Gli accessi a 43.000 server hackerati in vendita su MagBo

Mag 15, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Malware, News, RSS, Scenario 0

Sul negozio online i cyber criminali hanno messo in vendita le credenziali che consentono di accedervi. Coinvolti anche ospedali ed enti pubblici.

Se esiste un settore che non vive nessun tipo di crisi, è quello del cyber-crimine. La dimostrazione? Questa volta arriva da **KELA**, che ha pubblicato un report in cui "certifica" il successo di **MagBo**, lo store online che permette agli hacker di vendere e acquistare le credenziali di accesso a server compromessi.

Il portale, di cui abbiamo parlato quasi due anni fa in questo articolo, è la più cristallina conferma di come il settore della criminalità informatica sia strutturato in una filiera estremamente complessa, che ricorda da vicino quella del commercio internazionale.

Lo store online, che aveva cominciato la sua attività con un listino comprendente poco più di 1.500 server hackerati, offre adesso un "catalogo" che ne comprende la bellezza di 43.000, il 90% dei quali sono controllati tramite **Web Shell**.

Secondo quanto viene riportato da KELA, società di sicurezza informatica che ha monitorato l'attività di MagBo, la quantità di server "trattati" dai pirati informatici sarebbe però ben superiore. **Oltre ai 43.000 server invenduti, lo store online avrebbe piazzato la bellezza di 150.000 vendite**.

In altre parole: oltre 150.000 server sarebbero già stati compromessi e le credenziali cedute a soggetti che avevano un interesse a prenderne il controllo.

Quello che offre il portale, però, è un servizio completo. I server in questione, infatti, sono dotati di una backdoor realizzata su misura che permette facilmente di caricare sul server compromesso nuovi malware, moduli personalizzati e qualsiasi tipo di software malevolo il "cliente" voglia utilizzare.

Insomma: MagBo rappresenta, secondo i ricercatori, una formula di "access as a service" che porta l'attività di hacking a un nuovo livello di perfezionamento commerciale.

Condividi l'articolo

Troppi exploit per iOS: Zerodium fa crollare il mercato

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/05/15/gli-accessi-a-43-000-server-hackerati-in-vendita-su-magbo/?utm_source=rss&utm_medium=rss&utm_campaign=gli-accessi-a-43-000-server-hackerati-in-vendita-su-magbo

Troppi exploit per iOS: Zerodium fa crollare il mercato

Mag 15, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Addio al mito della sicurezza dell'iPhone? Secondo gli esperti del settore ci sono in circolazione addirittura troppi strumenti di attacco.

Fino a qualche tempo fa, trovare una vulnerabilità che consentisse di fare breccia in iOS equivaleva ad avere in tasca un biglietto vincente della lotteria. Sul "mercato grigio" che si occupa di compravendita di exploit, infatti, una falla di sicurezza di iPhone aveva valutazione

astronomiche.

Quei tempi, a quanto pare, sono finiti. A dirlo è **Zerodium**, la società specializzata nella compravendita di exploit che cinque anni fa era arrivata a offrire **1 milione di dollari** per acquistare strumenti di jailbreaking di iOS 9.

Adesso l'azienda ha comunicato via **Twitter** che per i prossimi mesi non intende acquistare exploit per l'elevazione dei privilegi in iOS, per l'esecuzione di codice in remoto su Safari o per evadere le sandbox. Motivo? Ne hanno già ricevute troppe.

Un annuncio che ha fatto alzare un sopracciglio a molti di esperti di sicurezza, soprattutto alla luce di una dichiarazione piuttosto "netta" (veicolata sempre via Twitter) dello stesso fondatore di Zerodium, **Chaouki Bekrar**.

> *iOS Security is fucked. Only PAC and non-persistence are holding it from going to zero…but we're seeing many exploits bypassing PAC, and there are a few persistence exploits (0days) working with all iPhones/iPads. Let's hope iOS 14 will be better.https://t.co/39Kd3OQwy1*
>
> *— Chaouki Bekrar (@cBekrar) May 13, 2020*

Insomma: secondo Bekrar il livello di sicurezza in iOS è precipitato ai minimi storici, al punto che la sua società prevede che i prezzi delle vulnerabilità per il sistema operativo mobile di Apple subiranno un crollo nel prossimo futuro. Difficile dire se si tratti di una semplice campagna di marketing o se ci sia un qualche reale fondamento.

Le prime avvisaglie di questo cambio di rotta, però, erano arrivate lo scorso settembre, quando Zerodium aveva aggiornato i suoi "listini" segnando **il sorpasso delle vulnerabilità per Android nei confronti di quelle per iOS**.

Per quanto le dichiarazioni di Bekrar vadano prese con le

pinze, il segnale per Apple non è dei migliori. Anche solo per l'impatto che può avere a livello di opinione pubblica. Tra qualche mese, probabilmente, avremo gli elementi per capire quanto questi timori possano essere fondati.

Condividi l'articolo

Gli accessi a 43.000 server hackerati in vendita su MagBo Ramsey prende di mira i computer isolati dalla rete

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/15/troppi-exploit-per-ios-zerodium-fa-crollare-il-mercato/?utm_source=rss&utm_medium=rss&utm_campaign=troppi-exploit-per-ios-zerodium-fa-crollare-il-mercato

---

Ramsey prende di mira i computer isolati dalla rete

Mag 14, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, Scenario 0

Gli autori del malware hanno creato una tecnica che gli

permette di raggiungere i PC privi di connessione ed esfiltrare i dati quando possibile.

In gergo viene chiamato “air gap” ed è considerata la misura di prevenzione più efficace per proteggere un dispositivo da un potenziale attacco informatico. La traduzione della strategia è semplice: disconnettere i computer che contengono informazioni sensibili o (quando possibile) gestiscono servizi critici dalla rete aziendale.

In questo modo si riduce esponenzialmente il rischio che un pirata informatico possa compromettere le macchine in questione attraverso il cosiddetto “movimento laterale”, cioè l’attacco a catena da un computer all’altro all’interno della rete.

I pirati informatici che hanno creato **Ramsey**, però, hanno deciso di provare a superare questa forma di protezione dotando il loro malware di una serie di strumenti che gli permettono di essere efficace anche i una situazione in cui i loro bersagli sono stati isolati completamente dalla rete.

Come spiegano i ricercatori di **ESET** in un corposo report, il

vettore di attacco scelto dai cyber criminali è l'uso delle memorie rimuovibili (chiavi USB e dischi esterni) che Ramsey sfrutta sia per diffondersi da una macchina all'altra, sia per esfiltrare i dati rubati.

Per quanto riguarda la diffusione, Ramsey sfrutta un classico schema che fa leva su una vulnerabilità di Word (CVE-2017-11882) per colpire il "paziente zero" all'interno della rete. Il malware poi inietta una copia del suo codice in tutti i file **Portable Executable (PE)** che riesce a raggiungere all'interno di unità di memoria rimuovibili.

La strategia, in pratica, conta sul fatto che prima o poi una delle unità di memoria venga collegata al computer isolato (d'altra parte questo è l'unico modo per scambiare dati con un PC protetto da air gap) permettendo così di infettarlo.

Lo stesso stratagemma viene utilizzato per l'esfiltrazione dei dati. Le informazioni ritenute sensibili (file in formato **DOC**, **PDF** e archivi **ZIP**) vengono memorizzate in una sezione nascosta dell'unità di memoria, in attesa che il malware con i dati rubati venga a "contatto" con un computer che ha accesso a Internet.

IL modulo dedicato all'esfiltrazione, spiegano i ricercatori, non è stato ancora individuato e analizzato a fondo. La logica riportata qui sopra, però, è l'ipotesi più credibile riguardo il suo possibile funzionamento.

Condividi l'articolo

Ecco la top ten delle vulnerabilità più usate dai pirati

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/14/ramsey-prende-di-mira-i-computer-isolati-dalla-rete/?utm_source=rss&utm_medium=rss&utm_campaign=ramsey-prende-di-mira-i-computer-isolati-dalla-rete

---

Ecco la top ten delle vulnerabilità più usate dai pirati

Mag 13, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

I dati del governo USA elencano gli exploit più utilizzati dal 2016 a oggi. In testa alla classifica le vulnerabilità di Microsoft Office.

Quali sono le falle di sicurezza preferite dai pirati informatici? Una risposta arriva da un white paper pubblicato dal governo USA, che ha pubblicato su Internet una sorta di "classifica" delle vulnerabilità più utilizzate dai cyber criminali tra il 2016 e il 2019.

Il rapporto ha l'obiettivo di sensibilizzare gli amministratori IT e prende in esame, a quanto si legge, le tecniche di attacco utilizzate dai pirati informatici specializzati in cyber-spionaggio (APT) collegati a governi stranieri.

La top ten delle vulnerabilità individuate dai tecnici statunitensi (e non è una sorpresa) è monopolizzata dalle falle di sicurezza del pacchetto **Office** di **Microsoft**. Un dato che conferma come le strategie di attacco dei gruppi APT sfruttino principalmente tecniche di phishing e prediligano la posta elettronica come vettore di attacco.

Le vulnerabilità indicate ai primi due posti (CVE-2017-11882 e CVE-2017-0199) sono infatti collegate a classici exploit che consentono di avviare l'esecuzione di codice in remote all'apertura del documento infetto.

Al terzo posto troviamo invece una vulnerabilità di **Apache Struts** (CVE-2017-5638). Anche in questo caso, a presenza in classifica della vulnerabilità conferma quanto sostengono da tempo gli esperti di sicurezza, cioè la tendenza da parte degli hacker di stato a utilizzare strumenti normalmente usati anche in fase di penetration testing.

Nel caso specifico il riferimento è a **JexBoss**, un software open source che gli esperti di sicurezza utilizzano per

portare attacchi come “red team” nel corso delle valutazioni sulla solidità dei sistemi informatici.

La prima vulnerabilità relativa al famigerato **Adobe Flash** (CVE-2018-4878) si piazza invece solo al settimo posto. A chiudere la classifica, a sorpresa, è invece una falla di sicurezza in **Drupal** (CVE-2018-7600) risalente al 2018.

Il report si chiude con la scontata (ma sempre valida) esortazione ad abbandonare software che non hanno più un servizio di supporto per gli aggiornamenti di sicurezza.

Condividi l’articolo

Ora tutti i dati degli hacker di WeLeakData sono sul Dark Web

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/13/ecco-la-top-ten-delle-vulnerabilita-piu-usate-dai-pirati/?utm_source=rss&utm_medium=rss&utm_campaign=ecco-la-top-ten-delle-vulnerabilita-piu-usate-dai-pirati

---

Ora tutti i dati degli hacker di WeLeakData sono sul Dark

Web

Mag 12, 2020 Marco Schiaffino Gestione dati, Hacking, In evidenza, Leaks, News, RSS, Scenario 0

Dopo la precipitosa (e misteriosa) chiusura del sito, tutte le informazioni contenute nel database sono state pubblicate sul Dark Web.

Chi di leak ferisce, di leak perisce. Il caso di **WeLeakData** è un perfetto esempio di come la legge del contrappasso si possa applicare anche nell'ambito della sicurezza informatica. Con conseguenze che, al momento, è difficile immaginare.

Il sito, che alcuni descrivono come un forum hacker, è (o sarebbe meglio dire "era") qualcosa di molto simile a WeLeakInfo, di cui abbiamo parlato qualche mese fa in questo articolo.

In pratica si trattava di un sito Internet in cui era possibile vendere e acquistare informazioni sottratte a qualsiasi genere di organizzazione, azienda e servizio Internet. **Una sorta di "gran bazar" che trattava solo dati rubati disponibili per il miglior offerente**.

Alla fine di aprile, WeLeakData è sparito e, se per quanto riguarda le cause della scomparsa ci si sta ancora interrogando sull'eventualità di un arresto di chi lo gestiva, il suo contenuto è invece riapparso abbastanza velocemente.

Ma che cosa c’è nel database? Oltre a tutti i dati rubati, che faranno indubbiamente la felicità dei pirati informatici che non aspettano altro di sfruttarli per attacchi diretti ai servizi online o per operazioni che seguono la strategia del credential stuffing, ci sono anche informazioni che potrebbero interessare (molto) alle forze di polizia.

Già, perché oltre al materiale conservato sui server per la compravendita clandestina, il database contiene anche messaggi privati scambiati all’interno del sito con tanto di email e indirizzi IP.

Insomma: dopo una (dis)onorata carriera dedicata a esporre i dati di ignare vittime, WeLeakData sta mettendo a disposizione di tutti informazioni che potrebbero permettere di individuare un buon numero di pirati informatici che hanno gravitato intorno al sito.

Condividi l’articolo

Gli hacker di Shiny Hunters fanno strage di aziende

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/12/ora-tutti-i-dati-degli-hacker-di-weleakdata-sono-sul-dark-web/?utm_source=rss&utm_medium=rss&utm_campaign=ora-tutti-i-dati-degli-hacker-di-weleakdata-sono-sul-dark-web

---

Gli hacker di Shiny Hunters fanno strage di aziende

Mag 11, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Leaks, News, RSS 0

Il gruppo sta pubblicando sul Dark Web dati sottratti a 10 aziende colpite nelle ultime ore. Tra le precedenti vittime anche Microsoft e Tokopedia.

C'è u nuovo pericolo pubblico nel Dark Web: sono gli hacker di **Shiny Hunters**, che nel giro di una manciata di giorni sono riusciti a catalizzare l'attenzione dell'opinione pubblica (o almeno di quella dedicata alla cyber security) grazie a una serie di leak di primo piano.

La saga degli Shiny Hunters è cominciata lo scorso 2 maggio, quando hanno pubblicato su Internet una parte dei dati (15 milioni di record) che hanno sottratto a **Tokopedia**, il più grande sito di e-commerce indonesiano. La seconda tranche dei dati rubati (91 milioni di record) invece, è stata messa in vendita per 5.000 dollari sul Dark Web.

Non contenti, a distanza di pochi giorni hanno rivendicato la

violazione di un repository privato di Microsoft su GitHub, il cui contenuto è stato diffuso gratuitamente su Internet.

Ora gli Shiny Hunters hanno letteralmente inondato i bassifondi di Internet con una serie di database sottratti a 10 società diverse, che avrebbero colpito in seguito.

L’elenco delle vittime comprende:

L’app di appuntamenti online **Zoosk** (30 milioni di record)

IL servizio di stampa online **Chatbooks** (15 milioni di record)

La piattaforma sudcoreana dedicata alla moda **SocialShare** (6 milioni di record)

Il servizio di cibo a domicilio **Home Chef** (8 milioni di record)

Il sito di e-commerce **Minted** (5 milioni di record)

Il sito di notizie online **Chronicle of Higher Education** (3 milioni di record)

La rivista di arredamento sudcoreana **GGuMim** (2 milioni di record)

La rivista dedicata al benessere **Mindful** (2 milioni di record)

Il sito di e-commerce indonesiano **Bhinneka** (1.2 milioni di record)

Il sito di notizie online statunitense **StarTribune** (1 milioni di record)

Insomma: un vero “tsunami” di informazioni rubate che coinvolgono milioni di utenti e che adesso sono disponibili per chiunque abbia la possibilità di acquistarli.

Condividi l’articolo

I pirati stanno reclutando disoccupati negli USA per usarli come “muli”

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/11/gli-hacker-di-shiny-hunters-fanno-strage-di-aziende/?utm_source=rss&utm_medium=rss&utm_campaign=gli-hacker-di-shiny-hunters-fanno-strage-di-aziende

---

I pirati stanno reclutando disoccupati negli USA per usarli come “muli”

Mag 08, 2020 Marco Schiaffino Hacking, In evidenza, News, Phishing, RSS 0

Il crollo dell'occupazione negli Stati Uniti offre ai cyber criminali un'occasione unica per reclutare compllici nel riciclaggio di denaro.

La crisi economica legata alla pandemia di **Covid-19** ha dei risvolti imprevisti, che coinvolgono anche il mondo della cyber security. Come spiegano i ricercatori di **PhishLabs**, il crescente numero di disoccupati negli Stati Uniti ha portato i cyber criminali ad avviare delle vere e proprie campagne di reclutamento che hanno l'obiettivo di trasformarli in "muli" per il riciclaggio del denaro sporco.

I cosiddetti muli rappresentano un tassello fondamentale nell'ecosistema dei cyber criminali, che li sfruttano per trasferire il denaro che rubano attraverso i loro attacchi dirottandolo attraverso sistemi di money transfer non tracciabili.

Ai loro "complici", che spesso non si rendono conto esattamente di quello che stanno facendo, i criminali permettono di trattenere una quota delle somme.

Naturalmente, nella prospettiva dei pirati informatici questo schema rappresenta una vera manna. Ad accollarsi tutti i rischi sono infatti i muli, che nel caso di intervento delle forze di polizia saranno gli unici a essere individuati.

La campagna di reclutamento rilevata dai ricercatori, spiegano in un report, è molto simile a quelle che circolano normalmente sul Web e che offrono la possibilità di "lavorare da casa" per ottenere un "guadagno extra".

In questa versione, però, i cyber criminali fanno riferimento espressamente alla pandemia da Coronavirus e sfruttano l'emergenza sanitaria non solo per giustificare una presunta "carenza di personale", ma anche per fare leva sul bisogno di denaro di chi ha perso l'impiego a causa dell'epidemia.

Il fenomeno è stato evidenziato anche dall'**FBI**, che in una serie di comunicati ha sottolineato come attività di questo tipo, anche se condotte inconsapevolmente, costituiscono un reato.

Condividi l'articolo

Nuova tecnica di attacco: lo skimmer è nascosto nell'icona favicon

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/08/i-pirati-stanno-reclutando-disoccupati-negli-usa-per-usarli-come-muli/?utm_source=rss&utm_medium=rss&utm_campaign=i-pirati-stanno-reclutando-disoccupati-negli-usa-per-usarli-come-muli

Nuova tecnica di attacco: lo skimmer è nascosto nell'icona favicon

Mag 07, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

I pirati hanno messo a punto uno stratagemma per introdurre codice malevolo in grado di rubare i dati delle carte di credito nei siti Web.

Gli attacchi attraverso **digital skimmer**, i JavaScript che consentono di sottrarre le credenziali delle carte di credito nei form di pagamento dei siti di e-commerce, sono sempre più frequenti. I maestri, in questo campo, sono i gruppi di pirati che gli esperti di sicurezza hanno battezzato con il nome di **Magecart**.

La nuova campagna di attacchi individuata dai ricercatori di **Malwarebytes**, però, rappresenta un perfetto esempio dell'inventiva che posseggono i pirati informatici nell'elaborare strategie per diffondere il loro codice malevolo.

Come si legge nel report della società di sicurezza, la gang di cyber criminali ha elaborato uno stratagemma terribilmente efficace per distribuire il loro JavaScript all'intero di immagini apparentemente innocue.

I pirati hanno realizzato un sito Internet (**MyIcons.net**) clonando i contenuti di un sito Internet perfettamente

legittimo (IconArchive) che mette a disposizione icone e strumenti grafici per la creazione di siti Internet.

Il sito, in pratica, funziona come un host che contiene al suo interno le icone utilizzate dal sito Internet, che vengono caricate sulla pagina Web “pescando” da MyIcons.

Per diffondere il malware, i pirati hanno scelto di sfruttare un elemento grafico di secondo piano come le **favicon**, cioè le icone personalizzate che compaiono nelle schede di navigazione dei browser. **Per nascondere la loro pericolosità, però, hanno messo in piedi un sistema che distribuisce il codice malevolo soltanto nelle pagine che gli interessano**.

In pratica, in tutte le pagine del sito che sfrutta il servizio di MyIcons le icone sono dei normali file PNG, assolutamente innocui. **Quando però un utente apre una pagina che contiene la parola chiave "checkout", il server fornisce un collegamento a un link diverso, che al suo interno nasconde il JavaScript che visualizza un form per il pagamento tramite carta di credito e che consente ai pirati di rubare le informazioni di pagamento**.

Una tecnica geniale, che ha permesso ai pirati di colpire un numero imprecisato di siti Internet su piattaforma **Magento**.

Condividi l'articolo

Attacchi a 900.000 siti WordPress

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/05/07/nuova-tecnica-di-attacco-lo-skimmer-e-nascosto-nellicona-favicon/?utm_source=rss&utm_medium=rss&utm_campaign=nuova-tecnica-di-attacco-lo-skimmer-e-nascosto-nellicona-favicon

Attacchi a 900.000 siti WordPress

Mag 06, 2020 Marco Schiaffino Attacchi, In evidenza, News, RSS, Vulnerabilità 0

I pirati sfruttano principalmente vulnerabilità XSS per inoculare una backdoor nel codice dei siti Internet presi di mira.

Ancora **WordPress**, ancora una campagna di attacchi a tutto campo che cercano di garantire ai pirati informatici un accesso ai siti Internet per prenderne il controllo e inserire al loro interno dei collegamenti a pagine nocive.

La segnalazione arriva da Defiant, che ha rilevato un'insolita attività online che sta prendendo di mira alcune vulnerabilità di plugin per WordPress.

In questo caso, spiegano i ricercatori, i pirati informatici non si stanno muovendo sulla base di nuove falle di sicurezza, ma sembrano puntare più che altro sulla legge dei grandi numeri. **I cyber criminali, infatti, starebbero utilizzando una serie di vulnerabilità piuttosto datate, nella speranza di individuare siti Internet i cui amministratori non hanno eseguito gli aggiornamenti che le correggono**.

Una strategia che, purtroppo, rischia di dare i suoi frutti. Molti utenti WordPress, infatti, hanno un atteggiamento piuttosto “lassista” negli aggiornamenti e nemmeno le ultime novità introdotte dagli sviluppatori del **Content Management System** (che prevede l’aggiornamento automatico dei plugin) sembra poter arginare questo tipo di attacchi.

Nel dettaglio, i cyber criminali starebbero sfruttando cinque vulnerabilità relative ad alcuni plugin e più precisamente **Easy2Map**; **Blog Designer**; **WP GDPR Compliance**; **Total Donations** e nel tema **Newspaper**.

La maggior parte delle vulnerabilità sono semplici XSS (Cross Site Scripting) e la maggior parte delgi attacchi sono quelli che sfruttano la falla in Easy2Map, corretta nell’agosto del 2019.

L’attacco sfrutta due modalità. Nel caso in cui l’amministratore non abbia effettuato l’accesso, lo script usato dai pirati imposta un dirottamento del sito verso un

indirizzo malevolo. Se invece l’amministratore ha eseguito l’accesso, cerca di iniettare una backdoor nel file PHP.

La soluzione, concludono i ricercatori, è piuttosto semplice: aggiornare i plugin in questione.

Condividi l’articolo

Attacchi hacker a un aereo? Qualcosa si può fare

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/06/attacchi-a-900-000-siti-wordpress/?utm_source=rss&utm_medium=rss&utm_campaign=attacchi-a-900-000-siti-wordpress

---

Attacchi hacker a un aereo? Qualcosa di può fare

Mag 05, 2020 Marco Schiaffino Hacking, In evidenza, News, RSS, Scenario, Tecnologia, Vulnerabilità 0

La tecnica di attacco consente di ingannare i sistemi automatici del velivolo e farlo reagire alla presenza

di un “aereo fantasma”.

La possibilità di un attacco informatico ai sistemi di volo di un aeroplano è uno degli scenari più suggestivi (e inquietanti) su cui gli esperti di cyber security lavorano da anni. Qualcosa di concreto, adesso, arriva dallo studio di **Pen Test Partners** che descrive una tecnica di hacking ai danni di uno dei sistemi di controllo di volo utilizzati sui velivoli di linea.

Il report pubblicato su Internet dai ricercatori spiega che la vulnerabilità interessa il sistema **TACS (Traffic Alert & Collision Avoidance System)** il cui compito è quello di notificare avvisi quando viene rilevata una possibile collisione in volo.

Il sistema, spiega l’autore del report, ha due modalità di funzionamento: la prima prevede la notifica di un avviso al pilota, mentre la seconda, che si attiva in alcune configurazioni (per esempio con i velivoli della **Airbus**) invia un segnale al pilota automatico che reagisce impostando le manovre per modificare l’altitudine.

I ricercatori, utilizzando una chiavetta USB per la trasmissione di video (costo: 10 dollari) e un transponder, hanno dimostrato come sia possibile ingannare il sistema TACS

creando “aerei fantasma” che verrbbero segnalati come reali ai piloti o, nel caso in cui il pilota automatico sia inserito, avviare le manovre automatiche di correzione dell’altitudine.

Il loro studio, ovviamente, è stato portato avanti su dei simulatori di volo, ma nel rapporto viene precisato che la tecnica è considerata efficace anche in uno scenario reale.

Ma quali possono essere le conseguenze di un attacco del genere? Oltre a “disturbare” la normale navigazione, secondo gli analisti di Pen Test Partners sarebbe possibile arrivare a **esasperare l’equipaggio al punto di indurre il pilota a disattivare TACS, riducendo così il livello di sicurezza del volo**.

Uno scenario senza dubbio preoccupante, anche se meno catastrofico di ipotesi di controllo di altri sistemi del velivolo (come l’accensione o lo spegnimento dei motori) prospettati in altri studi.

In ogni caso, sottolineano gli autori dello studio, la navigazione aerea è assistita attraverso controlli da terra che permetterebbero di verificare (e smascherare) le false letture del sistema TACS.

Condividi l’articolo

Attacco a un server MDM per diffondere un malware per Android

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/05/05/attacchi-hacker-a-un-aereo-qualcosa-di-puo-fare/?utm_source=rss&utm_medium=rss&utm_campaign=attacchi-hacker-a-un-aereo-qualcosa-di-puo-fare