

### CYBER ATTACK

FUCKUNICORN, NUOVO  
RANSOMWARE ITALIANO CHE  
ATTACCA LA SANITA'

### IN QUESTO NUMERO:

#### CYBER ATTACK

*pag. 04*

La sicurezza nel delivery delle App inizia dalla rete

*pag. 06*

Lavoro da remoto e nuove opportunità per gli MSP

*pag. 08*

Nel cloud configurazioni errate prima causa di rischi cyber

*pag. 09*

Fuck Unicorn, nuovo ransomware italiano che attacca la sanità

*pag. 10*

Le mail si confermano un punto critico per la cyber security

*pag. 12*

Ecco come si propaga e colpisce il malware GLUPTeba

#### SOLUZIONI

*pag. 14*

- Governare l'identità per proteggere il perimetro aziendale

*pag. 16*

- Una protezione flessibile difende da minacce in continua evoluzione

*pag. 18*

- Page Integrity Manager contrasta gli attacchi Magecart



# OAD: Osservatorio Attacchi Digitali in Italia

L'OAD, Osservatorio Attacchi Digitali, è l'unica iniziativa in Italia per l'analisi sugli attacchi intenzionali ai sistemi informatici delle aziende e degli enti pubblici in Italia, basata sui dati raccolti attraverso un questionario compilabile anonimamente on line.

Obiettivo principale di OAD è fornire reali e concrete indicazioni sugli attacchi ai sistemi informatici che possano essere di riferimento nazionale, autorevole e indipendente, per la sicurezza ICT in Italia e per l'analisi dei rischi ICT. La disponibilità di un'indagine sugli attacchi digitali indipendente, autorevole e sistematicamente aggiornata (su base annuale) costituisce una indispensabile base per contestualizzare l'analisi dei rischi digitali, richiesta ora da numerose certificazioni e normative, ultima delle quali il nuovo regolamento europeo sulla privacy, GDPR.

La pubblicazione dei rapporti OAD aiutano in maniera concreta all'azione di sensibilizzazione sulla sicurezza digitale del personale a tutti i livelli, dai decisori di vertice agli utenti.

OAD è la continuazione del precedente OAI, Osservatorio Attacchi Informatici in Italia, che ha iniziato le indagini sugli attacchi digitali dal 2008. In occasione del decennale OAD, in termini di anni considerati nelle indagini sono state introdotte numerose innovazioni per l'iniziativa, che includono:

- sito ad hoc come punto di riferimento per OAD e come repository, anno per anno, di tutta la documentazione pubblicata sull'iniziativa OAD-OAI: <https://www.oadweb.it>
- visibilità di OAD nei principali social network: pagina facebook @OADweb, in LinkedIn il Gruppo OAD <https://www.linkedin.com/groups/3862308>
- realizzazione di webinar gratuiti sugli attacchi agli applicativi: il primo, sugli attacchi agli applicativi, è in <https://aipsi.thinkific.com/courses/attacchi-applicativi-italia>
- questionario OAD 2018 con chiara separazione tra che cosa si attacca rispetto alle tecniche di attacco, con nuove domande su attacchi a IoT, a sistemi di automazione industriale e a sistemi basati sulla block chain
- omaggio del numero di gennaio 2018 della rivista ISSA Journal e di un libro di Reportec sulla sicurezza digitale ai rispondenti al questionario OAD 2018
- ampliamento del bacino dei potenziali rispondenti al questionario con accordi di patrocinio con Associazioni ed Ordini di categoria, quali ad esempio il Consiglio Nazionale Forense con i vari Ordini degli Avvocati territoriali
- Reportec come nuovo Publisher e Media Partner
- collaborazione con Polizia Postale ed AgID.



Security & Business 53  
maggio/giugno 2020

Direttore responsabile:  
Gaetano Di Blasio

In redazione:  
Giuseppe Saccardi, Paola  
Saccardi

Hanno collaborato:  
Riccardo Florio

Grafica: Aimone Bolliger  
Immagini: dreamstime.com  
www.securityebusiness.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

## AZIENDE ITALIANE SOTTO ATTACCO, BLOCCATA GEOX, SOTTO PRESSIONE ARUBA E REGISTER

Brutto inizio di giugno per la famosa azienda di Montebelluna, attaccata per la seconda volta con un ransomware. Se ne è parlato anche nelle cronache nazionali e, pertanto, non approfondiamo, limitandoci a evidenziare il supporto della polizia postale. Anche aziende del settore ICT hanno dovuto fronteggiare attacchi di diverso tipo. Aruba e Register hanno infatti resistito a diversi tentativi di bloccare le attività dei clienti, senza registrare danni gravi, se non contiamo brevi periodi di disservizio.

Più pericoloso, ma del quale non abbiamo numeri certi, l'attacco a gruppi di farmacie, che sono state prese di mira con un ransomware di matrice italiana, denominato Fuck Unicorn, nuovo ransomware italiano.

Resta, in sostanza, l'evidente pressione del cybercrime, che non accenna a diminuire.

Diverse analisi aiutano che deve studiare i trend. Per finire, come al solito alcune delle soluzioni presentate di recente dalle aziende della security. Infine vi segnaliamo uno strumento utile: un piccolo assessment sul livello della vostra sicurezza: basta compilare il Rapporto OAD (AOsservatorio Attacchi Digitali) in Italia.

La compilazione è stata ridotta rispetto lo scorso anno e resta totalmente anonima. Al termine avrete un indice della vostra sicurezza.

## LA SICUREZZA NEL DELIVERY DELLE APP INIZIA DALLA RETE

*La rete è indispensabile per la sicurezza e la distribuzione delle applicazioni, ma deve essere più semplice. I suggerimenti di Rodolfo Rotondo di VMware*

*di Giuseppe Saccardi*

È indubbio che la sicurezza sia divenuta una cosa incredibilmente complessa da assicurare a infrastrutture, dati ed applicazioni. Per quanto concerne l'infrastruttura, osserva Rodolfo Rotondo, Senior Business Solution Strategist di VMware, la rete è diventata un canale decisamente critico perché porta i dati dall'origine direttamente agli utenti finali. È in sostanza ciò che connette il data center, i diversi cloud, i sensori IoT che si trovano nell'edge, ovvero tutto ciò che oggi costituisce un'azienda. E' in pratica diventata centrale nel processo di ridefinizione della moderna sicurezza IT ma è con l'affermarsi progressivo di una rete definita dal software che questo è diventato realmente possibile.

Nonostante questa centralità, mette in luce una ricerca di VMware in collaborazione con Forrester, quasi due terzi (57%) dei responsabili IT in EMEA ritiene che sia davvero difficile ottenere una visibilità end-to-end della propria rete.

Tuttavia, i responsabili sembrano riconoscere che questo rappresenti un problema, con quasi la metà di essi che afferma che questa mancanza di visibilità

sia una delle principali preoccupazioni.

Più di un terzo (37%) poi ritiene che le sfide associate a questa mancanza di visibilità abbiano portato a un disallineamento tra i team di sicurezza e quelli IT, e un quarto (29%) non considera la possibilità di implementare una sola strategia per IT e di sicurezza, dato che in Italia raggiunge il 50%.

In ogni caso le aziende riconoscono che la trasformazione della rete sta diventando però essenziale per raggiungere i livelli di resilienza e sicurezza richiesti dalle aziende moderne, con il 43% delle organizzazioni europee che afferma che questa ha rappresentato e rappresenterà per loro una priorità chiave tra il 2019 e il 2021.

Ma, osserva Rotondo, come possono le organizzazioni affidarsi alla forza della rete per proteggere i dati in tutta l'organizzazione, dalla base all'utente finale? Vediamolo in sintesi.

### **Mettere la rete al primo posto**

In primo luogo la collaborazione tra i team competenti è fondamentale. Ad oggi, solo un terzo dei team di networking è coinvolto nello sviluppo di strategie di sicurezza, nonostante il 61% sia coinvolto nella loro esecuzione, il che evidenzia che i team di rete non sono percepiti con un ruolo paritario rispetto ai team IT o di sicurezza quando si tratta di cybersecurity.

Abbattere attivamente questi silos ed eliminare l'attrito tra i team dovrebbe essere considerato una

priorità critica perché solo adottando un approccio olistico è possibile affrontare il sofisticato panorama delle minacce.

### L'esigenza di un approccio intrinseco

Gli approcci tradizionali alla sicurezza erano stati progettati per una realtà diversa ma sono ora applicati a un panorama di minacce ben peggiore e si traducono in una complessità ingestibile e disfunzionale che si basa su troppi prodotti differenti e specifici.

Concentrandosi generalmente sul blocco delle minacce nel perimetro le soluzioni datate sono inadatte al mondo della trasformazione digitale di oggi, dove le infrastrutture devono essere agili e poter mutare e scalare.

«Nel mondo di oggi, definito dal software, è possibile tessere la sicurezza in ogni livello della digital foundation di un'azienda, riducendo significativamente la superficie di attacco esposta ai malware. Si tratta di un approccio più proattivo alla gestione delle minacce poiché non è più necessario essere in grado di riconoscere l'aspetto di queste. Piuttosto che aggiungere complessità, si rendono al contrario le cose più semplici, utilizzando l'infrastruttura software e gli endpoint esistenti dell'organizzazione e consentendo loro di progettare la sicurezza nelle applicazioni e nei dati fin dall'origine», osserva Rotondo, di certo con numerosi punti a favore.



### Pensare alle App moderne

Un altro aspetto da considerare è che le aziende sono in una fase di trasformazione applicativa al fine di guadagnarsi un vantaggio rispetto alla concorrenza e la modernizzazione delle app che utilizzano container e micro servizi rappresenta un approccio allo sviluppo del software che è dominante, e Kubernetes è de facto la piattaforma di orchestrazione dei container.

Questo è il motivo per cui un approccio software-first attraverso una Virtual Cloud Network (VCN) costituisce il punto di partenza ideale per le organizzazioni che vogliono evolvere rapidamente.

«Una VCN è un livello del software che attraversa l'intera infrastruttura del data center e oltre, dai server fisici al cloud pubblico e privato e all'edge. Fornisce alla rete agilità automatizzata, flessibilità e semplicità, consentendo alla stessa di diventare un vero abilitatore dei risultati di business, piuttosto che rappresentare solo un centro di costo. Fornendo una connettività sicura e pervasiva con la velocità e l'automatizzazione del software, una VCN contribuisce a bandire i silos e migliorare notevolmente la gestione dei problemi di sicurezza dell'azienda. La sicurezza della rete contribuisce positivamente alla competitività aziendale senza più essere solo un centro di costo poco efficiente», evidenzia Rotondo. In sintesi, la rete rappresenta il tessuto che realizza la connettività, la sicurezza intrinseca e la consegna delle applicazioni. Va quindi usata come una sorta di arma strategica, e non solo come un semplice impianto infrastrutturale.



# LAVORO DA REMOTO E NUOVE OPPORTUNITÀ PER GLI MSP

*Nel corso della giornata annuale degli MSP Barracuda ha presentato l'ultimo rapporto che analizza le opportunità e le sfide per il settore dei servizi gestiti*

*di Giuseppe Saccardi*

Lo scorso 21 maggio si è celebrata la terza giornata mondiale degli MSP, movimento lanciato da Barracuda nel 2018 per sostenere il settore dei servizi gestiti e i cambiamenti e le sfide che questo incontra ogni anno. In occasione dell'evento la società ha presentato l'ultimo rapporto dal titolo "The Evolving Landscape of the MSP Business Report 2020" ([https://barracudamsp.com/resources/pdf/reports/RP\\_MSP-Day-2020.pdf](https://barracudamsp.com/resources/pdf/reports/RP_MSP-Day-2020.pdf)).

Per l'MSP Day di quest'anno, la Computing Technology Industry Association (CompTIA), voce di spicco e sostenitrice dell'ecosistema globale IT, si è unita a Barracuda per il primo evento virtuale per la giornata degli MSP. Miles Jobgen, Director of Member Communities di CompTIA, ha affiancato Jason Howells, Director International MSP di Barracuda, e Neal Bradbury, VP MSP Strategic Partnership, per discutere il rapporto di quest'anno, oltre a presentare una serie di video e dibattiti sullo stato del settore.

Il report del 2020 ha approfondito l'analisi del mercato globale degli MSP nel momento in cui ai partner di canale di tutto il mondo è stata offerta l'opportunità di rafforzare la propria offerta di soluzioni di sicurezza per supportare la crescita della forza lavoro mobile, più vulnerabile, emersa a causa della pandemia da coronavirus.

Sono stati intervistati quasi 300 MSP globali coinvolgendo i paesi del Regno Unito, Stati Uniti, Germania, Canada, Irlanda, Belgio, Australia e Spagna. I risultati hanno rivelato che, indipendentemente dalla posizione, gli MSP in tutto il mondo si trovano ad affrontare sfide simili quando si tratta di approvvigionamento e opportunità di crescita relativamente alle future offerte di sicurezza.

«Dal lancio di MSP Day e del relativo report Evolving MSP Landscape, abbiamo assistito a un costante aumento della richiesta di servizi gestiti in tutto il mondo, il che è evidente nei risultati di quest'anno – ha dichiarato Brian Babineau, Senior VP e General Manager, MSP Solutions Barracuda -. Tra queste necessità, la sicurezza è il servizio più richiesto, in particolare data la attuale situazione globale e la volontà dei criminali informatici di sfruttare aziende che sono diventate improvvisamente molto più vulnerabili».



*Brian Babineau, Senior VP e General Manager, MSP Solutions Barracuda*

## Top ranking managed services according to MSPs.

2020	%	2019	%
1. Backup, Business Continuity and DR	59%	1. Network Monitoring and Management	76%
2. Network Monitoring and Management	41%	2. Backup, Business Continuity and DR	65%
3. Productivity Apps (eg Microsoft 365)	38%	3. Network Security	63%
4. Network Security	35%	4. Productivity Apps (eg Microsoft 365)	59%
5. Endpoint Security	31%	5. Cloud-based Infrastructure	59%

Security e Network Security sono tra i primi cinque servizi nella tabella dei top 5 per il 2020. Al contrario, nel 2019 la

### I principali dati emersi

Dal report sono emersi interessanti risultati che consentono di delineare quali saranno gli scenari futuri e le principali sfide e opportunità per il settore dei servizi gestiti. In particolare è emerso che:

- La maggioranza degli MSP prevede di espandere il proprio portafoglio di servizi nel 2020. Un significativo 91% degli MSP ha dichiarato di avere in programma di aumentare l'ampiezza e la capacità dei propri servizi nei prossimi 12 mesi.
- I servizi gestiti sembrano essere il principale generatore di fatturato per la stragrande maggioranza degli intervistati. Il 69% degli intervistati ha identificato nei servizi gestiti la più grande opportunità per aumentare le vendite nel 2020. Questa percentuale è aumentata significativamente rispetto al 2019, quando soltanto il 54% segnalava i servizi gestiti come la migliore opportunità.
- Gli MSP favoriscono un approccio ibrido ai servizi. Il 53% degli intervistati prevede di generare oltre la metà (51%) o più della propria attività attraverso i servizi gestiti nel 2020, con circa un altro 45% che prevede di generare fino al 50% del business attraverso i servizi gestiti.
- I servizi di sicurezza sono in cima alle priorità degli MSP quest'anno. Endpoint Security, Email

sicurezza della posta elettronica era l'unico servizio di sicurezza che si era posizionato fra i primi 5.

- I crescenti problemi di sicurezza e la mancanza di competenze tra gli utenti finali stanno alimentando la richiesta di fornitori di servizi terze parti. Una maggioranza pari al 79% degli MSP ha ritenuto che le preoccupazioni dei clienti relative alla sicurezza fossero una buona opportunità, in particolare con l'aumento dei lavoratori da remoto. Il 72% afferma che la mancanza di competenze di sicurezza interne tra i propri clienti sta creando nuove possibilità di entrate.
- La stragrande maggioranza concorda sul fatto che la domanda di servizi di sicurezza gestiti è in aumento. L'88% degli intervistati ha affermato che la domanda di servizi di sicurezza è "moderatamente" o "significativamente" in crescita. «La sicurezza come servizio gestito diventerà sempre più richiesta dal momento che le imprese continueranno a far fronte alla carenza di competenze e si adegueranno alle nuove condizioni di lavoro, offrendo agli MSP un'enorme opportunità per rafforzare la loro offerta e consolidarsi ulteriormente come partner vitali per la loro base clienti» ha commentato Carolyn April, Senior Director, Industry Analysis presso CompTIA. ❖

# NEL CLOUD CONFIGURAZIONE ERRATE PRIMA CAUSA DI RISCHI CYBER

*Una ricerca Trend Micro evidenzia come minacce e falle nella security, in diverse aree chiave, mettano a rischio dati sensibili e segreti aziendali*

di Giuseppe Saccardi



**N**egli ambienti cloud, gli errori di configurazione sono la prima causa di criticità legate alla cybersecurity e ogni giorno sono 230 milioni, in media, le problematiche di questo tipo.

Il dato emerge dall'ultima ricerca Trend Micro dal titolo "Exploring Common Threats to Cloud Security". Lo studio rende pubblici i numeri di Trend Micro Cloud One - Conformity, la piattaforma dedicata alla protezione degli ambienti cloud.

Secondo Gartner, nel 2021, oltre il 75% delle aziende medio grandi avrà adottato una strategia IT multi-cloud o ibrida[1]. Nel momento in cui le piattaforme cloud diventano prevalenti, l'IT e i team DevOps devono far fronte a preoccupazioni maggiori e incertezze legate al mettere al sicuro le infrastrutture cloud.

«Le operazioni cloud-based sono diventate la norma piuttosto che l'eccezione e i cybercriminali si sono adattati per capitalizzare gli errori nella configurazione o gestione degli ambienti cloud - ha affermato Salvatore Marcis, Technical Director Trend Micro Italia -. Le organizzazioni devono cambiare il modo

in cui pensano alla sicurezza del cloud, non come qualcosa che viene affrontato a posteriori, ma come parte integrante di un'implementazione cloud ben progettata e Trend Micro aiuta le organizzazioni ad avere successo in questo processo».

La ricerca ha riscontrato minacce e falle nella security in diverse aree chiave degli ambienti cloud, che mettevano a rischio dati sensibili e segreti aziendali. I cyber criminali che hanno voluto trarre profitto dagli errori di configurazione degli ambienti cloud, hanno attaccato le aziende con ransomware, cryptomining, s3-bucket exploit e data exfiltration. Sono stati trovati anche dei tutorial online fuorvianti che hanno aggravato il rischio in alcune aziende, portando a situazioni di credenziali e certificati cloud mal gestiti.

I team IT possono sfruttare gli strumenti cloud native per mitigare questa tipologia di rischi, ma non dovrebbero fare affidamento esclusivo su questi tool. Cosa fare per mettere al sicuro gli ambienti cloud? Quello che suggerisce Trend Micro è di:

- Adottare controlli con privilegi minimi -Restringere

- Comprendere il modello di responsabilità condivisa - Nonostante i provider cloud abbiano una built-in security, i clienti sono responsabili per la sicurezza dei propri dati
- Monitorare i sistemi mal configurati ed esposti - Strumenti come Trend Micro Cloud One—Conformity

- Integrare la security nella cultura DevOps - La sicurezza deve essere inclusa nei processi DevOps dall'inizio dello sviluppo software, correggere rischi di sicurezza durante il processo di sviluppo è molto meno oneroso che farlo a posteriori. ❖

## FUCKUNICORN, NUOVO RANSOMWARE ITALIANO CHE ATTACCA LA SANITÀ

### *A rischio anche falsi curricula e moduli di permesso per malattia*

di Gaetano Di Blasio

Con un nome che è tutto un programma, il nuovo ransomware FuckUnicorn sfrutta le email a tema Covid-19 per veicolare il malware attraverso un link che atterra su un dominio maligno, apparentemente simile al sito della Federazione Italiana Farmacisti.

Più precisamente, secondo quanto rivelato dai ricercatori di Check Point Software Technologies, convinti che il malware sia stato sviluppato da italiani, il link rimanda a un'applicazione per pc relativa al covid.

### **Più poveri e vulnerabili**

Gli esperti hanno inoltre rilevato altri attacchi: in particolare quelli che sfruttano falsi moduli di congedo o malattia e finti curricula, soprattutto negli



USA, per diffondere Trojans e infostealer con target relativo al mondo bancario, usando i file .xls. Inoltre, presso Check Point Software Technologies hanno scoperto una campagna dannosa che utilizza il malware Zloader per trafugare le credenziali delle vittime e altre informazioni. Zloader è un trojan bancario e una variante del famigerato malware Zeus che si rivolge specificamente ai clienti degli istituti finanziari.

Lo scenario che giunge dagli Stati Uniti, peraltro, lascia intendere che gli attacchi potrebbero ulteriormente intensificarsi considerata la crisi mondiale.

Lo scorso maggio la CNN ha riferito che da quando la pandemia di coronavirus ha congelato l'economia statunitense, oltre 40 milioni di statunitensi hanno chiesto per la prima volta il sussidio di disoccupazione, ma, nello specifico, circa il 25% degli americani lo ha chiesto durante la pandemia. Un dato più alto di sempre, Grande Depressione degli anni Trenta compresa.

Gli attacchi malware generici crescono man mano che le imprese riaprono.

Piccola consolazione: si è registrato un aumento del numero di attacchi legati ai coronavirus, nel complesso si è registrata una diminuzione del numero totale di attacchi.

"Al culmine della pandemia, in marzo, si è registrato una diminuzione del 30% degli attacchi malware rispetto a gennaio 2020.

È stata la conseguenza del lockdown: in molti paesi la maggior parte delle aziende sono state chiuse, riducendo notevolmente il numero potenziale di obiettivi per gli aggressori.

Così come tutti alzano la testa per riprendere il lavoro, anche i cyber criminali hanno intensificato le loro attività. A maggio i ricercatori di Check Point Software Technologies hanno infatti osservato un aumento del 16% degli attacchi informatici rispetto al periodo tra marzo e aprile, quando il coronavirus era al suo apice." ❖

## LE MAIL SI CONFERMANO UN PUNTO CRITICO PER LA CYBER SECURITY

*Gli hacker, allerta Check Point, inviano e-mail di phishing inerenti il training per il COVID-19 o sondaggi su #BlackLivesMatter.*

*di Giuseppe Saccardi*

I ricercatori di Check Point Software Technologies mettono in guardia dal fatto che i criminali informatici stanno approfittando del rientro in ufficio autorizzato dalle aziende: mentre si conducono webinar e corsi di formazione per aggiornare i dipendenti sulle nuove misure sanitarie.

Gli hacker utilizzano queste iniziative come strumento per la distribuzione di e-mail di phishing e malware.

Un'altra conseguenza del ritorno a una "nuova normalità" è che i criminali informatici utilizzano i titoli di notizie importanti come esca per le loro truffe, attraverso attività di hijacking.

Un esempio è legato al movimento "Black Lives Matter". All'inizio di giugno, quando le proteste hanno raggiunto il loro apice a livello globale, i ricercatori di Check Point hanno scoperto una campagna spam legata proprio a tali notizie.

Le e-mail hanno distribuito il malware Trickbot come

file doc, con oggetto delle mail quali “Dai la tua opinione confidenziale sul tema Black Lives Matter”, “Lascia una recensione anonima su Black Lives Matter” o “Vota anonimamente su Black Lives Matter”.

«I dipendenti di tutto il mondo dovrebbero essere prudenti quando aprono e-mail e documenti, assicurandosi che siano inviati da una fonte legittima all'interno della loro azienda. Ultimamente, stiamo assistendo a una tendenza degli hacker di sfruttare nomi ben noti, come Microsoft Office 365, per ingannare i dipendenti. Una cosa è certa: la pandemia da Coronavirus ci sta portando verso un'altra pandemia, quella informatica», ha commentato David Gubiani, Regional Director SE EMEA Southern di Check Point.

### **I paesi a rischio**

Gli ultimi dati di Check Point mostrano che il grado di rischio che un'azienda venga presa di mira da un sito web dannoso collegato

al Coronavirus dipende dal fatto che il Paese in cui ha sede sia tornato in attività o sia ancora in isolamento.

In regioni come l'Europa e il Nord America, dove si accenna una ripresa economia, è stata registrata una forte diminuzione della percentuale di organizzazioni che hanno subito l'impatto di tali siti web dannosi.

In regioni come l'America Latina e l'Africa, che sono ancora nel pieno della pandemia, vi sono continui e crescenti casi di aziende che vengono colpite da attacchi dannosi legati al Coronavirus.

### **I rischi del ritorno alla “nuova normalità”**

Per preparare i dipendenti alla cosiddetta “nuova normalità”, molte organizzazioni hanno predisposto webinar e brevi corsi di formazione per spiegare le restrizioni e i requisiti per le operazioni post pandemiche.

Check Point ha rilevato la presenza di cyber criminali che distribuiscono e-mail di phishing e file dannosi camuffati da materiale per i training anti Covid-19. Mail che cercano di adescare la vittima per indurla



*David Gubiani, Regional Director SE EMEA Southern di Check Point*



a iscriversi a un finto corso di formazione per dipendenti che porta effettivamente a un sito web dannoso.

### Attenzione ai Curriculum Vitae

A causa dell'aumento della disoccupazione i ricercatori di Check Point hanno notato anche un aumento degli attacchi informatici negli Stati Uniti e in Europa, dove i file dannosi erano CV fasulli.

In giugno, l'azienda israeliana ha riportato un aumento settimanale del 20% degli attacchi informatici basati su CV già a partire da maggio, uno su 370 file. Una tendenza simile si può osservare anche in altre parti del mondo: a partire da maggio, il numero di truffe settimanali sui CV è raddoppiato a livello globale nel mese di giugno, con un allegato malevolo su 1.270.

### Come rimanere protetti

Due sono i modi che Check Point suggerisce per proteggere una organizzazione dalle minacce di phishing.

La prima consiste nell'implementare una soluzione di sicurezza e di prevenzione per la posta elettronica che sia in grado di identificare e bloccare gli attacchi di phishing avanzato prima che raggiungano le caselle di posta degli utenti.

La seconda è quella di educare i dipendenti. Oltre a istruirli sui possibili attacchi e sulle conseguenze, Check Point consiglia di condividere costantemente informazioni aggiornate sulle tendenze attuali degli attacchi di phishing e di tenere aggiornati i dipendenti sui recenti tentativi di phishing - anche verso l'organizzazione stessa.

Più i collaboratori sono consapevoli di queste truffe, e meno sono inclini a diventarne vittime. ❖

## ECCO COME SI PROPAGA E COLPISCE IL MALWARE GLUPTTEBA

*I SophosLabs hanno spiegato come il malware Glupteba si sia evoluto in una rete di distribuzione di malware difficile da intercettare*

*di Giuseppe Saccardi*

Una delle tendenze più evidenti quando si parla di criminalità informatica è la mercificazione degli attacchi: pagando, i cybercriminali possono

aver accesso a qualunque strumento possa loro servire, incluse reti di dispositivi infetti che possono essere sfruttate per la diffusione di contenuti dannosi. I SophosLabs (sophos.com) hanno pubblicato in proposito un nuovo rapporto "Glupteba malware hides in plain sight" in cui viene evidenziato come Glupteba si sia evoluto in una rete di distribuzione di malware estremamente pericolosa e difficile da intercettare. Va osservato che il bot Glupteba è un malware sofisticato che crea backdoor con pieno accesso ai

dispositivi infetti che a loro volta vengono aggiunti alla sua botnet, peraltro in continua crescita.

I criminali informatici diffondono Glupteba attraverso AInjection su siti web legittimi, per poi sfruttarlo al fine di diffondere browser stealer o router exploiter.

Il rapporto dei SophosLabs spiega in modo approfondito le tecniche (TTP) utilizzate da Glupteba per eludere i sistemi di sicurezza e continuare il proprio attacco indisturbato.

Lo scopo principale di Glupteba è quello di infettare un computer al fine di installare malware senza che vengano prontamente rilevati.

Una volta fatto diventa possibile estrapolare una elevata quantità di dati del dispositivo, tra cui le informazioni di configurazione memorizzate, il numero BUILD del sistema operativo, il numero di serie della scheda madre, l'indirizzo MAC, il numero di serie dell'unità disco, la data di installazione del sistema operativo o della RAM.

La cosa preoccupante, osserva Sophos, e non è difficile essere d'accordo, è che gli sviluppatori di

Glupteba hanno dedicato le proprie energie ad assicurarsi che la loro creazione possa eludere i sistemi di rilevamento in diversi modi, ad esempio aggiungere Glupteba alle liste di esclusione dei Windows Defender, aggiornare, riavviare e camuffare i processi malevoli, o utilizzare la blockchain dei bitcoin per aggiornare segretamente gli indirizzi dei server di comando e controllo del bot.

«I più astuti cybercriminali progettano il loro malware in modo da farlo passare assolutamente inosservato. Per farlo, raccolgono il maggior numero di informazioni per impostare le proprie mosse e affinare le loro tecniche. Mentre analizzavamo Glupteba, ci siamo resi conto che gli hacker che gestiscono il bot investono una grande quantità di tempo ed energie per l'autodifesa. Inoltre, Glupteba è stato progettato per essere generico, in grado di implementare una vasta gamma di diverse attività dannose attraverso i suoi diversi componenti e le sue ampie funzioni di backdoor», ha spiegato, Luca Nagy, security researcher di Sophos e autore principale del report. ❖



## GOVERNARE L'IDENTITÀ PER PROTEGGERE IL PERIMETRO AZIENDALE

*Una governance efficace dell'identità indirizzata a fornire privilegi minimi è l'unico modo per implementare politiche di accesso capaci di garantire la compliance e ridurre proattivamente i rischi*

di Riccardo Florio

Per un'azienda i dati rappresentano la risorsa più preziosa il cui accesso viene stabilito in base all'identità di utenti e dispositivi, sia interni sia esterni. Predisporre un sistema di gestione delle identità ha, pertanto, un valore strategico per la gestione e la protezione di queste risorse.

### **Identità: il nuovo perimetro da proteggere**

Nel corso del tempo diversi modelli di protezione sono stati elaborati per garantire una protezione efficace.

Un grande successo ha riscosso l'approccio denominato Defense in depth, focalizzato prevalentemente nel rafforzamento delle risorse per prevenire gli attacchi provenienti dall'esterno del firewall.

Questo tipo di approccio andava bene in un contesto in cui la protezione doveva essere esercitata all'interno di un perimetro aziendale definito e circoscritto. Oggi questo perimetro non esiste più.

A farlo scomparire hanno contribuito: nuovi modelli di lavoro che richiedono di poter accedere alle

risorse aziendali sempre, ovunque e da qualsiasi dispositivo; requisiti di maggiore agilità che portano a condividere informazioni aziendali con partner, fornitori e persino clienti, delocalizzazione dei dati in uno scenario tecnologico dominato dal cloud e orientato ai servizi.

Peraltro, un approccio difensivo concentrato esclusivamente sugli attacchi esterni lascia esposta l'azienda alle minacce provenienti dall'interno che si sono dimostrate, nel tempo, tra le più insidiose e dannose. Non è in grado, neppure, di contrastare nuove modalità di attacco, come gli APT, che prevedono un processo di infiltrazione lento e progressivo in cui l'attaccante riesce a operare all'interno dell'azienda in modo inosservato per lungo tempo, continuando a scalare nel livello di accesso.

Il nuovo perimetro aziendale da proteggere si chiama identità e il modello più adatto per garantire una sicurezza efficace è Zero Trust.

### **La sicurezza Zero Trust**

Il modello di sicurezza Zero Trust sta incontrando una crescente adozione proprio perché è pensato per rispondere alla complessità dell'ambiente moderno e proteggere persone, dispositivi, applicazioni e dati ovunque si trovino.

Il fondamento di questo approccio è che non esista una condizione in cui la fiducia affidata a dipendenti e partner per connettersi tra loro e collaborare possa travalicare i confini delle risorse minime

*Pierpaolo Ali, Director  
Southern Europe Security,  
Risk & Governance di Micro  
Focus*



strettamente necessarie per svolgere il proprio lavoro.

Questo è un tema ancora più rilevante quando si ha a che fare con utenti che godono di ampi privilegi.

Per esempio, fornire all'amministratore delegato di un'azienda privilegi di accesso illimitati, incusa la possibilità di accedere a risorse aziendali che non gli servono per svolgere il proprio lavoro (come progetti tecnici coperti da segreto industriale), presuppone che disponga delle competenze per proteggere adeguatamente i suoi dispositivi e le sue credenziali di accesso: cosa generalmente non vera.

Per abilitare un modello di sicurezza Zero Trust capace di garantire la protezione senza diventare, nel contempo, un collo di bottiglia per lo svolgimento della attività lavorative è necessario predisporre una soluzione di identity governance come quella proposta da Micro Focus.

«Operare in sicurezza con una forza lavoro distribuita è diventato una necessità per la maggior parte delle aziende - osserva Pierpaolo Ali, Director Southern Europe Security, Risk & Governance di Micro Focus -. In pochi mesi abbiamo osservato anni di innovazione accelerando il passaggio da un modello ideale ad una necessità. L'architettura "Zero Trust" di Micro Focus offre alle aziende flessibilità, sicurezza e capacità di adattamento» .

### **Micro Focus NetIQ Identity Governance**

Micro Focus NetIQ Identity Governance è la soluzione che aiuta le aziende a realizzare efficaci campagne di certificazione dell'accesso e a implementare controlli di identity governance per rispondere alle esigenze di compliance e ridurre proattivamente i rischi

Questa soluzione mette a fattor comune tutte le informazioni sui diritti degli utenti legate a sistemi, applicazioni e dati per verificare se i privilegi di accesso esistenti sono appropriati e avviare eventuali azioni di revoca. In base all'analisi è possibile, in modo automatizzato, revocare rapidamente l'accesso alle risorse di cui gli utenti non hanno bisogno, per esempio nelle situazioni in cui i dipendenti cambiano posizione in azienda e accumulano inavvertitamente troppi privilegi.

Rispetto ad altre soluzioni analoghe Micro Focus NetIQ Identity Governance è in grado di esercitare una governance adattativa ovvero capace di adattarsi in tempo reale ai cambiamenti e agli eventi, per garantire una costante riduzione del rischio.

NetIQ Identity Governance permette di predisporre una serie di processi finalizzati a creare le condizioni per una corretta gestione dell'identità esercitabile tramite NetIQ Identity Manager.

### **Micro Focus NetIQ Identity Manager**

Micro Focus NetIQ Identity Manager è un framework centralizzato per gestire le identità degli

utenti attraverso il loro intero ciclo di vita all'interno di infrastrutture ibride.

Identity Manager automatizza le attività richieste per prendere le decisioni relative agli accessi, tra cui il provisioning dei privilegi minimi, il processo automatizzato di confronto e allineamento continuo tra i dati di accesso presenti nei sistemi IT e i permessi idonei, il de-provisioning e le opzioni

self-service per le richieste e le approvazioni degli accessi.

Inoltre, grazie a Micro Focus NetIQ Access Manager la gestione dell'accesso viene estesa con funzionalità di Single Sign-On su Web mettendo a disposizione un unico accesso sicuro a intranet e applicazioni basate su cloud da qualsiasi luogo, per qualsiasi utente e tramite qualunque dispositivo. ❖

# UNA PROTEZIONE FLESSIBILE DIFENDE DA MINACCE IN CONTINUA EVOLUZIONE

*FINIX ha reso disponibili soluzioni che difendono le infrastrutture IT e controllano la fruizione degli spazi commerciali in aderenza alle normative anti Covid*

*di Giuseppe Saccardi*

**N**ell'attuale contesto lavorativo, in cui la necessità di rispondere all'emergenza sanitaria ha spinto all'adozione dello smart working, è di vitale importanza la tutela della sicurezza dei dispositivi e dei dati e, non ultimo, il controllo degli spazi fisici per quanto riguarda le persone che li frequentano. «Nel campo della sicurezza informatica e della digital transformation la nostra azienda può vantare, da un lato, le soluzioni di Fujitsu, di cui siamo gli unici distributori in Italia, dall'altra l'esperienza maturata dalla capillare presenza sul territorio e un canale indiretto di vendita con una storia pluridecennale.

Con particolare riferimento alla nostra offerta in ambito security, il nostro obiettivo è di ampliarla con soluzioni di innovative aziende italiane e internazionali», ha osservato Danilo Rivalta, CEO di FINIX Technology Solutions.

Quello della cybersecurity è di certo un campo dell'IT che necessita di soluzioni innovative. Basta considerare che a marzo 2020 i soli attacchi ransomware sono aumentati del 148% rispetto al mese precedente; ed è in questa arena che FINIX (finix-ts.com) si propone di assumere un ruolo primario.

«In questi mesi abbiamo lavorato per individuare le migliori soluzioni di cybersecurity da offrire alle imprese e ai clienti nazionali: è il caso di Morphisec, per la protezione del punto più vulnerabile di una azienda, l'endpoint, che rappresenta l'elemento più critico di una soluzione di smart working. La soluzione che proponiamo rende l'endpoint praticamente inattaccabile ed è stato nominato 2020 Technology Pioneer dal World Economic Forum», ha evidenziato Rivalta.

## Morphisec, il futuro della sicurezza avanzata

Morphisec è una soluzione che affronta il problema della sicurezza informatica con un approccio di nuova concezione - Moving Target Defense (MTD) - in grado di proteggere l'intera organizzazione end-to-end da minacce avanzate come attacchi fileless e zero day, exploit in-memory e ransomware avanzato. Di derivazione militare, opera in base all'assunto che un target in movimento è più difficile da attaccare di uno fisso e sfrutta lo spostamento, la distribuzione e la crittografia dinamica dei dati in memoria per renderne più difficile l'attacco o il furto.

La maggior parte delle soluzioni di antivirus presenti sul mercato si focalizzano su un processo che prevede prima il riconoscimento della minaccia e solo successivamente il blocco della stessa. Morphisec al contrario, osserva FINIX, prima ancora di identificare il tipo di minaccia, le blocca attraverso la citata tecnologia brevettata MTD, in grado di trasformare lo spazio di memoria, spazio che, in quanto statico, costituisce il principale obiettivo degli attacchi evoluti.



*Danilo-Rivalta - CEO  
di FINIX Technology  
Solutions*

*Ulisse mantiene sotto  
controllo gli spazi,  
la temperatura e il  
comportamento dei  
visitatori*



## Prevenire le minacce

La peculiarità di Morphisec risiede nell'approccio attivo nella prevenzione delle minacce tramite la trasformazione continua dello spazio di memoria. Numerosi i benefici che apporta:

- **Blocco di minacce avanzate e zero-day:** Previene zero-day e attacchi avanzati senza la necessità di una conoscenza preliminare della forma, del tipo o del comportamento della minaccia.
- **Applicazione di patch virtuali:** Protegge l'infrastruttura dagli exploit della vulnerabilità quando le patch non sono ancora disponibili.
- **Protezione unica delle infrastrutture IT:** protegge dagli attacchi server Windows e Linux, endpoint, desktop virtuali come VMware Horizon View e Citrix e carichi di lavoro in cloud.
- **Implementazione semplice:** l'implementazione non presenta conflitti di sistema o di manutenzione, non richiede di configurare o aggiornare database, firme o regole, log o avvisi da analizzare.
- **Nessun impatto sul sistema:** opera come agent stateless leggero con ingombro minimo, privo di componenti run-time e di conseguenza senza impatto sulle prestazioni.

«Morphisec porta all'interno della cybersecurity un concetto innovativo puntando sulla prevenzione contro gli attacchi più evoluti, inclusi gli APTs, zero day e ransomware. Ha il vantaggio di poter essere implementata facilmente nell'infrastruttura di sicurezza esistente di un'azienda per costituire uno stack di prevenzione semplice e altamente efficace», ha osservato Rivalta.

### **Ulisse controlla gli spazi e i rischi sanitari del retail**

Se con Morphisec si è proposta di controllare i rischi cibernetici, con la soluzione Ulisse FINIX ha pensato al controllo ambientale e dei rischi sanitari.

Nella sua essenza, Ulisse è una soluzione sviluppata per supportare le aziende che hanno esigenze di controllo accessi e, al tempo stesso, ottenere più informazioni possibili nell'analisi dei dati relativi al comportamento dei visitatori e facendo leva sull'IoT e l'AI.

Nell'attuale situazione – in cui banche, negozi, uffici e servizi ad alta affluenza si trovano a dover affrontare sfide significative – gli ingressi sicuri e contingentati sono diventati un'esigenza impellente

per integrare la ripresa del business con le esigenze di salute pubblica.

A questo si aggiunge una complessità in più per il comparto Retail, che deve integrare tecnologie legacy con lo sviluppo di nuove soluzioni di trasformazione digitale.

Per far fronte a queste esigenze FINIX ha scelto di portare sul mercato la soluzione Ulisse, che poggia su un sistema di analisi dei flussi di persone negli spazi fisici basato su di un modello brevettato.

«L'analisi dei comportamenti all'interno degli spazi, anche commerciali, sarà sempre più fondamentale. Il motore di auto machine-learning in cloud, insieme ai modelli di analisi comportamentale creati sulla base dei dati raccolti giornalmente, analizza questa immensa mole di informazioni e suggerisce azioni migliorative in real time. Per questo motivo siamo particolarmente soddisfatti che una tecnologia come Ulisse sia entrata all'interno del nostro hub di innovazione» ha commentato Rivalta.

Funzionalmente Ulisse utilizza una tecnologia basata su sensori IoT a bassa complessità e algoritmi di Intelligenza Artificiale, mediante i quali è possibile ricavare tutta una serie di KPI propri delle attività



*Ulisse regola gli accessi in sicurezza alle aree*

dei clienti.

I sensori rilevano i flussi di persone tanto all'interno quanto all'esterno di uno spazio fisico, identificano eventi di affollamento e inviano in tempo reale i dati e le coordinate spaziali al sistema di proiezione che, in maniera dinamica, visualizza pattern luminosi o messaggi visuali sul pavimento del negozio.

Il proiettore, integrato nella scocca principale di Ulisse, abilita un sistema di comunicazione dinamica in tempo reale che attraverso mappature di luce suggerisce al visitatore un comportamento adeguato volto a favorire il distanziamento e contingentare gli accessi nel caso in cui ci sia un numero eccessivo di persone.

Una termo-camera, inoltre, permette di implementare un sistema di screening che può rilevare la temperatura sui flussi di visitatori con un margine di errore di 0,5 gradi Celsius. Sistemi di rilevazione della temperatura a distanza sono anche in grado di controllare eventi critici sul territorio per prevenire

il diffondersi di epidemie. Questo tramite un motore di auto-machine learning sul cloud per il consolidamento e l'analisi della vasta quantità di dati raccolti sul campo.

A livello funzionale la soluzione è indipendente dall'infrastruttura IT dei clienti, cosa che si traduce in facilità di implementazione e la disponibilità di configurazioni flessibili

Gli obiettivi di FINIX non si limitano però ad individuare nuove soluzioni ma sono più ampi .

«Il nostro obiettivo è di rafforzare ulteriormente la nostra posizione come centro di eccellenza negli ambiti di Cybersecurity, IoT e Artificial Intelligence. Vogliamo essere un centro di competenza non cattedratico, ma pratico e ricco di contenuti. E farlo anche attraverso scouting di aziende e start-up italiane particolarmente capaci che abbiano ideato o con cui ideare altre soluzioni innovative», ha spiegato Rivalta. ❖

## PAGE INTEGRITY MANAGER CONTRASTA GLI ATTACCHI MAGECART

*La soluzione di Akamai per contrastare i sofisticati attacchi usati per rubare i dati delle carte di credito*

*di Giuseppe Saccardi*

Akamai ha esteso l'Intelligent Edge Platform, per la protezione e la delivery di esperienze digitali, con il nuovo Page Integrity Manager. Si tratta di una, una soluzione di rilevamento delle minacce interne al browser progettata per individuare gli script compromessi che sono utilizzati per rubare i dati degli utenti o per influire negativamente sulle user experience.

Come ci spiegano presso Akamai, resi inizialmente popolari dai gruppi di hacker Magecart, e ora utilizzati da altri criminali, gli attacchi sferrati attraverso gli script di pagine web dannosi sono in aumento e sono diventati una fonte frequente di episodi di violazione dei dati.

Gli esperti di Akamai, aggiungono anche, che, solitamente, un sito web si affida a dozzine di fonti di terze parti, molte delle quali causano l'esecuzione di script nei browser degli utenti. questi script sono fondamentali per garantire le dinamiche user experience che i clienti si aspettano siti web, come ad esempio le pagine contenenti le informazioni sensibili utilizzate per i pagamenti, la gestione degli account e i moduli per l'inserimento di dati personali. Però, i gli addetti alla sicurezza hanno poca visibilità o un controllo ridotto su questi script forniti e gestiti da terze parti.

Per questo Akamai ha progettato Page Integrity Manager in modo di proteggere i siti web dalle minacce Javascript, come attacchi di web skimming, form jacking e Magecart, identificando le risorse più vulnerabili, individuando i comportamenti sospetti e bloccando le attività dannose.

Come ci spiegano presso Akamai, il rilevamento delle attività di script sospetti in tempo reale, consente a Page Integrity Manager di fornire un modo più efficace per sconfiggere gli attacchi alla supply chain difficili da rilevare, come, appunto, Magecart, quando si verificano.

«Il volume degli attacchi di web skimming rimane costantemente elevato in diversi settori, in



particolar modo in quelli retail, media e alberghiero», ha affermato Steve Ragan, Security Researcher di Akamai, aggiungendo: «Negli ultimi sette anni, abbiamo analizzato quasi cinque miliardi di codici Javascript eseguiti su 110 milioni di pagine visualizzate, registrando circa un migliaio di vulnerabilità, nessuna delle quali ha causato il furto di dati sensibili degli utenti».

Recentemente, l'FBI ha segnalato che gli attacchi di web skimming sono stati tenuti sotto controllo per quasi sette anni ma stanno aumentando perché i cybercriminali condividono i malware online diventando così più sofisticati.

Raja Patel, vicepresidente del reparto Products, Web Security di Akamai ha inoltre affermato: «Gli script delle pagine web sono intrinsecamente molto dinamici e gli script di terze parti sono particolarmente opachi, nel senso che creano un nuovo vettore di attacco difficile da contrastare», ha affermato. Page Integrity Manager offre ai nostri clienti la visibilità necessaria per gestire i rischi provenienti dagli script, inclusi quelli dei siti web visualizzati e di terze fino a N parti, con informazioni utili per prendere le decisioni aziendali più appropriate per la loro organizzazione». ❖