# Attacco Kerberos Bronze Bit: ecco perché aggiornare subito i sistemi

Dic 10, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

---

***Comparso il primo Proof of Concept che permette di sfruttare la tecnica per aggirare i sistemi di autenticazione in rete basati su Windows.***

Spesso gli esperti di sicurezza rischiano di essere considerati i "grilli parlanti" del mondo IT. I continui richiami ad applicare gli aggiornamenti, infatti, vengono spesso considerati eccessivi o allarmistici. L'urgenza, in questo caso, è però più che giustificata.

A far scattare l'allarme è un'applicazione pratica di **Kerberos Bronze Bit**, una vulnerabilità scoperta già da qualche tempo e che consentirebbe a un pirata informatico di accedere alle aree riservate delle reti aziendali aggirando **il sistema di autenticazione Kerberos**.

La vulnerabilità (CVE-2020-17049) è in realtà una variante di **Golden Ticket** e **Silver Ticket**, emerse negli anni scorsi. Si tratta di tecniche che permettono di sfruttare gli hash di autenticazione di un sistema compromesso per ottenere l'accesso ad altre macchine nella stessa rete.

Insomma, qualcosa che non consente l'intrusione ai pirati informatici, ma gli rende molto più facile eseguire il movimento laterale all'interno dei sistemi informatici.

Adesso **Jake Karnes**, ricercatore presso **NetSPI**, ha pubblicato

un report in cui descrive le conseguenze pratiche legate alla presenza della falla di sicurezza all’interno dei sistemi.

A rendere più spinosa la questione, però, è che in questo caso gli amministratori IT potrebbero avere maggiori resistenze nell’applicare la patch sviluppata da **Microsoft**.

**Un primo aggiornamento, infatti, era stato rilasciato già lo scorso novembre, ma la sua applicazione aveva creato seri problemi di funzionamento nel sistema di autenticazione e la maggior parte delle aziende aveva disinstallato l’aggiornamento**.

Insomma: il rischio non è solo che la vulnerabilità venga distrattamente percepita come qualcosa di “vecchio” o già corretto, ma anche che gli stessi tecnici preferiscano evitare grattacapi a livello di gestione di Kerberos.

Una scelta davvero rischiosa, considerato che Karnes ha anche sviluppato un Proof of Concept (consultabile a questo indirizzo Internet) per sfruttare la vulnerabilità e, di conseguenza, il suo utilizzo è adesso molto più semplice per chiunque.

Condividi l’articolo

---

Attacco a FireEye: “hanno rubato i nostri strumenti di hacking”

---

**Articoli correlati**

**Altro in questa categoria**

---

https://www.securityinfo.it/2020/12/10/attacco-kerberos-bronze-bit-ecco-perche-aggiornare-subito-i-sistemi/?utm_source=rss&utm_medium=rss&utm_campaign=attacco-kerberos-bronze-bit-ecco-perche-aggiornare-subito-i-sistemi

---

# Attacco a FireEye: “hanno rubato i nostri strumenti di hacking”

Dic 09, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, News, RSS, Scenario 0

---

***Il gruppo di pirati informatici ha violato i sistemi della società di sicurezza. Ora hanno tra le mani il loro arsenale cyber.***

Clamoroso attacco hacker ai sistemi informatici di **FireEye**. Ha confermarlo è la stessa azienda, che con un comunicato stampa

pubblicato sul suo sito Internet spiega di essere stata vittima di una violazione che ha portato al furto di informazioni riservate e degli **strumenti di hacking** utilizzati dai suoi esperti per mettere alla prova i sistemi di cyber security dei clienti.

Stando alle dichiarazioni di **Kevin Mandia**, amministratore delegato di FireEye, gli autori dell'attacco avrebbero utilizzato tecniche estremamente sofisticate, che gli stessi esperti di sicurezza non avevano mai visto usare in precedenza.

Si tratterebbe, quindi, di un attacco mirato che ha sfruttato una strategia elaborata "su misura" per colpire i sistemi di FireEye e che, probabilmente, è stata messa a punto da **un gruppo di professionisti che operano per conto di un governo straniero**.

Insomma: saremmo di fronte a un vero "colpaccio" messo a punto da **un gruppo APT (Advanced Persistent Threat)** che in un colpo solo sarebbe riuscito a mettere le mani sulle informazioni riguardanti i sistemi di protezione delle aziende che collaborano con FireEye e sugli strumenti di hacking che gli esperti dell'azienda usano per i loro penetration test.

**Volendo fare un paragone, è come se un gruppo di rapinatori fosse riuscito a rapinare un commissariato di polizia, rubando armi e informazioni sui sistemi di allarme delle maggiori banche della città**.

Le indagini per ricostruire i dettagli dell'attacco saranno condotte in collaborazione con l'FBI e Microsoft, che per il momento si limita a confermare i sospetti espressi da Mandia sull'attribuzione dell'attacco, considerando probabile che si tratti di un classico "hacking di stato".

Parallelamente alle investigazioni, FireEye ha avviato **un processo di condivisione di tutte le informazioni a sua disposizione con le altre società di sicurezza**, anche nell'ottica di consentire loro di predisporre le difese che conentano di bloccare eventuali attacchi portati con gli strumenti di hacking sottratti all'azienda.

Condividi l'articolo

Attacco Kerberos Bronze Bit: ecco perché aggiornare subito i sistemi Da Leonardo S.p.A. alle case farmaceutiche: raffica di attacchi in Italia

**Articoli correlati**

**Altro in questa categoria**

https://www.securityinfo.it/2020/12/09/attacco-a-fireeye-hanno-rubato-i-nostri-strumenti-di-hacking/?utm_source=rss&utm_medium=rss&utm_campaign=attacco-a-fireeye-hanno-rubato-i-nostri-strumenti-di-hacking

# Da Leonardo S.p.A. alle case farmaceutiche: raffica di attacchi in Italia

Dic 07, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Malware, News, RSS, Scenario 0

***Pirati scatenati: colpito il gigante dell'industria militare, sotto pressione le aziende impegnate nella produzione del vaccino per il Covid-19.***

Un dicembre terribilmente "caldo" per quanto riguarda la cyber security in Italia, investita da una serie di attacchi che stanno mettendo a dura prova gli addetti alla sicurezza

informatica.

Il primo caso che tocca il nostro paese è parte di un’ampia campagna di cyber attacchi che sta interessando aziende ed enti pubblici collegati allo sviluppo e alla produzione del vaccino per il Covid-19.

Come spiegano gli esperti di **IBM Security X-Force** in un report pubblicato su Internet, l’azione dei pirati informatici (che i ricercatori considerano molto probabilmente collegati a un governo) ha preso di mira il settore farmaceutico sfruttando un tema di attualità: la catena del freddo necessaria per conservare e distribuire il vaccino.

Il vettore di attacco usato è il phishing, e in particolare un messaggio di posta elettronica in cui i cyber criminali cercano di impersonare un dirigente della **Haier Biomedical**, un’azienda che risulta essere tra i fornitori dell’iniziativa **Cold Chain Equipment Optimization Platform (CCEOP)**.

Nel dettaglio, il messaggio proveniva da un indirizzo email molto simile a quello legittimo ed è stato inviato a numerosi bersagli tra cui organizzazioni della Commissione Europea e di varie nazioni, tra cui il nostro paese.

A subire pesanti attacchi, però, è stata anche **Irbm Pomezia**,

l’azienda che ha collaborato insieme all’**Università di Oxford** alla creazione del vaccino anti-Covid commercializzato da **AstraZeneca**.

Un capitolo a parte, invece, merita il caso dell’attacco ai danni del sistema informatico di **Leonardo S.p.A.** (ex **Finmeccanica**) emerso in seguito all’iniziativa giudiziaria della **Procura di Napoli**.

Come si legge nel comunicato pubblicato su Facebook (sigh!) dal **Commissariato della Polizia di Stato**, la vicenda risale al periodo 2015-2017, durante il quale l’azienda avrebbe subito un clamoroso furto di dati. **In questo caso, però, si sarebbe trattato di un lavoro dall’interno, i cui esatti contorni non sono ancora chiari**.

L’operazione del Pool Cybercrime della Procura ha portato a due arresti, il primo ai danni di **Antonio Rossi**, attuale responsabile della sicurezza di Leonardo, con l’accusa di **depistaggio**. Il secondo ha coinvolto **Arturo D’Elia**, ex dipendente di Finmeccanica che, secondo i magistrati, sarebbe stato l’autore materiale dell’attacco.

Nel dettaglio. D'Elia avrebbe installato manualmente un trojan su decine di computer: 33 nello stabilimento Leonardo di **Pomigliano D'arco**, 13 in una società del gruppo **Alcatel** e altri 48 in varie aziende attive nel settore aerospaziale.

Insomma: quella configurata dalla Procura di Napoli è un'azione di spionaggio su larga scala che avrebbe coinvolto numerose aziende che operano con le forze armate e il settore pubblico (la stessa Leonardo ha come maggiore azionista il **Ministero dell'economia e delle finanze italiano**) nella produzione di dispositivi estremamente "sensibili".

Nei due anni di attività, il trojan avrebbe esfiltrato 10 GB di dati (100.000 file), presumibilmente frutto di un sistema di keylogging e di un ulteriore modulo in grado di catturare screenshot dei computer infetti.

Lo scarno comunicato stampa di Leonardo (consultabile a questo link) **esclude che tra i dati rubati ci siano informazioni sensibili riguardanti i progetti militari del gruppo**. Per averne la conferma, però, sarà necessario aspettare gli sviluppi dell'inchiesta, che dovrà anche chiarire se la vicenda si inserisca in una caso di spionaggio architettato da un governo straniero.

Condividi l'articolo

---

Come ti rubo la carta di credito con l'icona di Facebook

---

## Articoli correlati

## Altro in questa categoria

---

https://www.securityinfo.it/2020/12/07/da-leonardo-s-p-a-alle-case-farmaceutiche-raffica-di-attacchi-in-

italia/?utm_source=rss&utm_medium=rss&utm_campaign=da-leonardo-s-p-a-alle-case-farmaceutiche-raffica-di-attacchi-in-italia

---

# Come ti rubo la carta di credito con l'icona di Facebook

Dic 04, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

---

***Nuova tecnica per colpire i siti di e-commerce. I pirati inseriscono il codice malevolo nelle icone per la condivisione sui social network.***

L'eterna rincorsa tra cyber criminali ed esperti di sicurezza interessa tutti i campi. Nel settore del furto di dati delle carte di credito, però, sembra che la competizione sia particolarmente feroce. L'ultima trovata dei pirati informatici coinvolge social network come **Facebook**, **Twitter** e **YouTube**.

Come spiegano i ricercatori di **Sansec**, la società di sicurezza informatica che ha segnalato il caso, la nuova strategia sfrutta una tecnica steganografica per nascondere il codice malevolo usato per sottrarre i dati delle carte di credito.

Nel loro report, i ricercatori spiegano che la nuova strategia adottata dai cyber criminali prevede l'uso di un malware che sfrutta due componenti distinti.

Il primo, che contiene il codice in grado di rubare le

credenziali delle carte di credito usate per i pagamenti, è integrato all'interno di icone assolutamente identiche a quelle utilizzate per consentire la condivisione di informazioni sui maggiori social network, come Facebook, Instagram e Twitter.

**Il codice malevolo è opportunamente codificato attraverso algoritmi che ne impediscono la lettura (e l'analisi) da parte dei software antivirus**.

Il secondo componente, che i pirati iniettano in un'altra sezione del sito Web compromesso, contiene il codice che consente di decodificare il modulo principale ed eseguire così il payload che permette di rubare i dati delle carte di credito.

Secondo gli autori del report, i due moduli hanno buone probabilità di ingannare gli strumenti di scansione più diffusi che, analizzando un singolo componente, non riescono a individuarne la potenziale dannosità.

I primi esemplari che sfruttano questa tecnica sono comparsi nello scorso giugno, ma l'uso di questa tecnica (che gli esperti considerano la prima in grado di sfruttare immagini apparentemente "perfette") potrebbe diffondersi nel prossimo futuro, alzando ulteriormente l'asticella nel confronto tra pirati ed esperti di sicurezza.

Condividi l'articolo

Doppia falla in Xerox DocuShare: documenti sensibili a rischio

**Articoli correlati**

**Altro in questa categoria**

https://www.securityinfo.it/2020/12/04/come-ti-rubo-la-carta-di-credito-con-licona-di-facebook/?utm_source=rss&utm_medium=rss&utm_campaign=come-ti-rubo-la-carta-di-credito-con-licona-di-facebook

# Doppia falla in Xerox DocuShare: documenti sensibili a rischio

Dic 03, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

***L'azienda ha rilasciato un aggiornamento per correggere le due vulnerabilità, che avrebbero consentito di accedere ai dati o modificarli.***

Quando una falla di sicurezza fa scomodare la **Cybersecurity and Infrastructure Security Agency (CISA)** statunitense, si può scommettere sul fatto che il bug riguarda uno dei "pezzi grossi" nel mondo business.

Anche questa volta la regola è confermata: **DocuShare** è infatti uno degli strumenti più apprezzati di **Xerox** che, a livello enterprise, rimane uno dei "giganti" nella fornitura di software e piattaforme per la gestione di database e documenti.

Le vulnerabilità, in questo caso, sono due (accorpate come CVE-2020-27177) e interessano le ultime release del software Xerox nelle versioni 6.6.1, 7.0 e 7.5.

**Un pirata informatico in grado di sfruttarle potrebbe, in pratica, accedere ai documenti conservati su un server ed eventualmente modificarli**.

Sui dettagli delle vulnerabilità, in realtà, si sa molto poco. Lo stringatissimo bollettino di sicurezza pubblicato da Xerox si limita a indicare i link per scaricare le patch per le varie versioni su **Linux**, **Windows** e **Solaris** (con eccezione della versione 7.5, che non è compatibile con il sistema operativo Solaris).

I pochi dettagli tecnici emersi parlano di possibili attacchi di tipo **Server-Side Request Forgery (SSRF)** ed **External XML Entity Injection (XXE)**.

Entrambe le tecniche di attacco, come anticipato,

consentirebbero di provocare un “leak” di informazioni e, potenzialmente, consentire a un cyber criminale di “inquinare” i dati contenuti sui server.

Dal momento che DocuShare è utilizzato normalmente da aziende di grandi dimensioni e che le infrastrutture di questo tipo sono spesso estremamente complesse, il richiamo da parte di CISA ha il chiaro obiettivo di sensibilizzare gli amministratori IT per applicare le patch il prima possibile.

Con il clima che si respira in questi mesi, in cui gli attacchi alle aziende e il numero di data breach è aumentato esponenzialmente, bug di questo tipo rischiano di rappresentare la classica goccia che può far traboccare il vaso.

Condividi l’articolo

---

Clamoroso bug in iOS permetteva un attacco “automatico” via Wi-Fi

---

## Articoli correlati

## Altro in questa categoria

---

https://www.securityinfo.it/2020/12/03/doppia-falla-in-xerox-docushare-documenti-sensibili-a-rischio/?utm_source=rss&utm_medium=rss&utm_campaign=doppia-falla-in-xerox-docushare-documenti-sensibili-a-rischio

---

# Clamoroso bug in iOS permetteva un attacco “automatico” via Wi-Fi

Dic 02, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

---

***La vulnerabilità è stata corretta a maggio, ma i dettagli sono stati resi pubblici soltanto adesso per evitare possibili attacchi.***

Il meccanismo della cosiddetta “responsible disclosure” delle vulnerabilità software ha ormai regole condivise da ricercatori di sicurezza e sviluppatori, con la previsione di tempi certi (di solito 60 o 90 giorni) per la pubblicazione degli aggiornamenti e dei dettagli dei bug.

Ci sono casi, però, in cui le cose vanno in modo diverso e i ricercatori stessi accettano di garantire un periodo di “riservatezza” più lungo. È quanto è accaduto nel caso di **un clamoroso bug di iOS** che il ricercatore **Ian Beer** ha deciso di rendere pubblico quasi un anno dopo il rilascio della patch che lo ha corretto.

Il motivo? Molto semplice: la vulnerabilità avrebbe avuto effetti potenzialmente devastanti. Si tratta infatti di un bug nel protocollo **AWDL**, che nei dispositivi Apple gestisce le reti wireless peer to peer e avrebbe consentito di sviluppare exploit in grado di portare attacchi in grado di compromettere i dispositivi senza che sia necessaria alcuna interazione da parte degli utenti.

**In sintesi: la vulnerabilità avrebbe consentito a un pirata informatico cdi creare un worm in grado di trasmettersi automaticamente attraverso il Wi-Fi**.

Nel monumentale report pubblicato sul blog di **Project Zero**, il team di sicurezza targato **Google** di cui fa parte Beer, il ricercatore spiega tutti i dettagli della vulnerabilità, che come viene dimostrato nel video che ha pubblicato su **YouTube** consente di avviare l'esecuzione di codice (in questo caso l'avvio della calcolatrice) in remoto su un iPhone sfruttando il bug.

[embedded content]

La pericolosità della falla della sicurezza, spiega Beer, dipende anche dal fatto che **AWDL opera a livello di kernel** e, di conseguenza, sfruttando il bug è possibile agire sul sistema operativo con privilegi elevati.

Nei sei mesi che il ricercatore ha dedicato allo studio della vulnerabilità, è riuscito a mettere a punto una serie di **Proof of Concept (PoC)** che hanno mostrato le potenzialità di un attacco di questo genere.

**Beer è infatti riuscito a sviluppare prototipi di malware, tra cui uno in grado di accedere a qualsiasi tipo di informazione e documento memorizzati nello smartphone**.

La vulnerabilità, comunicata ad Apple il 29 novembre 2019, è stata corretta con il rilascio della versione **13.1.1** del sistema operativo Apple il 28 gennaio 2020 e, successivamente, con un'altra patch in **iOS 13.5** nel maggio scorso.

La scelta di non divulgare informazioni sul bug, probabilmente, è stata dettata dalla necessità di aspettare che un numero ragionevole di utenti effettuasse l'aggiornamento.

Condividi l'articolo

IceRat: il trojan “virtuale” che sfugge agli antivirus

**Articoli correlati**

**Altro in questa categoria**

https://www.securityinfo.it/2020/12/02/clamoroso-bug-in-ios-permetteva-un-attacco-automatico-via-wi-fi/?utm_source=rss&utm_medium=rss&utm_campaign=clamoroso-bug-in-ios-permetteva-un-attacco-automatico-via-wi-fi

# IceRat: il trojan “virtuale” che sfugge agli antivirus

Dic 01, 2020 Marco Schiaffino In evidenza, Malware, News, RSS 0

***Il malware utilizza una macchina virtuale JavaScript per avviare un PHP che ne esegue il codice. Solo 2 motori antivirus su 3 lo riconoscono.***

Le tecniche di evasione che consentono ai malware di aggirare i controlli degli antivirus sono in costante evoluzione e sfruttano spesso tecniche innovative per eludere le analisi dei programmi di rpotezione. Il caso di **IceRat**, però, è davvero particolare.

Come spiegano i ricercatori di **G Data** in un report pubblicato

sul blog ufficiale della società di sicurezza, il trojan utilizza uno stratagemma che gli consente di sfuggire a un discreto numero di motori antivirus utilizzando **JPHP**.

SI tratta di una implementazione che consente di **eseguire PHP su una macchina virtuale Java** attraverso file in formato **.PHB**, che buona parte degli antivirus non supportano.

Oltre a utilizzare questo stratagemma per aggirare i controlli antivirus, IceRat sfrutta una struttura modulare estremamente complessa, in cui ogni componente esegue operazioni apparentemente innocue, che assumono una funzione dannosa solo se viste nel contesto complessivo.

**La procedura d'installazione di IceRat, inoltre, adotta un trucchetto che sembra essere pensato per "distrarre" la vittima dal vero obiettivo del malware**.

L'installer principale (Browes.EXE) avvia infatti due installazioni. Una di queste è **CryptoTab**, l'altra è

**cheats.EXE**. Il secondo eseguibile è quello che ha come obiettivo il download e l'esecuzione del componente principale del trojan, chiamato klient.EXE.

CryptoTab, invece, è **un browser con funzionalità dedicate al mining di criptovalute** e la sua procedura d'installazione non è occultata in alcun modo. Secondo l'autore del report, la sua installazione sarebbe un semplice diversivo per nascondere la reale attività del trojan.

Il modulo principale del malware è composto da numerosi eseguibili che hanno scopi diversi: il primo è in grado di sottrarre informazioni da numerosi browser. L'elenco completo comprende i più diffusi come **Chrome** e **Firefox**, ma anche software meno noti come **Amigo**, **kometa** e **Orbitum**.

Un altro eseguibile ha invece funzioni di miner (separate da quelle di CryptoTab) che consentono all'autore del trojan di sfruttare la potenza di calcolo del PC infetto per generare criptovaluta a insaputa della vittima.

Condividi l'articolo

---

Quando l'Intelligenza Artificiale diventa una minaccia

**Articoli correlati**

**Altro in questa categoria**

https://www.securityinfo.it/2020/12/01/icerat-il-trojan-virtuale-che-sfugge-agli-antivirus/?utm_source=rss&utm_medium=rss&utm_campaign=icerat-il-trojan-virtuale-che-sfugge-agli-antivirus

# Quando l'Intelligenza Artificiale diventa una minaccia

Nov 30, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Tecnologia 0

***Non solo business e software di protezione: AI e Machine Learning possono essere sfruttati anche dai pirati informatici per i loro scopi.***

Esistono tecnologie buone e tecnologie cattive? Più che una questione filosofica, quella a cui hanno cercato di rispondere **Trend Micro**, **Europol** e **United Nations Interregional Crime and Justice Research Institute (UNICRI)** è una domanda che molti ricercatori di sicurezza si stanno ponendo negli ultimi anni.

Il tema è quello dell'Intelligenza Artificiale e dei possibili utilizzi che possono esserne fatti nel settore della cyber

security. **In altre parole, è il timore (condiviso dai più) che presto l'AI non venga utilizzata solo da software antivirus e strumenti di protezione, ma anche dai cyber criminali**.

Il corposo report stilato dai ricercatori (consultabile a questo indirizzo Web) prova a disegnare un quadro dei possibili utilizzi malevoli dell'AI che vadano oltre quelli visti finora, che si sono limitati alla produzione di deepfake più o meno accurati.

Lo scenario più inquietante, cioè quello dell'uso di tecnologie di intelligenza artificiale per **la creazione di malware di nuova generazione**, viene per fortuna archiviato in un prossimo (e si spera lontano) futuro.

Secondo gli autori del report, infatti, questo tipo di attività è per il momento limitata a qualche esperimento portato avanti da ricercatori di sicurezza per scopi accademici o comunque puramente teorici.

I pochi esperimenti portati avanti, come **DeepHack** e **DeepExploit**, hanno comunque suscitato un certo interesse nel mondo del cyber crimine, come testimoniano alcuni post intercettati da Trend Micro su forum frequentati da hacker.

Più probabile che l'utilizzo dell'AI possa essere indirizzato

al potenziamento di tecniche di attacco già esistenti, come la creazione di messaggi di spam o di phishing che siano in grado di aggirare i filtri utilizzati dai software di protezione.

Anche l'applicazione dell'AI ai **sistemi di crittografia**, sia in chiave di sviluppo di nuovi algoritmi, sia in funzione dello sviluppo di strumenti per la sua violazione, è ancora a uno stato embrionale.

Gli studi in questo senso, però, hanno già dimostrato come i possibili sviluppi consentirebbero di creare sistemi di comunicazione pressoché impossibili da decifrare.

La sezione dedicata agli indizi individuati in rete da Trend Micro sull'utilizzo di sistemi di intelligenza artificiale nel mondo del cyber crimine indicano però un progressivo sviluppo di queste tecnologie.

I riferimenti, per il momento, si limitano alla creazione di reti di bot per i social network (come Instagram) che siano in grado di simulare il comportamento umano e consentire così ai pirati informatici di aggirare i sistemi di controllo (come **CAPTCHA**) utilizzati per individuare i sistemi automatizzati.

Un possibile utilizzo dell'AI con scopi malevoli, secondo i ricercatori, potrebbe però trovare presto una sua applicazione nel mondo del gaming e, soprattutto, nell'ambito dei videogiochi in cui l'accumulo di denaro virtuale (ma convertibile in valuta reale) ha un ruolo preminente.

Un impiego simile potrebbe riguardare **la compravendita di criptovalute**, secondo uno schema che al momento è pura fantasia, ma che è già stato ipotizzato spesso in varie truffe online.

Insomma: lo stato delle cose, a quanto si legge nel report, è ancora uno scenario in cui ai tanti timori corrisponde solo un certo interesse dei pirati per il tema. Le cose, però, potrebbero cambiare molto, molto rapidamente.

Condividi l’articolo

---

IceRat: il trojan “virtuale” che sfugge agli antivirus Trova due falle zero-day in Windows 7 e 2008 Server… per caso

---

**Articoli correlati**

**Altro in questa categoria**

---

https://www.securityinfo.it/2020/11/30/quando-lintelligenza-artificiale-diventa-una-minaccia/?utm_source=rss&utm_medium=rss&utm_campaign=quando-lintelligenza-artificiale-diventa-una-minaccia

---

# Trova due falle zero-day in Windows 7 e 2008 Server… per caso

Nov 27, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

---

***Il ricercatore francese ha “incrociato” le vulnerabilità aggiornando uno strumento per individuare configurazioni errate nel sistema operativo.***

Due vulnerabilità zero-day per **Windows** di quelle che “fanno male”. Non tanto per la gravità (si tratta di falle che

consentono una escalation di privilegi e non l’esecuzione di codice in remoto) quanto per il fatto che interessano due versioni del sistema operativo ormai non più supportate: **Windows 7** e **Windows Server 2008**.

Le due falle di sicurezza riguardano i servizi **RPC Endpoint Mapper** e **DNSCache**. Sfruttandole, in pratica, è possibile iniettare delle DLL con privilegi a livello SYSTEM (il più elevato) attraverso una funzionalità pensata in origine per consentire agli sviluppatori di verificare le performance del sistema quando su di esso “girano” componenti personalizzati.

A trovarle è stato **Clément Labro**, uno sviluppatore che si è trovato in una situazione piuttosto spinosa. Labro, infatti, non era affatto alla ricerca di bug nel sistema operativo Microsoft, ma stava semplicemente aggiornando **PrivescCheck**, uno strumento software che ha l’obiettivo di individuare configurazioni errate di Windows.

Nel suo aggiornamento, lo sviluppatore ha introdotto una serie di controlli per verificare tecniche di escalation dei privilegi e, in questo modo, si è imbattuto nelle due vulnerabilità.

**Il problema è che Labro non ha avuto modo di procedere a una vera e propria responsible disclosure**. Quando ha realizzato che il suo update aveva acceso i riflettori su due bug di Windows, l'aggiornamento era già disponibile su Internet.

Insomma: lo sviluppatore si è trovato nella brutta situazione di aver fornito involontariamente gli strumenti per sfruttare due vulnerabilità di Windows senza aver prima avvertito Microsoft.

A questo punto, Labro ha deciso di pubblicare tutto su Internet sperando che le informazioni sulla vulnerabilità possano permettere di rilasciare al più presto una patch per i due bug e, lato utenti, di utilizzare tutti gli accorgimenti per mitigare il rischio di un attacco che sfrutti le vulnerabilità.

La buona notizia è che, per trarre vantaggio dalle falle di sicurezza, un eventuale pirata informatico dovrebbe aver già ottenuto un accesso alla macchina vulnerabile. Beh, speriamo in bene…

Condividi l'articolo

---

Google lancia Privacy Sandbox. Ecco il progetto per il futuro del Web

---

## Articoli correlati

## Altro in questa categoria

---

https://www.securityinfo.it/2020/11/27/trova-due-falle-zero-day-in-windows-7-e-2008-server-per-caso/?utm_source=rss&utm_medium=rss&utm_campaign=trova-due-falle-zero-day-in-windows-7-e-2008-server-per-caso

# Google lancia Privacy Sandbox. Ecco il progetto per il futuro del Web

Nov 26, 2020 Marco Schiaffino In evidenza, News, Privacy, RSS, Scenario, Tecnologia 0

***Addio ai cookie di terze parti e intelligenza artificiale per profilare gli utenti. Ma è un "work in progress" che verrà delineato col tempo.***

Come tenere insieme pubblicità online e diritto alla privacy degli utenti? A chiederselo non è un'associazione di consumatori ma Google, una delle aziende che (in diversi ruoli) ha proprio i suoi maggiori interessi nella gestione delle informazioni raccolte sul Web e il loro utilizzo a scopi pubblicitari.

La soluzione, secondo quanto dicono dalle parti di Mountain View, passerebbe per una piccola (ma neanche tanto) rivoluzione che ha un nome piuttosto evocativo: **Privacy Sandbox**. A illustrarlo in un incontro (virtuale) con la stampa è stato **Nicola Roviaro Head of EMEA Data Privacy Specialist** dell'azienda statunitense**.**

Il punto di partenza del ragionamento è semplice: aumentare la tutela della riservatezza dei dati personali senza mettere in discussione l'attuale modello di funzionamento del Web, che di quei dati personali ha un tremendo bisogno.

A prima vista sembra di trovarsi di fronte alla classica sfida

di salvare capra e cavoli, ma secondo Roviaro la soluzione potrebbe essere più semplice di quanto non sembri, almeno a livello concettuale.

I principi alla base del progetto Privacy Sandbox (se ne trova un riassunto in questa pagina Web) prevedono, in pratica, di eliminare tutti quegli aspetti della raccolta di informazioni che a oggi sono fonte di possibili abusi e, in particolare, dei famigerati cookie di terze parti utilizzati spesso per il tracciamento della  navigazione su Internet.

Ma con cosa verrebbero sostituiti? Qui il tutto si fa un po' più fumoso, ma stando a quanto si è capito del progetto di Google, l'idea sarebbe quella di **utilizzare sistemi di intelligenza artificiale che consentano di profilare gli utenti sulla base dei loro interessi e delle loro abitudini direttamente… attraverso il browser**.

Insomma: al posto di inondare di cookie gli utilizzatori, questi verrebbero "studiati" direttamente da algoritmi integrati nei software per la navigazione su Internet (o nei dispositivi) e questi dati verrebbero poi utilizzati per far "girare" il grande circo della pubblicità programmatica.

Secondo gli esperti di Google, questo permetterebbe di mantenere intatto il sistema che prevede la visualizzazione di pubblicità “mirate” e, al tempo stesso, ridurre la quantità di informazioni necessarie allo scopo, così come il numero di soggetti che vi accedono.

Il tutto, nei progetti di Google, dovrebbe essere portato avanti in maniera aperta e partecipativa, coinvolgendo tutti i soggetti interessati (a partire dagli sviluppatori di browser) nell’ambito del **World Wide Web Consortium (W3C)** per arrivare alla definizione di uno standard internazionale.

Insomma: un percorso molto trasparente che a ben vedere, però, potrebbe generare qualche problemino. Il primo è capire quanto possano essere felici tutti gli attori del mondo del Web advertisement di scompaginare il meccanismo attuale, affidandolo a un numero ridotto di soggetti (sviluppatori di browser e di sistemi operativi?) che a questo punto governerebbero buona parte del flusso delle informazioni.

A voler essere maligni, poi, si potrebbe pensare che il progetto somigli un po’ troppo a un tentativo di spostare il

baricentro del controllo in un settore in cui Google, con l’abbinata tra Chrome e Android) ha una indiscussa posizione dominante.

**E il termine “posizione dominante” apre un’altra questione: come la prenderanno le varie autorità antitrust in Europa e negli USA?**

E infine, che cosa impedirebbe a un qualche maniaco della privacy di proporre un browser (o un sistema operativo) privo di questi meccanismi facendo così saltare il banco?

Condividi l’articolo

---

Un milione di utenti Android colpiti da finti mod per Minecraft

---

## Articoli correlati

## Altro in questa categoria

---

https://www.securityinfo.it/2020/11/26/google-lancia-privacy-sandbox-ecco-il-progetto-per-il-futuro-del-web/?utm_source=rss&utm_medium=rss&utm_campaign=google-lancia-privacy-sandbox-ecco-il-progetto-per-il-futuro-del-web