioni containerizzate, pipeline DevOps, sistemi IoT e dispositivi di Operational Technology (OT).

Sono tutte attività complesse in cui, evidenzia l'esperto, Qualys può essere di supporto. ❄

MICRO FOCUS RAFFORZA LA SECURITY INTELLIGENCE CON INTERSET

Micro Focus amplia il suo portafoglio di soluzioni di Security, Risk & Governance con l'acquisizione di Intersect, azienda canadese che porta in dote una sofisticata tecnologia per l'analisi dei comportamenti basata su algoritmi di Intelligenza Artificiale

di Riccardo Florio

Nel mondo della Digital Transformation non solo gli attacchi crescono in numero, ma spesso hanno poco o nulla a che fare con il rilascio di codice nocivo. Anche il "nemico" da fronteggiare è cambiato e non è fatto più di individui isolati, ma di organizzazioni criminali strutturate. In molti casi, come nei cosiddetti attacchi APT (Advanced Persistent Threat) anche la fase di sottrazione dei dati avviene in modo nascosto, cercando di protrarsi il più a lungo possibile.

Prevenire è meglio che subire

Di fronte a questi scenari l'utilizzo di modelli di protezione di tipo preventivo, che bloccano gli attacchi prima che possano sortire qualunque effetto, appare come la modalità d'intervento più logica anziché basare la sicurezza sulla mera classificazione del malware e su un approccio reattivo, intervenendo quando il danno è già stato fatto.

Per questo motivo la sicurezza è sempre più basata su modelli di Security intelligence, che sfruttano le tecnologie di Intelligenza artificiale e Machine learning per individuare e interpretare le tracce che ogni tentativo di attacco porta con sé. Si tratta di un



*Pierpaolo Ali,
Director Southern
Europe di Micro
Focus Security*

trend confermato anche dagli analisti come Gartner, secondo cui "entro il 2025, il Machine learning rappresenterà una componente normale delle pratiche di sicurezza e compenserà alcune carenze di competenza e di personale" (fonte: Gartner top 6 Security and Risk management trends for 2018).

È in questo contesto che si inserisce la recente mossa strategica di Micro Focus, colosso mondiale del software, che si è rafforzato ulteriormente nell'ambito delle soluzioni di Security, Risk & Governance grazie all'acquisizione di Intersect.

"Micro Focus prosegue nel percorso di rafforzamento delle sue soluzioni di sicurezza - ha osservato Pierpaolo Ali, Director Southern Europe di Micro Focus Security - attraverso un piano di investimenti avviato 18 mesi fa di oltre 300 milioni di dollari in Ricerca e Sviluppo, per mantenere le nostre

tecnologie sempre all'apice dell'innovazione e in grado di rispondere alle reali esigenze degli utenti. Negli ultimi 12 mesi Micro Focus ha emesso 10 nuove release delle sue piattaforme e molte altre novità sono in arrivo”.

Intersec impara a individuare i comportamenti anomali

Intersec è un'azienda canadese con sede a Ottawa, creata da un team di matematici per progettare algoritmi di Intelligenza Artificiale e Machine Learning finalizzati all'analisi comportamentale in “use case” di sicurezza.

L'omonima soluzione software integra oltre 200 algoritmi ed è stata sviluppata sulla base dell'analisi di “use case” reali per rilevare in modo rapido e accurato potenziali minacce. Intersec utilizza algoritmi di apprendimento non supervisionato che sono in grado di analizzare l'esperienza dell'utente, interpretare le classi di eventi e riclassificare le modalità con cui analizzare gli input successivi per effettuare nuove previsioni.

Intersec si basa sull'attribuzione di indici di rischio individuali. L'indice di rischio viene definito in base all'analisi del comportamento di un utente, verificando se e quanto questo si discosta dal modello esperienziale passato dello stesso utente, di utenti con un profilo analogo o dai comportamenti ritenuti anomali rispetto alle regole aziendali (per esempio eccessivo volume di traffico in uscita o accesso ad alcuni componenti che non competono al suo profilo). L'analisi comportamentale permette di intervenire anche nei casi che sfuggono alla rilevazione delle regole deterministiche, che riescono a identificare le attività potenzialmente malevole solo nel caso di superamento di specifiche soglie (per esempio la



ripetizione di un tentativo di accesso molte volte in un limitato intervallo di tempo).

Le anomalie comportamentali individuate da Intersec possono generare eventi che possono essere sia gestiti automaticamente dalla soluzione software sia a livello di SOC.

Le caratteristiche chiave della tecnologia Intersec includono:

- funzioni di analytics estese con molteplici impostazioni pronte all'uso per affrontare specifiche minacce quali: minacce interne, attacchi mirati e frodi;
- una libreria di oltre 350 modelli di Machine learning e analytics avanzata per rilevare, correlare e quantificare i comportamenti a più alto rischio;
- la combinazione di un motore di analytics avanzata con tecnologia open source e Big data, tra cui Kafka, Spark, Phoenix, Hadoop, HBase, Elasticsearch, ZooKeeper, d3 e Kibana; questo motore può essere implementato nelle infrastrutture Vertica, Hortonworks o Cloudera, scalando per soddisfare le esigenze anche degli ambienti più grandi e con requisiti elevati.

La tecnologia Intersec è in fase di integrazione all'interno dell'ecosistema di soluzioni di sicurezza di Micro Focus, incluso il motore di correlazione di ArcSight e la piattaforma Vertica.

FORTINET ANALIZZA IL PROBLEMA DELLA CYBERSECURITY IN AMBITO OT

Circa il 74% degli ambienti OT ha subito un'intrusione di malware negli ultimi 12 mesi. Fortinet fa il punto sulla situazione e sul come porvi rimedio

di Giuseppe Saccardi

Fortinet, attiva a livello mondiale nelle soluzioni di cyber sicurezza integrate e automatizzate, ha presentato i risultati di un'indagine che dà una visione approfondita della cyber security in ambito OT. Il sondaggio, svoltosi a inizio 2019 negli USA, ha come attori i Plant Operation leader di grandi società in diversi settori strategici. Ha coinvolto figure professionali che si occupano di procedure di Operational Technology e asset per la cybersecurity in aziende con più di 2.500 dipendenti nei settori manifatturiero, energia e utility, healthcare e trasporti. L'Operational Technology (OT), ha osservato l'azienda, è di vitale importanza per la sicurezza pubblica e per il benessere economico, in quanto controlla le apparecchiature che gestiscono gli impianti di produzione, le reti elettriche, i servizi idrici, le compagnie di trasporto marittimo e molto altro ancora. Se tradizionalmente le reti OT e IT hanno operato separatamente, di recente le tecnologie IT-based come i sensori, il machine learning (ML) e i big data vengono integrate con i network OT per ottenere nuovi vantaggi competitivi e incrementare



l'efficienza. Questo comporta l'aumento delle aree potenzialmente vulnerabili.

L'indagine svolta da Fortinet ha evidenziato dati particolarmente rilevanti:

- Gli attacchi informatici hanno un forte impatto sugli ambienti OT: circa il 74% ha subito un'intrusione di malware negli ultimi 12 mesi, con gravi ripercussioni su produttività, fatturato, fiducia nel brand, proprietà intellettuale e sicurezza fisica.
- Uno scarso livello di sicurezza informatica contribuisce ad aumentare il rischio. Il 78% delle società ha una visibilità parziale della cyber sicurezza dei propri ambienti OT, il 65% non ha il controllo degli accessi basato sui ruoli e più della metà non usa l'autenticazione a più fattori o la segmentazione della rete interna.
- Le aziende che intendono migliorare la sicurezza OT spesso devono tener conto di due fattori: da un lato la necessità di stare al passo con i cambiamenti sempre più rapidi e dall'altro la mancanza di personale. Quasi i due terzi (64%) dei responsabili OT sostengono che tenere il passo

con il cambiamento sia la più grande sfida che sono chiamati ad affrontare. Quasi la metà (45%), inoltre, considera un limite la carenza di figure qualificate.

- Le società stanno ponendo un'attenzione sempre maggiore al tema della cybersecurity, con un 70% che pianifica di affidare la sicurezza dell'OT al CISO nel corso del prossimo anno (attualmente solo il 9% dei CISO si occupa di monitorare la sicurezza OT) e il 62% dei budget dedicati a tale ambito è in aumento.

Cybersecurity, cosa fare per migliorarla

Gli ambienti OT, spiega Fortinet, sono soggetti a un rischio elevato: quasi 8 su 10 hanno subito attacchi informatici nel corso dello scorso anno, la metà di essi ha riportato un numero di violazioni che va da 3 a 10.

Questa ricerca identifica quei fattori che devono essere presi in esame per ridurre il rischio, come il fatto che il 78% delle società abbia una visibilità parziale della cyber sicurezza, il 56% non ha un'autenticazione a più fattori e il 53% non utilizza ancora una segmentazione del network aziendale, best practice fortemente raccomandata.

Tuttavia, i responsabili delle Operation in ambito OT dichiarano di influire sulla scelta delle soluzioni per la sicurezza informatica. In particolare, evidenziano che lo fanno cercando sistemi in grado di massimizzare la produttività riducendo al minimo i costi. Rispetto alle organizzazioni in ambito OT che hanno subito più di 6 intrusioni in 12 mesi, quelle che non ne hanno subite si dichiarano favorevoli a:

- Utilizzare un'autenticazione a più fattori (100%)

- Utilizzare un controllo degli accessi basato sui ruoli (94%)
- Gestire e monitorare eventi di sicurezza, oltre ad eseguirne l'analisi (68%)
- Utilizzare la segmentazione della rete (51%)
- Pianificare verifiche di conformità della sicurezza (46%)

Il malware sembra farla da padrone. Quasi tre quarti (74%) delle organizzazioni OT hanno sperimentato almeno un'intrusione di malware nell'ultimo anno e metà di esse (50%) ha subito da 3 a 10 o più intrusioni.

Il malware rappresenta in sostanza la principale forma di intrusione, seguita da phishing (45%), spyware (38%) e violazioni della sicurezza dei dispositivi mobili (28%).

Per ovviare alla mancanza di visibilità a livello centralizzato e alla scarsità di personale, suggerisce Fortinet, è bene tenere conto delle seguenti raccomandazioni:

- È importante adottare soluzioni di sicurezza in grado di operare in sinergia per fornire la visibilità più ampia possibile della portata dell'attacco subito, abbracciando gli ambienti OT e IT.
- È necessario applicare un approccio fabric-based alla sicurezza che offra protezione integrata su tutti i dispositivi, network e applicazioni.
- È buona pratica ricercare funzionalità di sicurezza automatizzate, con soluzioni in grado di coordinare la reazione a una minaccia e che utilizzino tecnologie come il machine learning.
- Ridurre al minimo il rischio attuando best practice per la cyber sicurezza OT come segmentazione della rete, autenticazione a più fattori e controllo dell'accesso basato sui ruoli. ❄

È anche disponibile, sul tema delle diverse sfaccettature del cloud e relativa sicurezza, un white paper di Reportec scaricabile gratuitamente.

FIREEYE ACQUISISCE IL LEADER NELLA SECURITY INSTRUMENTATION VERODIN

La migliore risposta agli attacchi informatici è la verifica costante e il continuo adattamento della sicurezza alle minacce reali.

di Edmondo Espa

«La sicurezza informatica oggi si basa su assunzioni: le tecnologie funzionano come dichiarano i vendor, i prodotti sono installati e configurati correttamente, i processi sono pienamente efficaci e le modifiche all'ambiente sono adeguatamente comprese, comunicate e implementate. Tuttavia per quasi tutte le organizzazioni la realtà è molto diversa e questo spesso viene scoperto solo dopo una violazione», dichiara Chris Key, co-fondatore di Verodin e CEO prima dell'acquisizione da parte di FireEye.

L'efficacia dei sistemi di sicurezza non sembra, quindi, essere sempre proporzionata agli sforzi messi in

atto dalle aziende, le quali frequentemente non tengono conto della rapida evoluzione degli attacchi informatici e della crescente determinazione dei gruppi di attacco ad allargare il proprio campo di azioni criminali in settori fino a ieri risparmiati.

Come è riportato infatti nel Mandiant® M-Trends® 2019 report rilasciato lo scorso Marzo da FireEye, non solo sono sensibilmente aumentati gli attacchi distruttivi, immediatamente visibili e accompagnati da richieste di riscatto, ma, mentre fino a pochi anni fa i settori colpiti erano relativamente pochi, Finanze in primis, ora non c'è settore che venga risparmiato o considerato non profittevole dagli hacker.

L'acquisizione di Verodin da parte di FireEye è la risposta alle esigenze di una sicurezza digitale generalizzata e costante nel tempo, ed è finalizzata ad estendere e integrare reciprocamente la capacità di aiutare i clienti nell'adottare un approccio proattivo per comprendere e mitigare i rischi, le inefficienze e le vulnerabilità nei loro ambienti.

Da sinistra:
 David Grout (CTO, EMEA),
 Marco Riboli (Senior Vice
 President Southern Europe),
 Luca Brandi (Channel Sales
 Leader, EMEA Southern
 Region)



Come infatti dichiara Kevin Mandia, CEO di FireEye, «Verodin ci dà la possibilità di automatizzare i test di efficacia utilizzando attacchi sofisticati, alla cui risposta dedichiamo solitamente centinaia di migliaia di ore, fornendo così un approccio sistematico, quantificabile e continuo alla convalida dei programmi di sicurezza. Riteniamo che non vi sia modo migliore per addestrare le persone e gli strumenti di sicurezza se non effettuando attacchi continui verso l'ambiente e adattando i controlli di sicurezza alle minacce reali. Finalmente, le organizzazioni avranno un modo affidabile e coerente per quantificare

il rischio informatico, in maniera comprensibile sia per i tecnici in prima linea sia per il Board.»

La piattaforma Verodin integra i prodotti di sicurezza informatica e i servizi tecnologici già installati. Verodin si integrerà con le funzionalità di orchestrazione della sicurezza di FireEye® Helix™, per aiutare i clienti a dare priorità e automatizzare il miglioramento continuo dei controlli di sicurezza. I clienti potranno, inoltre, implementare le soluzioni di misurazione e convalida della sicurezza informatica Verodin "as-a-service" attraverso il servizio FireEye Managed Defense e come parte dell'offerta Expertise On Demand.

Le soluzioni di Verodin continueranno ad essere disponibili in maniera autonoma attraverso i rivenditori dell'azienda, così come attraverso la comunità globale dei partner di canale di FireEye. ❁

CON TREND MICRO APEX ONE LA SICUREZZA ENDPOINT È DEFINITIVA

Rilevamento e risposta automatizzate, unite a una visibilità approfondita per l'IT e i team di security, la soluzione all-in-one vuole ridefinire la sicurezza degli endpoint

di Giuseppe Saccardi

È un dato di fatto che il mondo IT stia vivendo un grande cambiamento. Le migrazioni cloud, e multicloud, la convergenza di IT e OT, un'adozione sempre maggiore di tecnologie per lo smart working e una connettività in crescita, creano nuove opportunità di business per le aziende ma anche nuovi possibili punti di attacco per i cyber criminali.

Questi cambiamenti obbligano a ridefinire il concetto di protezione degli endpoint.

Se prima la sicurezza degli endpoint tendeva a essere considerata una commodity, ora, osserva Trend

Micro, acquisisce un valore intrinseco molto forte e per questo non è più trascurabile.

Le aziende si troveranno, infatti,, ad affrontare pericoli concreti sempre più sofisticati, che metteranno a dura prova gli asset strategici, il patrimonio di dati, la compliance alle normative e la reputazione. «In Trend Micro, ci impegniamo quotidianamente per garantire un altissimo livello di protezione ai nostri utenti. Nell'ultimo anno abbiamo pensato a come poter supportarli in un modo totalmente nuovo e che fosse il più possibile funzionale in ottica futura. Così è nata Apex One, la nuova soluzione all-in-one che automatizza il rilevamento e la risposta fornendo una visibilità completa all'IT e ai team di security. Rispetto alle precedenti soluzioni tradizionali di antimalware, Apex One si presenta come una piattaforma unificata per la gestione di diversi servizi, ridefinendo in questo modo la sicurezza degli endpoint, grazie alle sue vaste capacità offerte attraverso un singolo agente, sia negli ambienti SaaS che nei deployment on-premise» ha commentato Salvatore Marcis, Technical Director Trend Micro Italia.

Tre le principali innovazioni presenti in Apex One:

- **Automated Detection & Response:** Apex One si basa sulle tecniche di sicurezza di XGen, un mix intergenerazionale di tecniche di difesa dalle minacce che applica in maniera intelligente la tecnologia nel momento adatto. Il prodotto include le capacità di virtual patching, oltre a tecnologie moderne che rilevano e bloccano gli attacchi avanzati, incluse le minacce fileless.

Salvatore Marcis, Technical Director Trend Micro Italia



- **Actionable Insights:** Apex One introduce capacità estese di endpoint detection and response (EDR). Inoltre, si connette al servizio Trend Micro di managed detection and response (MDR), che permette ai team interni un rilevamento e monitoraggio migliori
- **All-in-one:** Apex One potenzia la EDR con strumenti automatici di detection & response, che semplificano il deployment ed eliminano la segregazione tra sistemi, detta "silos"

«Con Apex One rivoluzioniamo la gestione e il controllo della sicurezza informatica, aiutando i clienti ad affrontare le minacce attuali, in modo estremamente funzionale e preciso e con parità di funzionalità per le versioni on-premise e SaaS», ha aggiunto Marcis.

Operativamente Apex One sostituisce OfficeScan. I clienti OfficeScan riceveranno un update gratuito alla soluzione Apex One. Alcune caratteristiche, come le investigazioni EDR potrebbero richiedere però ulteriori licenze. ❁

L'ABBRACCIO MORTALE PER LA SICUREZZA DEI ROOTKIT SCRANOS

Bitdefender ha messo in guardia come il rootkit Scranos sia una minaccia di livello tale che deve indurre le aziende a migliorare il proprio livello di sicurezza

di Giuseppe Saccardi

Una delle principali preoccupazioni delle aziende di oggi è rappresentata dalle minacce sofisticate, e di certo i rootkit sono tra questi. E' un fronte che non lascia di certo tranquilli e i malintenzionati si adoperano con solerzia per inventarsi costantemente nuove modalità di attacco per entrare nelle reti sfruttando punti di ingresso non protetti in ambienti che tra cloud e end user mobili sono sempre più complessi.

In proposito il gruppo dei Bitdefender Cyber-Threat Intelligence Labs ha scoperto le complessità alla base di una nuova operazione spyware multipiattaforma conosciuta come Scranos. Le previsioni relative all'attività di questa campagna basata sullo spyware rootkit Scranos ritengono che avrà la stessa capacità di diffusione dell'adware Zacinlo. Il nome poetico non deve trarre in inganno. Si tratta, mette in guardia Bitdefender, di uno spyware estremamente sofisticato, attivo in gran segreto sin dal 2012 e che ha fruttato a chi l'ha creato notevoli guadagni e compromesso la privacy delle vittime. Il punto dolens è la capacità di sopravvivere su differenti piattaforme, cosa che gli consente di raggiungere

una vasta gamma di endpoint aziendali, soprattutto dispositivi Android.

Un funzionamento particolarmente subdolo

Fingendosi un software o un'applicazione legittima, per esempio lettori di e-book, riproduttori video, driver e con estrema sfacciataggine persino prodotti antimalware, Scranos è parte di un piano più ampio. I malintenzionati che muovono i fili di Scranos apportano poi costantemente leggere modifiche al software, aggiungendo componenti su dispositivi già infetti e migliorando le funzionalità più mature. I criminali informatici per infiltrarsi in un'azienda utilizzano come principali punti di ingresso i suoi dipendenti, considerati e non a torto l'anello più debole della sicurezza informatica aziendale, facilmente raggrigibili, oppure sfruttano gli strumenti di terze parti quali fornitori aziendali più piccoli o meno protetti. Poiché si tratta di una campagna basata su rootkit, Scranos è progettato per nascondersi dalla gestione di sistema e potrebbe facilmente disabilitare i firewall e i tradizionali programmi antimalware in base



alle istruzioni impartite. È persistente e sfrutta le funzionalità di cloaking per ripresentarsi anche dopo essere stato rilevato e rimosso. Dato che l'obiettivo primario è l'esfiltrazione dei dati, la posta in gioco è alta: da problemi legati alla gestione del rischio, al furto di proprietà intellettuale fino al danneggiamento della reputazione di un brand.

Scranos può anche sfruttare l'infrastruttura aziendale per lanciare ulteriori attacchi, cosa che solleva serie preoccupazioni legali e incide sulla reputazione del marchio e, in ultima analisi, sui profitti.

Analizzare l'intero ciclo di vita delle minacce

Il dato di fatto è che per rilevare e bloccare attacchi complessi e contrastare minacce persistenti e mascherate oggi un approccio semplicistico che include firewall e password di otto cifre non è più sufficiente, ciò che è fondamentale, ritiene Bitdefender e si può essere di certo d'accordo con l'azienda, sono funzionalità antiransomware, analisi comportamentale, controllo avanzato delle minacce e machine learning.

Per garantire il livello di flessibilità e scalabilità necessario a soddisfare le esigenze dell'azienda e il crescente numero di "cose" da proteggere, le soluzioni di sicurezza e le attività correlate dovrebbero essere agili. Inoltre, al fine di migliorare il livello di sicurezza generale, le aziende dovrebbero anche perfezionare la loro capacità di rilevamento e risposta alle minacce e prendere in considerazione l'intero ciclo di vita della minaccia.

Gli analisti dei SOC possono ad esempio utilizzare tecnologie che includono le soluzioni Sandbox Analyzer per analisi dettagliate delle minacce sofisticate, Network Traffic Security Analytics per analizzare il traffico di rete e le anomalie del traffico degli endpoint e la tecnologia Hypervisor-based Memory Inspection per identificare le minacce zero-day con la stessa facilità di qualsiasi exploit noto.

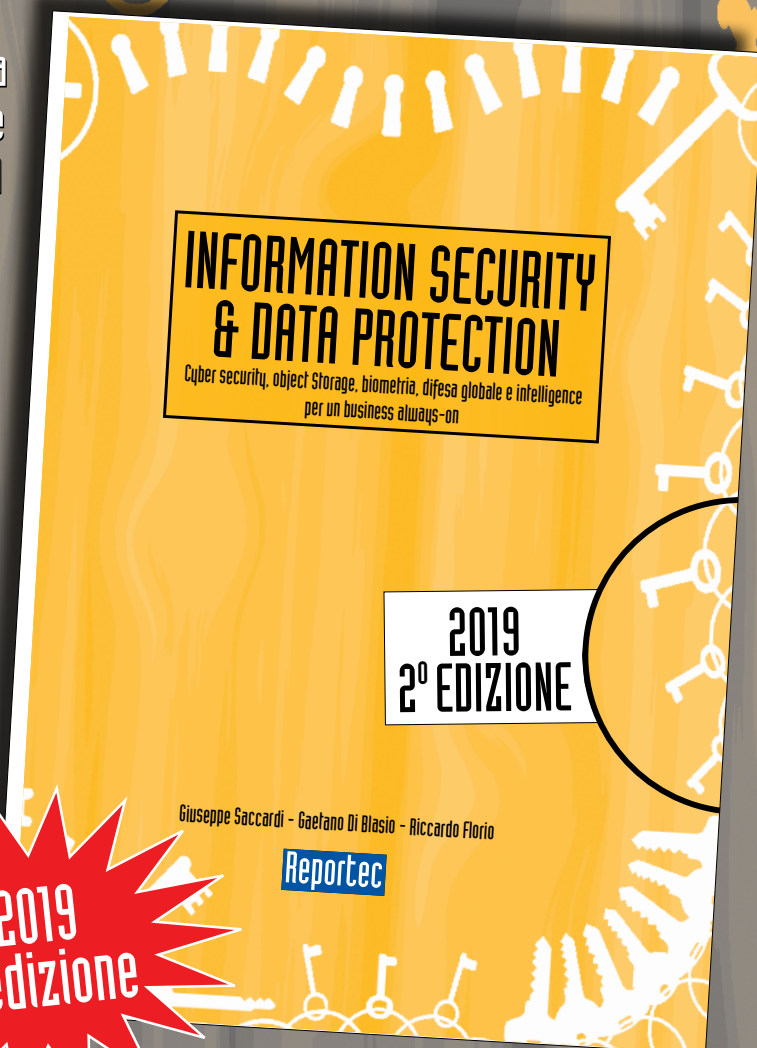
L'analisi degli indicatori di compromissione (IoC)

Gli analisti dei SOC, evidenzia Bitdefender, non solo devono bloccare operazione complesse, ma anche comprendere chi sono gli aggressori che le perpetrano, e automatizzare le risposte per diversi vettori d'attacco. Per farlo, devono poter disporre di dati dettagliati per ottimizzare la caccia alle minacce e ridurre il tempo sprecato a rincorrere "fantasmi". In proposito, nella loro analisi approfondita del funzionamento del rootkit Scranos, i Bitdefender Cyber-Threat Intelligence Labs hanno scoperto centinaia di indicatori di compromissione unici, inclusi gli hash dei file, i domini, le chiavi di registro, gli indirizzi URL e IP.

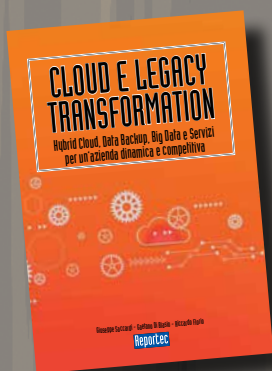
La ricerca sul rootkit Scranos è peraltro solo una parte del loro lavoro quotidiano di studio e analisi delle minacce. Ogni giorno, i soli laboratori Bitdefender analizzano e bloccano circa 600.000 IoC utilizzando diverse tecnologie, tra cui il machine learning, l'euristica avanzata e l'analisi dei contenuti. Si tratta di numeri e di rischi che devono far pensare, e soprattutto agire. ❁

È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**

In oltre 200 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business. Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate. Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.



**2019
2ª edizione**



È disponibili anche
CLOUD E LEGACY TRANSFORMATION

Il libro è acquistabile al prezzo di 30 euro (IVA inclusa) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444