AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Newsletter

ANNO 2023 **n. 7/ 2023** **luglio 2023**

Safety, Cybersecurity delle AI: la standardizzazione come "chiave di volta"

Nella newsletter di maggio 2023 abbiamo già iniziato a ragionare insieme di AI e delle implicazioni sulla sicurezza degli individui o dei rischi di un uso malevolo. La proposta di legge di *AI Act europeo* è stato un primo passo proprio in questa direzione e rappresenta di fatto la prima legge sull'intelligenza artificiale da parte di un organismo regolatore di rilievo. La legge assegna le applicazioni dell'AI a tre categorie di rischio: la prima è costituita dalle applicazioni e dai sistemi che creano un rischio inaccettabile: ne sono esempi la manipolazione cognitivo-comportamentale di persone o specifici gruppi vulnerabili quali giocattoli ad attivazione vocale che incoraggiano comportamenti pericolosi nei bambini; oppure il punteggio sociale di matrice cinese che classifica le persone in base al comportamento, allo stato socio-economico o alle caratteristiche personali; o anche i sistemi di identificazione biometrica remota e in tempo reale, come il riconoscimento facciale. Il secondo livello è costituito dalle applicazioni ad alto rischio che devono essere soggette a requisiti legali specifici. I sistemi di AI che incidono negativamente sulla sicurezza o sui diritti fondamentali considerati ad alto rischio sono suddivisi in due categorie: i Sistemi di intelligenza artificiale utilizzati nei prodotti che rientrano nella legislazione dell'UE sulla sicurezza dei prodotti (include giocattoli, aviazione, automobili, dispositivi medici e ascensori); i sistemi di AI che rientrano in otto aree specifiche che dovranno essere registrate in una banca dati dell'UE: identificazione biometrica e categorizzazione delle persone fisiche; gestione e funzionamento delle infrastrutture critiche; istruzione e formazione professionale; occupazione, gestione dei lavoratori e accesso al lavoro autonomo; accesso e fruizione dei servizi privati essenziali e dei servizi e benefici pubblici; applicazione della legge; migrazione, asilo e gestione dei controlli alle frontiere; assistenza nell'interpretazione giuridica e nell'applicazione della legge.

Infine, ci sono le applicazioni non esplicitamente vietate perché non considerate ad alto rischio che quindi, in gran parte, sono lasciate non regolamentate.

Per i requisiti di trasparenza invece, l'AI generativa, (es. CHAT GPT), dovrebbe rispettare i requisiti di trasparenza: rivelare che il contenuto è stato generato dall'intelligenza artificiale, progettare il modello per evitare che generi contenuti illegali, pubblicare riepiloghi di dati protetti da copyright utilizzati per la formazione.

Per sostenere la decisione dei parlamentari europei sul testo in fase di proposta, l'ENISA (European Union Agency for Cybersecurity), Agenzia per la Sicurezza Europea, ha pubblicato nel marzo di quest'anno un documento dal titolo "*Cybersecurity of AI e Standardizzazione*", che fornisce una panoramica degli standard esistenti, in fase di elaborazione, in esame e pianificati, relativi alla sicurezza informatica dell'intelligenza artificiale (AI), per valutarne la copertura e identificare le lacune nella standardizzazione. Per farlo il documento considera le specificità dell'AI come ad esempio l'apprendimento automatico, coniugando sia la visione della sicurezza informatica ricompresa nel paradigma "tradizionale" di riservatezza-integrità-disponibilità, sia il concetto più ampio di affidabilità dell'AI. Infine, la relazione esamina in che modo la normazione può sostenere l'attuazione degli aspetti di cybersicurezza (questi stessi criteri sono incorporati nella proposta di regolamento dell'UE dell' AI Act - COM 2021- 206 final, n.d.r.).

Le conclusioni dello studio di ricerca e analisi hanno permesso di suggerire che gli standard generali per la sicurezza delle informazioni e la gestione della qualità (in particolare ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 9001) possono mitigare parzialmente i rischi di sicurezza informatica legati alla riservatezza, all'integrità e alla disponibilità dei sistemi di AI. Questa conclusione è basata sul presupposto che l'AI sia nella sua essenza software, e quindi ciò che è applicabile al software può essere applicato all'AI, se viene fornita una guida adeguata. Sebbene sia una generica raccomandazione, l'ENISA raccomanda un'integrazione basata su un'analisi specifica del sistema rispetto al dominio di applicazione (ad esempio basandosi su ISO/IEC 15408-1:2009).

Tuttavia, è ancora oggetto di dibattito fino a che punto la valutazione della conformità ai requisiti di sicurezza risultanti, possa basarsi su standard orizzontali specifici dell'AI e in che misura possa basarsi su standard verticali/settoriali specifici. Poiché la sicurezza informatica è trasversale a una serie di requisiti di affidabilità (ad esempio governance dei dati, trasparenza), è importante che le attività di standardizzazione relative a questi requisiti trattino la sicurezza informatica in modo coerente. Attualmente sono stati evidenziati dei gap di standardizzazione:

1. la tracciabilità dei dati e dei componenti dell'intelligenza artificiale durante il loro ciclo di vita resta un problema che attraversa la maggior parte delle minacce e rimane in gran parte irrisolto nella pratica;
2. le caratteristiche intrinseche del Machine learning non sono pienamente riflesse negli standard esistenti, soprattutto in termini di metriche e procedure di test;
3. in alcuni settori le tecnologie correlate sono ancora in fase di sviluppo e non sono ancora abbastanza mature per essere standardizzate (ovvero gli standard esistenti non possono essere adattati o i nuovi standard non possono ancora essere completamente definiti).

Per la messa in pratica della proposta di legge sull'AI act invece l'ENISA ha individuato che ad oggi non esistono norme che coprano adeguatamente la sicurezza informatica e descrivano le competenze delle organizzazioni per l'audit, la certificazione e il collaudo dei sistemi di AI (e dei sistemi di gestione dell'AI) e dei loro valutatori; tale lacuna nei settori oggetto di ricerca e sviluppo è rilevante per l'attuazione del progetto di legge sull'AI, in particolare per quanto riguarda le casistiche di dati alterati (*poisoning data*) e le applicazioni poste in essere dai criminali digitali.

Il testo dell'ENISA fornisce precise raccomandazioni finali su ogni fronte dei gap evidenziati e auspica un comune sforzo di continua analisi delle tecnologie in favore della standardizzazione come mezzo di supporto alla sicurezza informatica e un parallelo impegno per le valutazioni di conformità come guida della componente legislativa regolatoria.

Il 14 giugno 2023, i deputati hanno adottato una *posizione negoziale del Parlamento sulla legge* sull'AI che mira a garantire l'adozione di AI "sicure e trasparenti". Ora inizieranno i colloqui con i paesi dell'UE in sede di Consiglio sulla forma finale della legge. I materiali documentali e il documento fornito da ENISA costituiscono una solida base di lavoro.

L'obiettivo è raggiungere un accordo entro la fine di quest'anno.

Alessia Valentini

Consulente di Cybersecurity, Advisor e Giornalista. Fa parte delle "Women for Security" la community di Cyberladies nata nell'ambito del Clusit. È Giornalista presso l'ODG del Lazio dal 2013. Ha conseguito la certificazione CISA /ISACA nel 2017. È stata consigliere direttivo in Afcea (Armed Forces Electronic Association) dal 2014 al 2016

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

ATTIVITA' DELL'ASSOCIAZIONE

ATTIVITA' DI EDUCATION

Proseguono le attività di formazione per soci e simpatizzanti per l'anno 2023.

L'accordo con IsacaRoma consente ai soci AIIC di partecipare ai loro seminari (svolti principalmente in modalità webinar) su cybersecurity, risk management e protezione dei dati.

Stiamo valutando le modalità di svolgimento di altri eventi possibilmente – se le condizioni pandemiche lo consentiranno – in modalità mista, presenza e distanza.
Inoltre, come avrete notato, abbiamo ripreso le visite aziendali presso enti/imprese di rilevanza nazionale.
Vi terremo informati.
Vi ricordiamo anche che proprio per fornire un valore aggiunto ai nostri associati, alcuni eventi saranno riservati soltanto a chi è in regola con il pagamento delle quote associative.

RINNOVO ASSOCIATIVO ANNO 2023

Il 31 dicembre 2022 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare per tempo l'iscrizione alla nostra associazione versando il relativo contributo.
La partecipazione associativa inalterata da anni, pari ad euro 40, con delibera del Consiglio Direttivo del 19.9.2022 è stata aumentata di una modesta quota pari ad euro 10 per l'aumento generale dei costi di gestione.
La nuova quota per il rinnovo individuale è quindi adesso di euro 50 e può essere versata con bonifico sul conto corrente presso Banca Intesa Business, IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando come causale "rinnovo socio ordinario nome e cognome anno 2023".
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it. La nostra segreteria è a disposizione, per ogni informazione, alla mail segreteria@infrastrutturecritiche.it.
Ricordiamo ai soci che non hanno ancora rinnovato che **la data limite per il rinnovo annuale, come da regolamento, è fissata al 31 marzo 2023. Dopo questa data, si decade dalla qualifica di socio e sarà necessario procedere ad una nuova iscrizione versando anche il contributo per le spese di segreteria.**

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

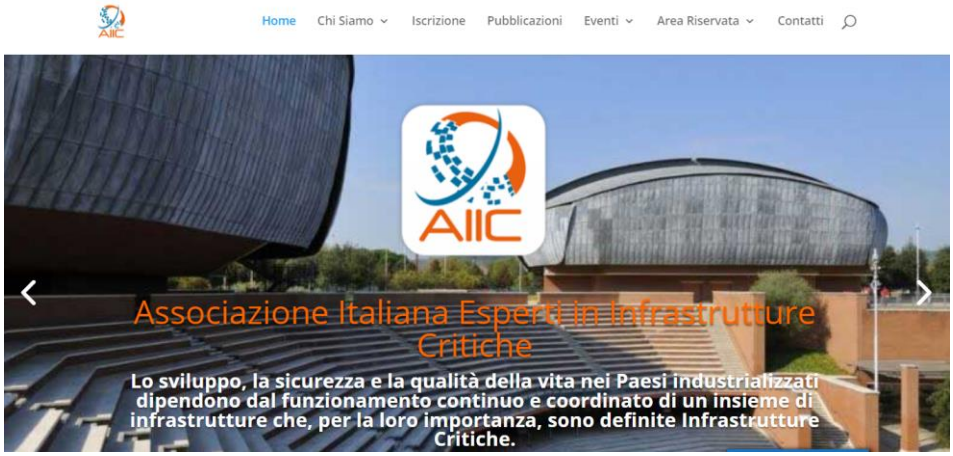
Ricordiamo ai soci che nella pubblicazione di un articolo o di un libro **non è possibile** firmarsi qualificandosi come "Associazione Italiana esperti in Infrastrutture Critiche", in quanto solo chi ha la rappresentanza legale dell'Associazione può esprimersi a nome AIIC.
La stessa regola vale anche se si partecipa ad un evento in qualità di organizzatore, relatore o chairman.

La possibilità di pubblicare o partecipare ad eventi a nome AIIC deve essere approvata dal Consiglio Direttivo dell'Associazione su richiesta del socio che, pertanto, è pregato di contattare il CD con ragionevole anticipo.

È invece raccomandato indicare, nel proprio profilo professionale, l'appartenenza ad AIIC, Associazione Italiana esperti in Infrastrutture Critiche, in qualità di socio.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Ricordiamo che è attivo il nuovo sito dell'Associazione Italiana Esperti in Infrastrutture Critiche.
L'indirizzo è sempre **www.infrastrutturecritiche.it** ma il sito è stato completamente rinnovato, sia nelle veste grafica che nei contenuti e nelle funzioni a disposizione.
Vi invitiamo a consultarlo e anche a farci pervenire le vostre osservazioni: i vostri suggerimenti sono sempre preziosi e ci aiutano a migliorare il prodotto.
Vi ricordiamo inoltre che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'associazione**, accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa.
Potete scriverci al nostro solito indirizzo email: *segreteria@infrastrutturecritiche.it*



NEWS E AVVENIMENTI

Un anno di cyber security nazionale: che cosa ha fatto l'ACN

La **relazione annuale dell'Agenzia per la Cyber Security Nazionale**, appena presentata alle Camere come stabilito dalla legge di istituzione, fornisce **un quadro completo delle attività, dei dati e dei progetti dell'ACN durante il periodo compreso tra il 1° gennaio e il 31 dicembre 2022**.

Indice degli argomenti

Un anno di cyber security nazionale

Tale anno di attività è stato caratterizzato da una complessa evoluzione dell'Agenzia, istituita tramite decreto nella seconda metà del 2021, e la necessità di lavorare tempestivamente sulla sicurezza cyber del Paese ha richiesto un'azione operativa anche durante il processo di strutturazione interna.

La strategia- *(continua…)*

https://www.cybersecurity360.it/outlook/un-anno-di-cyber-security-nazionale-che-cosa-ha-fatto-lacn/

Cybersecurity360*-Luisa Franchina-Tommaso Maria Ruocco -20 Giu 2023*

Intelligence, più efficienza e collaborazione con l'università: ecco la riforma Mantovano

Annunciato dal sottosegretario di Stato alla presidenza del consiglio, Alfredo Mantovano, un rinnovamento all'interno del comparto Intelligence per aumentarne l'efficienza e favorire una collaborazione più stretta con il settore della formazione universitaria. Ecco che c'è da sapere

In occasione del seminario "L'intelligence economica nell'era digitale" che si è tenuto presso la Luiss Business School di Roma, il sottosegretario di Stato alla presidenza del Consiglio Alfredo Mantovano ha annunciato che "è in corso nel settore dell'intelligence un lavoro di studio finalizzato a un **restyling del comparto per renderlo più efficiente, più funzionale ed evitare sovrapposizioni** che non avevano senso".

Indice degli argomenti

Una nuova veste del comparto Intelligence

Grazie a questo rinnovamento del comparto, si avrà "una migliore articolazione amministrativa, soprattutto nel settore economico finanziario con una disciplina seria delle garanzie funzionali, che non riguarda solamente il tema delle intercettazioni telefoniche".

Mantovano menziona l'estensione delle garanzie funzionali, per esonerare funzionari di Aise e Aisi da responsabilità penale in caso di azioni configurabili come reato all'interno del loro operato, argomento molto delicato, che merita, però, di essere affrontato.

Inoltre, dato che l'intelligence economica ha preso piede negli ultimi anni e la tecnologia si è affermata sempre più come settore centrale, è fondamentale puntare, secondo Mantovano, al potenziamento dell'innovazione tecnologica delle singole nazioni e allo snellimento delle filiere produttive. *(continua..)*

https://www.cybersecurity360.it/cybersecurity-nazionale/intelligence-piu-efficienza-e-collaborazione-con-luniversita-ecco-la-riforma-mantovano/
Cybersecurity360- *Marco Santarelli- 29 Giu 2023*

Ransomware Halts Operations at Japan's Port of Nagoya
LockBit 3.0 claims responsibility for the cyberattack that shuttered the largest port in Japan, according to authorities.
Cargo containers filled with imports and exports from all over the world have been stuck at the Port of Nagoya following a ransomware attack on its networks early Tuesday morning.
The port is the largest in Japan and the central shipping hub for international carmaker Toyota. According to its operator, Nagoya Harbor Transportation, it received a ransom demand from LockBit 3.0 after a system failure on Tuesday at 6:30 a.m., the Japan Times reported.
The port authority said it expects to resume operations on Thursday morning.
"We will closely monitor any impact on production while carefully examining the parts inventory," Toyota told the Japan Times.
LockBit 3.0 is a prolific Russian-based ransomware operation used to target organizations, including the Italian Tax Agency.
https://www.darkreading.com/attacks-breaches/ransomware-halts-operations-at-japan-port-of-nagoya
Dark Reading - *Dark Reading Staff -July 05, 2023*

New tool exploits Microsoft Teams bug to send malware to users
A member of U.S. Navy's red team has published a tool called TeamsPhisher that leverages an unresolved security issue in Microsoft Teams to bypass restrictions for incoming files from users outside of a targeted organization, the so-called external tenants.
The tool exploits a problem highlighted last month by Max Corbridge and Tom Ellson of UK-based security services company Jumpsec, who explained how an attacker could easily go around Microsoft Teams' file-sending restraints to deliver malware from an external account.
The feat is possible because the application has client-side protections that can be tricked into treating an external user as an internal one just by changing the ID in the POST request of a message.
Streamlining attacks on Teams
'TeamsPhisher' is a Python-based tool that provides a fully automated attack. It integrates the attack idea of Jumpsec's researchers, techniques developed by Andrea Santese, and authentication and helper functions from Bastian Kanbach's 'TeamsEnum' tool.
"Give TeamsPhisher an attachment, a message, and a list of target Teams users. It will upload the attachment to the sender's Sharepoint, and then iterate through the list of targets," reads the description from Alex Reid, the developer of the red team utility. *(continua…)*
https://www.bleepingcomputer.com/news/security/new-tool-exploits-microsoft-teams-bug-to-send-malware-to-users/
Bleepingcomputer - *Bill Toulas - July 5, 2023*

Le priorità cyber degli Usa commentate dall'avvocato Mele
Il bilancio è in linea con i pilastri della strategia nazionale. Comprendere l'agenda americana serve "non solo per posizionarci nella scia del nostro più importante alleato, ma anche per cogliere quelle che

potrebbero essere per il nostro Paese alcune delle priorità politiche in questo settore", commenta Stefano Mele (Gianni & Origoni)

Da poco più di quattro cinque mesi gli Stati Uniti hanno una nuova Strategia nazionale di cybersicurezza per uno spazio digitale difendibile, resiliente e in linea con i valori democratici. Da più cinque mesi, invece, **Kemba Walden** ha assunto il ruolo di National Cyber Director *ad interim* dopo le dimissioni di metà febbraio di **Chris Inglis**, primo a svolgere tale incarico alla Casa Bianca. In estate dovrebbe essere pubblicato il piano di attuazione della Strategia nazionale di cybersicurezza.

Nonostante questa situazione, l'Ufficio del direttore nazionale per la cybersicurezza e l'Ufficio per la gestione e il bilancio hanno pubblicato un memorandum che delinea le cinque priorità di bilancio per la cybersecurity per i dipartimenti e le agenzie federali per l'anno fiscale 2025, in linea con gli altrettanti pilastri della nuova strategia: difendere le infrastrutture critiche; distruggere e smantellare i cyber-attaccanti; modellare le forze di mercato per promuovere la sicurezza e la resilienza; investire in un futuro resiliente; creare partnership internazionali per perseguire obiettivi condivisi. *(continua…)*

https://formiche.net/2023/07/le-priorita-cyber-degli-usa-commentate-dallavvocato-mele/

***FORMICHE** - Gabriele Carrer - 06/07/2023 -*

Cybercrime, attacco ransomware all'Azienda Ospedaliera Luigi Vanvitelli di Napoli

Attacco ransomware all'Azienda Ospedaliera Luigi Vanvitelli di Napoli. L'ACN invia una squadra di esperti del CSIRT per contribuire all'analisi dell'attacco e al ripristino dei sistemi impattati. L'Azienda Ospedaliera Universitaria Luigi Vanvitelli di Napoli ha reso noto di essere stata vittima di un cyber attacco di tipo ransomware e che sono in corso valutazioni per definire la sua portata, oltre che la natura dei dati oggetto della violazione. Lo rende noto l'Agenzia per la Cybersicurezza Nazionale (ACN), che ha inviato una propria squadra di esperti di cybersecurity presso il nosocomio napoletano per contribuire all'analisi dell'attacco e al ripristino dei sistemi impattati. "Il CSIRT, la squadra operativa dell'Agenzia, sta lavorando da stamattina per comprendere le esatte dimensioni dell'attacco e dare ogni forma di supporto all'ospedale napoletano per un ripristino che ci auguriamo possa essere rapido ed efficace – ha dichiarato il Direttore Generale dell'ACN, il prefetto Bruno Frattasi -. Rinnovo, pertanto, l'invito a tutte le realtà pubbliche del settore sanitario, i più impattati nel nostro Paese, a proteggere i propri sistemi informatici adottando le soluzioni tecniche ed organizzative del caso, anche attraverso il loro aggiornamento costante per non cadere vittima di questi attacchi. (continua…).

https://www.difesaesicurezza.com/cyber/cybercrime-attacco-ransomware-allazienda-ospedaliera-luigi-vanvitelli-di-napoli/

***Difesa e Sicurezza** -Francesco Bussoletti -6 Luglio 2023*

A man from Tracy, California, has been charged with a computer attack on the Discovery Bay water treatment facility.

Rambler Gallo (53), a man from Tracy (California) has been charged with intentionally causing damage to a computer after he allegedly breached the network of the Discovery Bay Water Treatment Facility.

The man targeted the water treatment facility in the Town of Discovery Bay, California, which provides treatment for the water and wastewater systems for the town's 15,000 residents. Gallo was an employee of a private Massachusetts-based company (Company A), which contracted with Discovery Bay to operate the town's wastewater treatment facility.

According to the press release published by the DoJ, Gallo intentionally uninstalled the main operational and monitoring system for the water treatment plant and then shut down off the servers running those systems.

"The indictment alleges that while Gallo was employed with Company A, he installed software on his own personal computer and on Company A's private internal network that allowed him to gain remote access to Discovery Bay's Water Treatment facility computer network. Then, in January of 2021, after Gallo had resigned from Company A, he allegedly accessed the facility's computer system remotely and transmitted a command to uninstall software that was the main hub of the facility's computer network and that protected the entire water treatment system, including water pressure, filtration, and chemical levels." states the DoJ.
"The indictment charges Gallo with one count of transmitting a program, information, code, and command to cause damage to a protected computer, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)(i)."
The man faces up to 10 years in prison and a $250,000 fine, and the court may order an additional term of supervised release, additional assessments, and restitution, if appropriate.
In March 2023, the Biden administration **announced** that it will make it mandatory for the states to conduct cyber security audits of public water systems. *(continua…)*
https://securityaffairs.com/148258/cyber-crime/discovery-bay-water-treatment-facility-attck.html
Security Affairs- *Pierluigi Paganini- July 7, 2023*

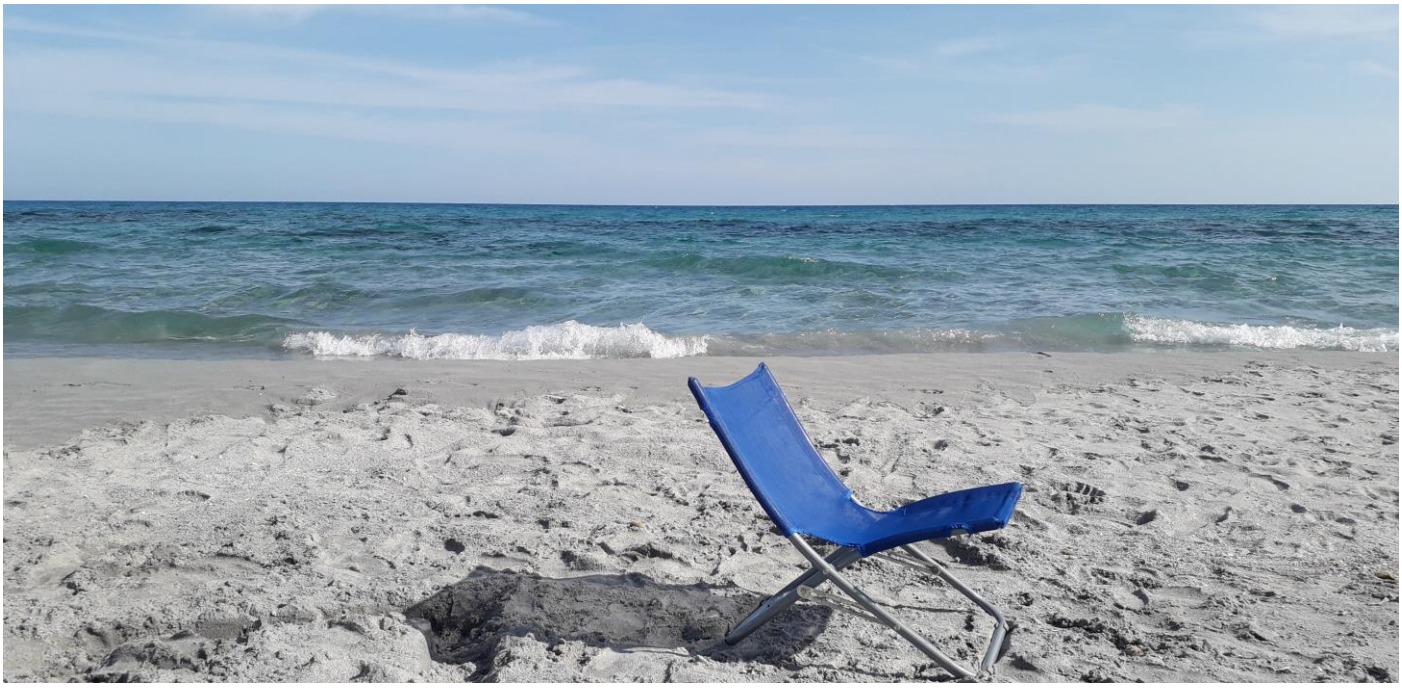
Iran-linked APT group tracked TA453 has been linked to a new malware campaign targeting both Windows and macOS systems.
The Iran-linked threat actor TA453 has been linked to a malware campaign that targets both Windows and macOS.
TA453 is a nation-state actor that overlaps with activity tracked as Charming Kitten, PHOSPHORUS, and APT42.
TA453 in May 2023 started using LNK infection chains instead of Microsoft Word documents with macros.
The spear-phishing message appears as a benign conversation lure masquerading as a senior fellow with the Royal United Services Institute (RUSI) to the public media contact for a nuclear security expert at a US-based think tank focused on foreign affairs.
The messages demand feedback on a project called "Iran in the Global Security Context" and requested permission to send a draft for review.
"The initial email also mentioned participation from other well-known nuclear security experts TA453 has previously masqueraded as, in addition to offering an honorarium. TA453 eventually used a variety of cloud hosting providers to deliver a novel infection chain that deploys the newly identified PowerShell backdoor GorjolEcho." reads the analysis published by Proofpoint. "When given the opportunity, TA453 ported its malware and attempted to launch an Apple flavored infection chain dubbed NokNok by Proofpoint. TA453 also employed multi-persona impersonation in its unending espionage quest."
The researchers observed the TA453 using a variety of cloud hosting providers to deliver a new infection chain aimed at deploying a new PowerShell backdoor dubbed GorjolEcho. *(continua…)*
https://securityaffairs.com/148275/apt/ta453-malware-windows-macos.html
Security Affairs- *Pierluigi Paganini- July 8, 2023*

PROSSIMI EVENTI

La "AEIT - Associazione Italiana di Elettrotecnica, Elettronica, Automazione, Informatica e Telecomunicazioni", costituita il 1° gennaio 1897, dal 1° novembre 2013 ha assunto la attuale

denominazione. Nella AEIT è confluita la AIIT - Associazione Italiana Ingegneri delle Telecomunicazioni, fondata nel 1962. Dal 1910, con un Regio Decreto, la AEIT ha ricevuto il riconoscimento di "Ente Morale".
Da 5 al 7 ottobre AEIT terrà la 115 International conference. La call for papers è a: https://convegni.aeit.it/aeit2023/documenti/aeit2023_save_the_date.pdf

Come ogni anno, la nostra Newsletter AIIC va in vacanza. Ci rivedremo a settembre. Buone ferie!



NOTIZIE D'INTERESSE:

Le indicazioni per chi vuole iscriversi come nuovo socio sono contenute nel sito AIIC al link *http://www.infrastrutturecritiche.it/new/per-iscriversi/*

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo email o altro) di comunicare I nuovi dati a segreteria@infrastrutturecritiche.it. La mancanza di tali comunicazioni potrebbe impedire, al socio, la ricezione delle comunicazioni.

RIFERIMENTI DELL'ASSOCIAZIONE

AIIC è una associazione apolitica il cui scopo è promuovere attività e conoscenze nell'ambito delle infrastrutture critiche, della loro gestione, protezione e sicurezza.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Per maggiori informazioni sull'Associazione inviare una mail a
segreteria@infrastrutturecritiche.it
o visitate il sito
www.infrastrutturecritiche.it

ATTENZIONE

Per ricevere questa newsletter è necessario inviare una richiesta all'indirizzo
segreteria@infrastrutturecritiche.it

L'iscrizione alla newsletter NON comporta alcun onere e non è richiesta la comunicazione di alcun dato personale ad eccezione dell'indirizzo di posta elettronica.

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Urbino 31 – 00182 ROMA Tel. +39 06 64871209 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirsi al gruppo si può usare il link http://www.linkedin.com/ groups/96335
Versione stampabile della newsletter	Nella sezione "Newsletter"del sito http://www.infrastrutturecritiche.it è disponibile l'archivio delle Newsletter.
Comitato di Redazione	Alberto Traballesi Glauco Bertocchi Silvano Bari Gianluca Cipriani Andrea Agostino Fumagalli *ai quali potete inviare suggerimenti e quesiti scrivendo a:* *segreteria@infrastrutturecritiche.it*

La NewsLetter ha lo scopo di rendere note le principali informazioni nell'ambito delle Infrastrutture Critiche e le attività dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC). Tutti i contenuti relativi alla sezione NEWS e Eventi sono pubblici on line e di proprietà dei rispettivi editori.