Iran: malware per Android che aggira l’autenticazione a due fattori

Set 21, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Il gruppo Rampant Kitten usa una tecnica che gli permette di rubare dagli smartphone i codici di autenticazione inviati tramite SMS.

Una strategia su doppio binario, che coinvolge i sistemi Windows e quelli Android. Ad adottarla è un gruppo di cyber-spioni legati al **governo di Teheran** che è finito anche sotto la lente d’ingrandimento dell’**FBI**.

I pirati informatici iraniani di **Rampant Kitten** hanno avviato negli scorsi mesi una serie di campagne che prendevano di mira varie associazioni politiche in **Azerbaijan** e **Belucistan** (un’area geografica compresa tra Iran, Pakistan e Afghanistan – ndr) utilizzando un trojan per **Windows**.

La backdoor utilizzata per infettare i PC Windows, che viene distribuita utilizzando un documento Word contenente codice malevolo, prende di mira **Telegram** e **KeePass**, un’applicazione per la gestione delle password.

Insomma: si tratterebbe di un “grimardello” pensato per garantire ai pirati informatici l’accesso a tutti i servizi utilizzati dalle vittime.

Come spiegano i ricercatori di **Check Point** in un report pubblicato sul sito della società di sicurezza, l’elemento più rilevante in questa ondata di attacchi è l’utilizzo di un malware per Android che è in grado di rubare i codici usati per l’autenticazione a due fattori di numerosi servizi.

Il malware per Android, in pratica, integra una funzionalità che gli permette di inoltrare a un numero controllato dai pirati informatici tutti gli SMS che contengono il testo “G-“, usato normalmente dal sistema di autenticazione a due fattori di **Google**.

Non solo: il trojan sarebbe in grado di inoltrare anche tutti i messaggi ricevuti su **Telegram** e altre applicazioni social. Un elemento questo, che concorda con la versione Windows del malware utilizzato da Rampant Kitten per spiare le sue vittime.

Per distribuirlo, i pirati hanno usato un’app che si propone come uno strumento per aiutare le persone che parlano persiano a ottenere la patente in Svezia.

Uno stratagemma che lascia pochi dubbi sugli obiettivi degli hacker: la Svezia (e i paesi nordici in generale) ospitano infatti una nutrita comunità di dissidenti iraniani, che hanno abbandonato il loro paese e chiesto asilo politico in Europa.

Condividi l’articolo

In Germania la prima morte provocata da un attacco informatico?

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/21/iran-malware-per-android-che-aggira-lautenticazione-a-due-fattori/?utm_source=rss&utm_medium=rss&utm_campaign=iran-malware-per-android-che-aggira-lautenticazione-a-due-fattori

---

In Germania la prima morte provocata da un attacco informatico?

Set 18, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, Scenario 0

La vittima doveva essere ricoverata con urgenza, ma un attacco ransomware ha obbligato a portarla in un altro ospedale.

L’ultima parola, probabilmente, spetterà alla magistratura tedesca, ma per il momento l’ipotesi degli investigatori sembra essere quella di configurare, per la prima volta, il reato di omicidio in capo agli autori di un cyber attacco.

Il caso, riportato dal sito di news **RTL.de**, riguarda un attacco subito dall’**Ospedale Universitario di Düsseldorf** lo scorso 10 settembre. Il ransomware, che ha colpito 30 server utilizzati dal personale della struttura sanitaria, ha bloccato temporaneamente il pronto soccorso dell’ospedale.

Un evento che ha obbligato le autorità a dirottare tutte le ambulanze su un altro ospedale, a circa 35 km dalla cittadina tedesca. **In un caso, però, la paziente soccorsa è deceduta prima di poter ricevere le cure dei sanitari**.

Le autorità starebbero di conseguenza valutando se possa essere configurabile una responsabilità in capo ai pirati informatici, che potrebbero a questo punto essere accusati di **omicidio colposo**.

Secondo quanto è emerso dalle analisi forensiche, l’attacco all’ospedale non sarebbe stato intenzionale. Il messaggio di posta elettronica che conteneva il ransomware, infatti, sarebbe stato diretto all’Università di Düsseldor e la struttura sanitaria sarebbe stata coinvolta solo perché inserita nello stesso network.

Un elemento, questo, che potrà però ridurre di ben poco la gravità delle accuse nel caso in cui le autorità dovessero decidere di confermare la presenza del nesso causale tra l’attacco informatico e il decesso della donna.

Il tema della responsabilità giuridica in caso di cyber attacchi in cui si verifichino danni fisici a persone sta diventando sempre più di attualità. La scorsa settimana, per esempio, gli analisti di **Gartner** hanno ipotizzato che nel prossimo futuro i CEO delle aziende possano essere considerati penalmente responsabili per episodi del genere.

Non è escluso che l’episodio verificatosi in Germania possa aprire nuovi orizzonti anche sotto questo punto di vista.

Condividi l’articolo

Attacco BLESA ai dispositivi Bluetooth: miliardi di dispositivi a rischio

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/18/in-germania-la-prima-morte-provocata-da-un-attacco-informatico/?utm_source=rss&utm_medium=rss&utm_campaign=in-germania-la-prima-morte-provocata-da-un-attacco-informatico

---

Attacco BLESA ai dispositivi Bluetooth: miliardi di dispositivi a rischio

Set 17, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La falla interessa la procedura di riconnessione e consentirebbe di inviare informazioni manipolate o

alterate ai dispositivi collegati.

Si chiama **BLESA** (Bluetooth Low Energy Spoofing Attack) ed è una nuova tecnica di attacco che consente di colpire i dispositivi che utilizzano il collegamento BLE.

A scoprirla un gruppo di accademici, che hanno concentrato la loro attenzione sulle procedure di riconnessione tra i dispositivi collegati con il protocollo wireless a basso consumo.

Nel dettaglio, i ricercatori hanno scoperto che in fase di riconnessione è possibile aggirare la procedura di autenticazione e, di conseguenza, "inserirsi" nel collegamento per inviare dati manipolati.

La procedura di riconnessione viene avviata automaticamente quando due dispositivi connessi tra loro perdono il collegamento, ad esempio a causa di una distanza superiore a quella "coperta" dal collegamento BLE.

In questa fase, però, il protocollo BLE prevede che la verifica delle chiavi crittografiche sia soltanto opzionale. Uno spiraglio che apre la strada all'attacco BLESA.

Per portare l'attacco, un pirata informatico deve trovarsi all'interno del raggio d'azione del Bluetooth e forzare la disconnessione tra i dispositivi che ha preso di mira.

Nulla di particolarmente difficile, come dimostra il video pubblicato dagli accademici in cui utilizzano BLESA per alterare i dati inviati da un dispositivo IoT.

[embedded content]

La vulnerabilità, spiegano nel loro report, interesserebbe miliardi di dispositivi. Per quanto riguarda gli smartphone, i ricercatori segnalano come **Apple** abbia già corretto la falla di sicurezza (CVE-2020-9770) mentre i dispositivi **Android** risultano ancora vulnerabili.

Resta aperto, però, il problema di tutti quei dispositivi IoT che utilizzano il collegamento Bluetooth per comunicare e che in molti casi, segnalano gli esperti, non prevedono nemmeno un sistema di aggiornamento che consenta di applicare la patch.

Insomma: il rischio è che buona parte dei device vulnerabili, o per lo meno quelli più datati, possano rimanere esposti a eventuali attacchi.

Il problema risulta particolarmente spinoso nel caso dei dispositivi utilizzati in ambito industriale, dove un'eventuale attacco in grado di modificare i dati inviati tramite BLE potrebbe portare a conseguenze potenzialmente devastanti.

Condividi l'articolo

In tempi di Covid il pericolo arriva dai QR Code

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/17/attacco-blesa-ai-dispositivi-bluetooth-miliardi-di-dispositivi-a-rischio/?utm_source=rss&utm_medium=rss&utm_campaign=attacco-blesa-ai-dispositivi-bluetooth-miliardi-di-dispositivi-a-rischio

---

In tempi di Covid il pericolo arriva dai QR Code

Set 16, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Vengono utilizzati sempre più spesso per ridurre il contatto fisico, ma gli utenti non hanno la percezione dei rischi collegati al loro utilizzo.

Tra gli effetti collaterali dell'emergenza Covid-19 c'è, senza dubbio, la crescita esponenziale dell'uso dei QR Code. A trainare il fenomeno, prima di tutto, ci sono ristoranti e bar, che per adeguarsi alle normative che suggeriscono di non utilizzare menu cartacei, hanno usato i codici QR per consentire ai clienti di visualizzarli su smartphone.

Secondo gli esperti, però, i QR Code potrebbero trasformarsi in un formidabile vettore di attacco a disposizione dei pirati informatici. Inquadrare un codice, infatti, è esattamente come fare clic su un collegamento che non si è verificato. Di più, visto che i codici QR, in realtà, possono anche avviare operazioni diverse sul dispositivo, come la redazione di un messaggio di posta o l'invio di un SMS.

Come messo in evidenza da **MobileIron** in un sondaggio, la percezione a livello dei rischi per la sicurezza nell'utilizzo dei codici QR tra gli utenti è terribilmente bassa.

D'altra parte, verificare se un QR code sia sospetto, come si fa abitualmente controllando l'indirizzo Internet di un collegamento che stiamo per attivare, è pressoché impossibile.

Di conseguenza, ogni volta che si inquadra un codice lo si fa "al buio" e, nel caso in cui dovesse contenere un collegamento malevolo o attivare comandi in qualche modo dannosi, l'unico strumento di difesa sarebbe l'antivirus.

Il condizionale, però, è d'obbligo. Secondo lo studio di MobileIron, condotto su un campione di **2.100 persone tra USA e Regno Unito**, solo il 51% degli utenti ha un software di protezione installato sul telefono.

Gli altri dati statistici riguardanti l'uso dei QR Code non sono più rassicuranti. Se il 67% sa che la scansione può aprire un sito Internet, sono pochi (19%) a essere consapevoli che possa interagire con la posta elettronica, avviare una telefonata (20%) o creare un SMS (24%).

Insomma: secondo i ricercatori potremmo assistere a breve a un incremento di attacchi che sfruttano i QR Code a cui, a quanto pare, non siamo affatto preparati.

Condividi l'articolo

Attacco BLESA ai dispositivi Bluetooth: miliardi di dispositivi a rischio Attacchi a tappeto contro i siti di e-commerce Magento

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/09/16/in-tempi-di-covid-il-pericolo-arriva-dai-qr-code/?utm_source=rss&utm_medium=rss&utm_campaign=in-tempi-di-covid-il-pericolo-arriva-dai-qr-code

Attacchi a tappeto contro i siti di e-commerce Magento

Set 15, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Vulnerabilità 0

Almeno 2.000 negozi online colpiti nel corso del weekend. Gli esperti: "L'attacco automatizzato più massiccio dopo quello del 2015".

Ormai vengono comunemente chiamati attacchi **MageCart**, nome derivato da uno dei gruppi specializzati in questo tipo di operazioni. In sintesi, prendono di mira i siti di e-commerce iniettando al loro interno un JavaScript in grado di rubare i dati delle carte di credito degli utenti.

Gli attacchi sfruttano tecniche diverse, che negli ultimi mesi hanno coinvolto anche i bucket su cloud. Questa volta, però, l'azione dei pirati informatici segue una linea più tradizionale, prendendo di mira i siti di e-commerce basati su piattaforma **Adobe Magento**, una delle più diffuse nel settore del commercio elettronico.

Gli attacchi si distinguono per avere un volume impressionante: i siti coinvolti sarebbero stati 10 nella giornata di venerdì, 1058 sabato, 603 domenica e 233 lunedì.

Il fenomeno è stato rilevato da **Sansec**, che in un report pubblicato su Internet sottolinea come la maggior parte dei siti colpiti dai cyber criminali utilizzino una vecchia versione di Magento, per cui non è più previsto il supporto a partire dallo scorso giugno.

L'ipotesi degli esperti è che i pirati informatici stiano sfruttando una vulnerabilità zero-day di Magento che sarebbe comparsa sugli store del Dark Web nei giorni scorsi, al prezzo di 5.000 dollari.

Stando a quanto hanno potuto ricostruire i ricercatori, i cyber criminali starebbero utilizzando due server per dialogare con il pannello di amministrazione di Magento attraverso una funzionalità chiamata **Magento Connect**.

La compromissione avverrebbe attraverso un malware contenuto in un file chiamato **mysql.php** che, una volta avviato sul

server, installa il JavaScript **prototype.js**, che “rastrella” i dati delle carte di credito.

Il quadro che si delinea, quindi, è particolarmente preoccupante. Partendo dal presupposto che la vulnerabilità consenta di attaccare i siti Magento 1.x (la versione per cui è scaduto il supporto) **il numero complessivo dei siti vulnerabili si aggirerebbe intorno ai 95.000**.

Condividi l’articolo

Bug INVDoS di Bitcoin tenuto segreto per due anni

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/15/attacchi-a-tappeto-contro-i-siti-di-e-commerce-magento/?utm_source=rss&utm_medium=rss&utm_campaign=attacchi-a-tappeto-contro-i-siti-di-e-commerce-magento

---

Bug INVDoS di Bitcoin tenuto segreto per due anni

Set 14, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La falla di sicurezza è stata considerata troppo pericolosa per renderne pubblici i dettagli. È emersa adesso perché individuata da un altro ricercatore.

Troppo “sensibile” per essere divulgata nei dettagli anche una volta che l’aggiornamento era disponibile. Stiamo parlando di **INVDoS**, un bug relativo alla gestione della blockchain **Bitcoin** che è stato scoperto nel 2018 da **Braydon Fuller**, un ricercatore specializzato nel settore.

La vulnerabilità, classificata come CVE-2018-17145, ha seguito una sorta di “corsia preferenziale”. Nonostante sia stato sviluppato e distribuito un aggiornamento, infatti, nessun dettaglio tecnico è stato reso pubblico come succede abitualmente. **Il rischio che qualcuno la sfruttasse, infatti, è stato considerato troppo elevato.**

INVDoS è una classica vulnerabilità Denial of Service, in grado cioè di bloccare il funzionamento del software in questione. Parlando di Bitcoin, però, l’ipotesi di un malfunzionamento o di una semplice “sospensione” di funzionamento ha potenziali conseguenze che qualcuno definirebbe devastanti. **Di qui una scelta che, tutto sommato, ha delle fondamenta piuttosto solide**.

Prima di tutto perché un blocco delle operazioni in un sistema blockchain rappresenta, di per sé, un problema notevole. In secondo luogo perché un evento del genere potrebbe inserirsi in una strategia più ampia, **per esempio nell'ipotesi in cui un attacco basato sulla vulnerabilità venga messo a segno in un momento particolarmente "sensibile", come quello del lancio di una nuova cripto-valuta**.

Il codice utilizzato da Bitcoin Core, infatti, è stato "riciclato" da altre cripto-valute e individuare tutte le implementazioni della porzione affetta dal bug era tutt'altro che facile.

Cos'è cambiato adesso? Semplice: la stessa falla è stata individuata da un altro ricercatore (**Javed Khan**) che ha invece deciso di utilizzare il classico "protocollo" per la comunicazione dei dettagli riguardanti la vulnerabilità.

Fuller, di conseguenza, ha deciso di pubblicare un report completo (consultabile a questo indirizzo) in cui affronta il tema fornendo tutti i dettagli che fino a oggi aveva tenuto

nascosti.

Insomma: nel settore delle cripto-valute è un momento molto particolare, in cui molti esperti di sicurezza si domandano se i 24 mesi trascorsi siano stati sufficienti per mettere tutti al riparo da potenziali attacchi. La conferma potrà arrivarci solo nelle prossime settimane e il rischio è che di INVDoS si senta parlare ancora.

Condividi l’articolo

Attacchi a tappeto contro i siti di e-commerce Magento I pirati di TeamTNT all’assalto dei container su cloud

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/14/bug-invdos-di-bitcoin-tenuto-segreto-per-due-anni/?utm_source=rss&utm_medium=rss&utm_campaign=bug-invdos-di-bitcoin-tenuto-segreto-per-due-anni

---

I pirati di TeamTNT all’assalto dei container su cloud

Set 10, 2020 Marco Schiaffino Attacchi, In evidenza, Intrusione, News, RSS 0

I cyber criminali stanno utilizzando uno strumento di monitoraggio per portare attacchi alle istanze cloud su Docker e Kubernetes.

Se chi si occupa di cloud può essere felice del fatto che sia protagonista assoluto per quanto riguarda l'evoluzione dei sistemi IT delle aziende, la sua centralità nel mondo della cyber security viene probabilmente vissuto con un minore entusiasmo.

Negli ultimi mesi, infatti, le cronache hanno riportato tanti (troppi) casi in cui i pirati informatici hanno preso di mira i sistemi virtualizzati su cloud e, in particolare, i sistemi basati su container che "girano" su piattaforme come **Docker** e **Kubernetes**.

Come dimostra l'ultimo caso, infatti, l'ecosistema cloud è ancora ben lontano dall'avere un livello di sicurezza adeguato.

Protagonisti della vicenda sono i pirati informatici del **TeamTNT**, un gruppo ben conosciuto dagli esperti di sicurezza proprio per essere specializzato nel prendere di mira i servizi cloud.

Come spiegano i ricercatori di **Intezer** in un report pubblicato su Internet, la nuova campagna di attacchi del gruppo TeamTNT ha però caratteristiche diverse dalle altre a cui abbiamo assistito.

I pirati, infatti, non usano malware o iniezioni di codice malevolo, ma uno strumento che normalmente viene utilizzato dagli amministratori IT. Si tratta di **Weave Scope**, un software open source pensato per avere visibilità delle applicazioni e delle infrastrutture cloud.

I cyber criminali prendono di mira i server con configurazioni “deboli” e utilizzano Weave Scope per mappare le funzionalità disponibili e inviare comandi, utilizzando di fatto il software come se fosse una backdoor, **consentendo al TeamTNT di prendere il completo controllo delle infrastrutture**.

Trattandosi però di un software utilizzato normalmente per gestire i servizi su cloud, l’individuazione di attività sospette diventa molto difficoltosa e, secondo i ricercatori, la strategia migliore per mitigare il rischio di questo tipo di attacco è quello di adottare una strategia “zero trust” che consenta di tenere alla larga eventuali tentativi di intrusione.

Condividi l’articolo

I migliori trucchi di phishing usati dai pirati

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/10/i-pirati-di-teamtnt-all

assalto-dei-container-su-cloud/?utm_source=rss&utm_medium=rss&utm_campaign=i-pirati-di-teamtnt-allassalto-dei-container-su-cloud

---

I migliori trucchi di phishing usati dai pirati

Set 09, 2020 Marco Schiaffino Attacchi, In evidenza, News, Phishing, RSS, Scenario 0

La classifica stilata da Sophos e pubblicata sul suo blog ufficiale. Tra le trovate dei cyber criminali ce ne sono di davvero fantasiose.

Tra le tecniche di attacco utilizzate dai pirati informatici, il phishing risulta essere quella in continua crescita. Che si tratti di attirare le potenziali vittime su siti contenenti codice malevolo o di tentativi di ingannarli per rubargli le credenziali di accesso a un servizio, i cyber criminali fanno sempre più affidamento sulla cosiddetta "ingegneria sociale".

Gli esperti di **Sophos** hanno stilato una classifica delle tecniche più usate e di quelle più particolari che hanno intercettato nel corso della loro attività. Il campionario che ne esce, pubblicato in un post sul blog ufficiale dell'azienda, contiene delle vere "chicche".

Nella top ten stilata da Sophos ci sono dei classici intramontabili, come la comunicazione di nuove linee guida per il comportamento in ufficio, in cui il messaggio appare provenire dalla sezione delle risorse umane, fino all'invio di "messaggi di prova" delle nuove email inviati da un presunto

amministratore di sistema.

Alcuni attacchi phishing, però, sfruttano stratagemmi più sofisticati. È il caso dell’assegnazione di compiti attraverso software di gestione delle attività effettivamente usati dall’azienda. **In questo caso i pirati sfruttano il fatto che il dipendente sia rassicurato dall’uso di uno strumento abitualmente utilizzato sul lavoro, senza riflettere sul fatto che, per i cyber criminali, scoprire quale software venga usato non è affatto difficile**.

Altrettanto interessante è una tecnica particolare utilizzata per il furto di credenziali di posta elettronica. Nel caso riportato, il messaggio di phishing propone un allegato descritto come “documento aziendale riservato” e chiede di inserire username e password del proprio account di posta per potervi accedere.

La migliore in assoluto a nostro giudizio, però, è quella che deve essere costata ai pirati un notevole sforzo di fantasia. **Si tratta di un messaggio apparentemente proveniente dall’amministrazione dell’azienda e che avverte che qualcuno ha lasciato le luci della macchina accesa nel parcheggio**.

Il messaggio contiene un collegamento che, teoricamente, dovrebbe permettere di visualizzare la fotografia

dell’automobile in questione. Naturalmente si tratta di un trucco e il link avvia l’installazione di un malware. L’esca, in questo caso, è però davvero originale e non ci sono dubbi che abbia funzionato piuttosto bene.

Condividi l’articolo

Il CEO responsabile penalmente se il cyber attacco provoca vittime?

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/09/i-migliori-trucchi-di-phishing-usati-dai-pirati/?utm_source=rss&utm_medium=rss&utm_campaign=i-migliori-trucchi-di-phishing-usati-dai-pirati

---

Il CEO responsabile penalmente se il cyber attacco provoca vittime?

Set 08, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario 0

La previsione di Gartner segnerebbe una vera rivoluzione in ambito di responsabilità per gli attacchi informatici con conseguenze "fisiche".

Se per il momento la preoccupazione dei dirigenti delle aziende in tema di cyber security è concentrata sulla possibilità di sanzioni legate al **GDPR** e alle altre normative sul trattamento dei dati, in futuro il problema della responsabilità potrebbero diventare molto più spinoso.

A evidenziare il tema è **Gartner**, che fonda la sua analisi a partire dal fenomeno dell'evaporazione nella distinzione tra reparti IT e OT, legati allo sviluppo dei sistemi digitali di controllo (ICS) a livello industriale.

In sostanza, gli analisti mettono in evidenza come il rischio di infortuni e danni fisici legati a cyber attacchi stiano diventando sempre più probabili e che in futuro potranno essere decisamente frequenti. In buona sostanza, quindi, si potrebbe configurare una forma di responsabilità simile a quella che la maggior parte dei sistemi giudiziari prevedono per le misure di sicurezza "fisiche".

La società si spinge anche a previsioni più dettagliate, arrivando a sostenere in un comunicato stampa che entro il 2024 il 75% degli amministratori delegati saranno "personalmente responsabili" per gli incidenti fisici legati ad attacchi cyber.

Per quanto riguarda l’impatto finanziario di questo tipo di incidenti, gli analisti lo stimano in 50 miliardi di dollari nel 2023. Una valutazione che comprende spese di assicurazione, eventuali cause giudiziarie e compensazioni.

D’altra parte l’esplosione dell’IoT è particolarmente “forte” nel settore industriale, energetico, farmaceutico e sanitario, tutti ambiti in cui eventuali incidenti possono portare a conseguenze estremamente serie se non catastrofiche.

Insomma: se il GDPR ha portato a porre una maggiore attenzione al tema della sicurezza informatica, in futuro lo stesso meccanismo potrebbe essere alimentato dal principio di responsabilità oggettiva legato alle ripercussioni fisiche degli attacchi dei cyber criminali.

A guardare il bicchiere mezzo pieno, può rappresentare un motivo in più per spingere su una reale cultura della cyber security a livello globale.

Condividi l’articolo

I migliori trucchi di phishing usati dai pirati Gli USA fissano le regole di cyber security per le missioni spaziali

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/08/il-ceo-responsabile-penalmente-se-il-cyber-attacco-provoca-vittime/?utm_source=rss&utm_medium=rss&utm_campaign=il-ceo-responsabile-penalmente-se-il-cyber-attacco-provoca-vittime

---

Gli USA fissano le regole di cyber security per le missioni spaziali

Set 07, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario 0

Il documento delinea le strategie per la sicurezza informatica cui dovranno attenersi le agenzie spaziali per bloccare eventuali attacchi.

La corsa allo spazio, nel prossimo futuro, potrebbe subire un fortissimo impulso. Ne sono convinti, per lo meno, dalle parti

della Casa Bianca e lo stesso **Donald Trump** lo ha ripetuto più volte, arrivando ad avviare il progetto per la futuribile **Space Force**, la forza armata che dovrebbe tutelare gli interessi statunitensi nello spazio.

In quest'ottica, l'amministrazione USA ha pensato bene di predisporre un documento chiamato **Space Policy Directive-5** in cui vengono fissate le regole di cyber security necessarie per mitigare il rischio di attacchi hacker in grado di danneggiare l'attività nello spazio.

Il memorandum, piuttosto stringato, fissa come primo punto quello di introdurre una logica di "s**ecurity by design**", specificando che i "sistemi spaziali e le loro infrastrutture" dovranno essere progettate e gestite da ingegneri con competenze in ambito di cyber security, con l'obiettivo di impedire che le loro operazioni possano essere "manipolate, negate, degradate, distrutte, sorvegliate o spiate".

Nel testo, inoltre, viene posto un accento particolare sulla necessità di crittografare e proteggere le comunicazioni e i

sistemi di accesso agli apparati considerati “critici”, come il controllo dei veicoli e dei sistemi di sopravvivenza.

Il testo del SPD-5 prende in esame anche i requisiti dei sistemi di sicurezza (tecnologici e fisici) delle strutture a terra che fanno parte dell’infrastruttura necessaria per la gestione delle operazioni spaziali.

Anche in ambito spaziale, l’amministrazione USA sembra estremamente attenta alla questione legata alle tecnologie utilizzate. Un punto specifico fa infatti riferimento alla filiera produttiva (supply chain) e alla necessità che le scelte dei fornitori siano ispirati all’affidabilità.

Uno dei timori, infatti, sembra essere quello di finire in un altro “caso 5G”, in cui la sicurezza possa essere messa in dubbio dall’utilizzo di tecnologie provenienti da nazioni concorrenti. Insomma, se corsa allo spazio sarà, potrà esserlo solo se totalmente “Made in USA”.

Condividi l’articolo

Falla di sicurezza in Cisco Jabber apre la strada agli attacchi

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/07/gli-usa-fissano-le-regole-di-cyber-security-per-le-missioni-spaziali/?utm_source=rss&utm_medium=rss&utm_campaign=gli-usa-fissano-le-regole-di-cyber-security-per-le-missioni-spaziali