AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Newsletter

ANNO 2022	N. 4/ 2022	Aprile 2022

L'intelligenza artificiale ha imparato a programmare, quali conseguenze per le aziende?

Dopo aver imparato a parlare e a scrivere, l'intelligenza artificiale (IA) ora sta imparando a programmare. L'automazione avanzata sta facendo passi da gigante nelle mansioni che potremmo definire di concetto: se poco tempo fa ci si stupiva per un sistema IA che risolveva un ticket o che sosteneva correttamente una conversazione al telefono, oggi osserviamo come l'asticella si va alzando inesorabilmente sempre più in alto. Le stesse tecnologie alla base della comprensione del linguaggio vengono ora usate per conferire ai sistemi IA la capacità di scrivere righe di codice.

L'anno scorso OpenAI, l'azienda di San Francisco che pochi anni fa rilasciò un importante modello di comprensione e generazione del linguaggio chiamato GPT-3, ha lanciato un prodotto chiamato GitHub Copilot, sviluppato in collaborazione con GitHub di Microsoft. Copilot affianca lo sviluppatore umano generando suggerimenti di completamento per il programma che si sta modificando, basandosi sia sui commenti all'interno del file, sia sul codice scritto in precedenza. Ciò significa, in sostanza, che quando un programmatore inizia a scrivere codice, dopo un po' Copilot "capisce" cosa sta cercando di fare l'essere umano e inizia a suggerire diversi modi per completare il codice. Il meccanismo funziona più o meno allo stesso modo in cui diversi software di comunicazione ci suggeriscono quale parola scrivere quando iniziamo a digitare le prime lettere.

Il sistema è molto potente, perché addestrato su miliardi di codici pubblici ospitati su GitHub. Ma Copilot, come suggerisce il nome, non mira a rimpiazzare lo sviluppatore umano, bensì ad assisterlo come un fedele co-pilota. Il sistema IA non è in grado di scrivere programmi interamente da solo, non quando la qualità del codice o semplicemente il corretto funzionamento del programma sono fattori importanti. Le sue funzioni sono utili per aiutare gli sviluppatori a superare passaggi tediosi o per suggerire soluzioni a cui non avevano pensato. Bisogna poi essere consci di alcune sue limitazioni. Ad esempio, poiché il modello è stato addestrato con repository pubblici, potrebbe suggerire frammenti di codice provenienti da vecchi moduli o da vecchie librerie, rischiando così di inserire codice obsoleto nel programma.

Per diversi mesi GitHub Copilot è stato l'unico software di questo tipo. Poi qualche settimana fa anche DeepMind (che fa parte della galassia Google) è scesa in campo con il suo sistema in grado di scrivere codice. AlphaCode, questo il nome del modello IA, è stato addirittura in grado di posizionarsi a metà classifica in una competizione di programmazione, risolvendo problemi che necessitavano di logica, generazione di algoritmi, pensiero critico, comprensione del linguaggio naturale e ovviamente sviluppo di codice. Non facciamoci ingannare dalla posizione a metà classifica: si tratta di un grande successo per un sistema al suo esordio, in particolare in un ramo dell'intelligenza artificiale finora scarsamente battuto.

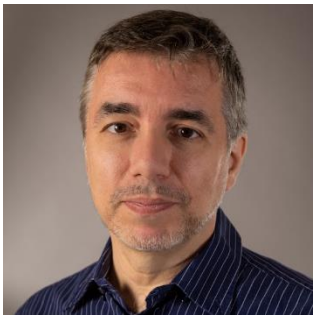
Fin qui le notizie. Ora però non possiamo fare a meno di pensare a come cambieranno le cose per gli sviluppatori che lavorano nelle nostre aziende e per i programmi che girano nei nostri sistemi, anche *mission critical*. Anzitutto, nel breve termine i potenziamenti derivanti dall'intelligenza artificiale saranno d'aiuto a chi oggi sviluppa codice, vuoi per velocizzare alcuni passaggi tediosi, vuoi per trovare

soluzioni a problemi dove da soli non si riusciva a venirne a capo. Il risultato è che gli attuali sviluppatori avranno una funzione in più su cui poter contare.

Dal lato dell'azienda, tuttavia, è innegabile che se per realizzare lo stesso software in futuro serviranno sette persone anziché dieci, potremo prevedere una contrazione dei team di sviluppo, in particolare per quello che riguarda gli sviluppatori entry-level, quelli cioè alle prime armi e indirizzati dai colleghi a occuparsi dei compiti più tediosi e ripetitivi.

Sul piano del codice prodotto dall'IA, attualmente gli sviluppatori più esperti esprimono perplessità sulla capacità di programmazione dell'intelligenza artificiale, trovando talvolta codice inadeguato, proveniente magari da librerie obsolete, inutilmente gonfiato e, in alcune occasioni, con bug. Si tratta però delle stesse obiezioni che qualche anno fa venivano mosse ai sistemi IA di scrittura, che oggi hanno invece raggiunto livelli estremamente sofisticati. È probabile che in pochi anni anche i sistemi IA di programmazione raggiungeranno velocemente livelli avanzati, producendo codice in linea con gli standard richiesti dalle aziende. A quel punto si procederà alla stessa trasformazione che abbiamo visto, ad esempio, nel mondo delle traduzioni, dove il lavoro umano si sta spostando via dalla prima stesura – la traduzione vera e propria – per finire nel *proofreading*, ovvero nel passaggio successivo dove si controlla e si migliora il lavoro svolto dalle macchine.

In ogni caso sarà assolutamente necessario che le aziende impegnate nella realizzazione di software per le infrastrutture critiche (IC), oltre che le stesse IC, siano al corrente di questi nuovi sviluppi e che osservino con attenzione come viene creato il codice dei programmi che andranno a far funzionare i loro sistemi critici. Non sarà possibile, oltre che futile, cercare di prevenire o limitare l'uso dell'IA generatrice di codice, ma sarebbe opportuno chiedere e ottenere trasparenza su quali porzioni di codice sono state realizzate da un sistema di intelligenza artificiale, effettuando magari verifiche addizionali su quei passaggi.



Luca Sambucci è Head of Artificial Intelligence di SNGLR Holding AG, un gruppo svizzero specializzato in tecnologie esponenziali con sedi in Europa, USA e UAE, dove cura i programmi inerenti all'intelligenza artificiale. Dopo la laurea in Management ha conseguito una specializzazione in Business Analytics a Wharton, una certificazione Artificial Intelligence Professional da IBM e una sul machine learning da Google Cloud. Ha trascorso la maggior parte della carriera – trent'anni - nel settore della cybersecurity, dove fra le altre cose è stato consigliere del Ministro delle Comunicazioni e consulente di Telespazio (gruppo Leonardo). Oggi si occupa prevalentemente di intelligenza artificiale, con consulenze sull'AI per le infrastrutture critiche per la Commissione Europea, in particolare con la European Defence Agency e il Joint Research Centre. Cura il sito di notizie sull'intelligenza artificiale **www.Notizie.ai**.

ATTIVITA' DELL'ASSOCIAZIONE

AIIC augura una serena Pasqua a tutti i nostri lettori e alle loro famiglie

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

ELEZIONI PER IL RINNOVO DEL CONSIGLIO DIRETTIVO DI AIIC

Il Consiglio Direttivo uscente, nella sua riunione del 28 gennaio 2022, ha deliberato di fissare al 6 e 7 giugno 2022, tramite piattaforma online, la data per le elezioni del nuovo Consiglio Direttivo.
Tutte le informazioni e il Regolamento Elettorale sono stati messi a disposizione dei Soci sia tramite invio email sia tramite pubblicazione sul sito web.

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.

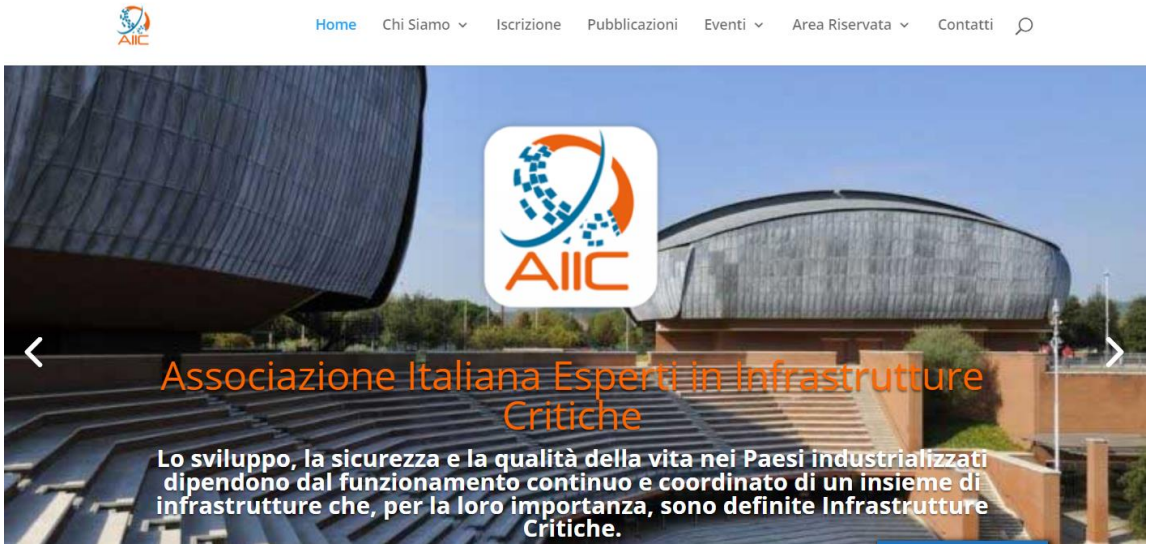
AIIC ha sottoscritto convenzioni di collaborazione con altre Associazioni. In particolare con:

- **ARPIC –** La convenzione tra AIIC e ARPIC (Romanian Association for Critical Infrastructures and Services Protection) è entrata in vigore il 01/04/2012. ARPIC e AIIC, hanno concordato di collaborare sulla base di una partnership attiva, con lo scopo di:
usare la loro esperienza comune per aiutare l'implementazione di aspetti critici del concetto di infrastruttura nell'ambito dell'UE e del quadro giuridico nazionale,
costruire e promuovere una rete europea di organizzazioni professionali ed esperti che lavorino nel campo dei servizi e della protezione delle infrastrutture critiche.
- **CENTRO RICERCHE THEMIS** – la convenzione tra AIIC e THEMIS è stata firmata il 21 marzo 2016. Le due Associazioni si sono impegnate a collaborare per la realizzazione congiunta di iniziative e servizi da proporre agli associati, secondo forme e modalità da stabilire con appositi accordi.
- **EUCONCIP** – AIIC è membro fondatore di EUCONCIP (European Cooperation Network on Critical Infractructures Protection) assieme a Fondazione Formit, ARPIC (Romanian Asociation for Critical Infrastructures and Services Protection), CCI (Centro de Ciberseguridad Industrial), CESS (Centre for European Security Strategies), S21Sec. EUCONCIP è un'associazione con sede legale in Italia, costituita nel 2016 con lo scopo di promuovere la cooperazione tra paesi e tra settori nel campo della protezione delle infrastrutture critiche. L'obiettivo principale di EUCONCIP è contribuire allo sviluppo di un approccio armonizzato da adottare per la protezione delle infrastrutture critiche che sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza, del benessere economico e sociale delle persone (Direttiva UE 2008/114 / CE).

- **AFCEA ROMA** - la convenzione tra AIIC e AFCEA – Armed Forces Communications & Electronics Association – Capitolo di Roma è stata firmata il 18 settembre 2017. Scopo della convenzione è di promuovere principi e tecniche professionali reciproche e di interesse per entrambe le Associazioni, avvicinando così le due community nazionali su tematiche comuni. La collaborazione permetterà di dare evidenza a eventi organizzati da ciascuna associazione, attraverso i propri canali di comunicazione, e di sviluppare e sostenere iniziative congiunte su temi di comune interesse.
- **AIAS** – la convenzione tra AIIC e AIAS Associazione professionale Italiana Ambiente e Sicurezza) è stata firmata il 15 febbraio 2016 con durata triennale. Le due associazioni intendono promuovere forme di collaborazione tra le attività di AIAS e delle sue società appartenenti al Networkaias e precisamente AIAS Academy e di AIASCert e le attività di AIIC al fine di promuovere una cultura applicativa di una prevenzione efficace che tenga conto di tutti gli aspetti di sicurezza
- **CLOUD SECURITY ALLIANCE ITALY CHAPTER –** la convenzione tra AIIC e CLOUD SECURITY ALLIANCE ITALY CHAPTER è stata firmata il 26 aprile 2012, con l'intento di collaborare per dare reciprocamente visibilità alle iniziative sviluppate autonomamente da ciascuna delle due associazioni in occasione di incontri, corsi e seminari di studio.
- **ISACA Rome Chapter** La convenzione con ISACAROMA (capitolo di Roma della *Information Systems Audit And Control Association*, associazione internazionale con circa 140.000 soci nel mondo) è stata firmata il 7 dicembre 2018 con l'intento promuovere la collaborazione tra le due associazioni per l'organizzazione di eventi, seminari sulla cyber security e le infrastrutture critiche.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

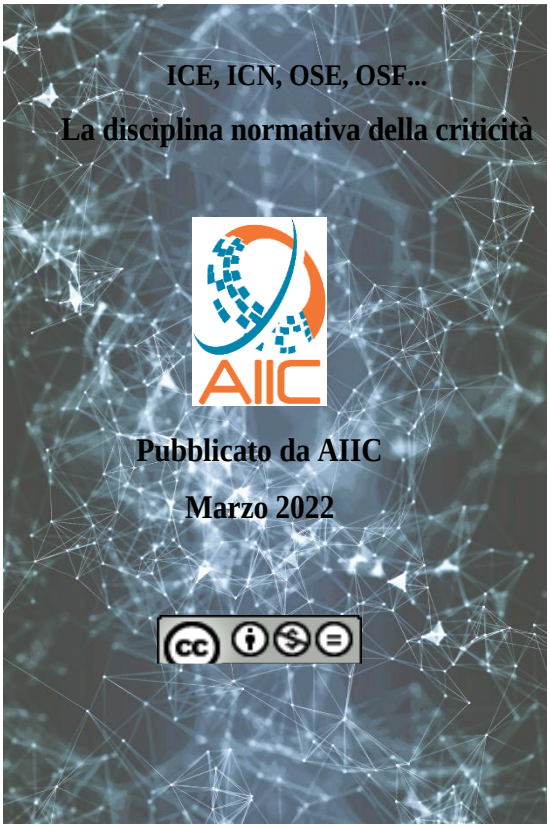
Ricordiamo che è attivo il nuovo sito dell'Associazione Italiana Esperti in Infrastrutture Critiche.
L'indirizzo è sempre **www.infrastrutturecritiche.it** ma il sito è stato completamente rinnovato, sia nelle veste grafica che nei contenuti e nelle funzioni a disposizione.
Vi invitiamo a consultarlo 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*

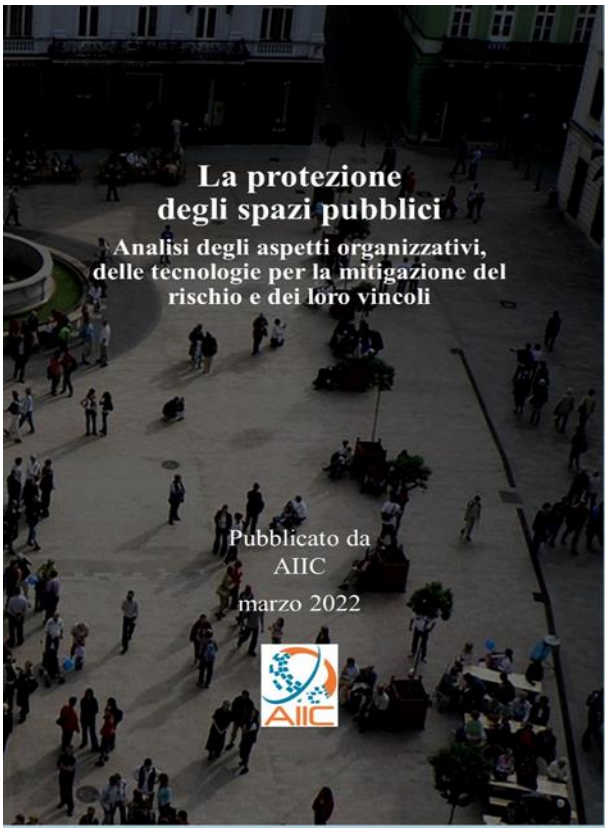


AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

GRUPPI DI LAVORO AIIC

Sono terminati i due Gruppi di Lavoro AIIC su **"Disciplina normativa della criticità**" coordinato da Luisa Franchina e su **"Protezione degli spazi pubblici**" coordinato da Sandro Bologna. Due apposite pubblicazioni, sono disponibili nella Pagina HOME del sito dell'Associazione *https://infrastrutturecritiche.it/.* I risultati verranno presentati, ai soci e ai non soci, in occasione di prossimi incontri, in presenza o on-line.
Di seguito le copertine delle due pubblicazioni.





NEWS E AVVENIMENTI

Sicurezza IoT: il conflitto in Ucraina genera nuovi allarmi - Dalla Cybersecurity and Infrastructure Agency statunitense, dal National Cyber Security Center e dal Cyber Security Incident Response Team italiano arriva l'allarme: il conflitto russo-ucraino si combatte anche nello spazio cyber. A rischio infrastrutture critiche, organizzazioni finanziarie e sanitarie.
Di sicurezza IoT, in particolare in relazione a tutto quanto attiene sia all'IoT industriale, sia all'IoT applicato alle infrastrutture critiche, abbiamo scritto molto su queste pagine, mettendo in luce come l'assenza di policy adeguate, unita a una non trascurabile complessità tecnica dovuta alla pluralità di dispositivi e protocolli, abbia aperto la strada ad attacchi che hanno compromesso l'operatività delle imprese e la sicurezza delle infrastrutture.
In questo scenario, di per sé già critico, si aggiungono oggi allarmi ulteriori, correlati, come è facile intuire, al conflitto in Ucraina.

Indice degli argomenti
L'allarme della CISA statunitense e dell'NCSC britannico
Chi ricorda NotPetya?
Le contromisure da implementare
(continua)
https://www.internet4things.it/sicurezza-iot/sicurezza-iot-il-conflitto-in-ucraina-genera-nuovi-allarmi/
INTERNET4THINGS *- Maria Teresa Della Mura - 2 Marzo 2022*

Guerra, perché non c'è stato ancora nessun vero attacco informatico - Finora solo disinformazione, ddos e qualche malware dall'effetto limitato. La cyberwar si fa attendere. Vari esperti internazionali si interrogano a riguardo. Diversi i motivi. E la guerra tra Russia e Ucraina ci permette così anche di capire meglio il ruolo di una cyber war in un conflitto.
L'invasione russa dell'Ucraina ha sfruttato moltissime armi basate su sofisticate tecnologie dai droni ai missili di crociera ad armi anticarro ed anti elicotteri. A questi scontri fisici si sono accoppiate battaglie sui social media per la diffusione di informazioni che sono arrivate fino ad utilizzare i referaggi dei ristoranti per diffondere notizie sull'invasione e violare cosi la censura russa e i classici ddos a siti di banche e istituzione per seminare caos.
Ma chi, come il sottoscritto, immaginava che gli attacchi fisici fossero accompagnati da attacchi informatici, una delle caratteristiche distintive di un conflitto del 21° secolo, è stato fino ad ora smentito.
Indice degli argomenti
I pochi attacchi informatici in Ucraina
Perché la cyber non gioca un ruolo nella guerra
Aiuto degli alleati
Non c'è bisogno di attacchi cyber quando la guerra è scoppiata
Evitare una escalation
Ma ancora non è detta l'ultima parola: la cyber war in arrivo
(continua)
https://www.agendadigitale.eu/sicurezza/perche-non-ci-sono-attacchi-informatici-nella-guerra-in-ucraina/
Agenda Digitale *- Fabrizio Baiardi - 04 Mar 2022*

Droni per valutare lo stato dei ponti ferroviari: i vantaggi nell'utilizzo delle tecnologie - L'utilizzo dei sistemi aerei a pilotaggio remoto (SAPR – droni) rappresenta una tecnologia promettente nell'applicazione delle ispezioni dei ponti. RFI S.p.A. (Rete Ferroviaria Italiana) ha avviato negli ultimi anni una campagna di sperimentazioni al fine di approfondire e comprendere come tale tecnologia possa fornire un valido contributo per l'esecuzione delle visite ispettive delle opere d'arte. Nel presente articolo vengono illustrati i principali risultati delle attività svolte.
La Rete Ferroviaria Italiana
La rete ferroviaria italiana, per la particolare e complessa struttura orografica del territorio nazionale, è in Europa tra quelle con il maggior numero di ponti. La maggior parte dell'infrastruttura esistente si è sviluppata a partire dalla seconda metà del secolo XIX. RFI S.p.A. (Rete Ferroviaria Italiana) gestisce, in 16.7821 km, circa 23.100 opere d'arte (ponti, viadotti, sottovia/sottopassi, cavalcavia e sovrappassi).

Il bacino totale delle opere d'arte presenti sul territorio italiano è composto per il 37% da sottovia/sottopassi, per il 34% da ponti, per il 22% da cavalcavia e per il 7% da viadotti.

L'esigenza di valutare lo stato di manutenzione delle opere

Al fine di monitorare l'intera rete ferroviaria e di valutare lo stato di conservazione e di manutenzione delle opere d'arte (ossia ponti, viadotti, sottovia, etc.), RFI, in accordo con quanto prescritto dalla normativa nazionale ed internazionale, prevede un ciclo di visite ispettive per i ponti, viadotti e sottovia su base sessennale. In particolare, sono previste visite ispettive con frequenza annuale, definite "ordinarie", quelle con cadenza triennale, o anche chiamate "principali", ed infine quelle ogni sei anni, definite "generali". Dal 2014 è stato aggiornato il contesto normativo aziendale al fine di garantire l'integrità, la sicurezza, la regolarità e la funzionalità dell'esercizio ferroviario attraverso l'emissione della Procedura "Visite di controllo ai ponti, alle gallerie e alle altre opere d'arte dell'infrastruttura ferroviaria" e della Metodologia Operativa

(continua)

https://www.ingenio-web.it/33910-droni-per-valutare-lo-stato-dei-ponti-ferroviari-i-vantaggi-nellutilizzo-delle-tecnologie

INGENIOWEB **-** *Iacobini Franco, Vecchi Andrea, Lopez Nazzareno, Polimanti Giulia, Fussotto Marco - 11/03/2022*

Cyber crime, le minacce al sistema bancario e al settore energetico - L'attuale crisi russo-ucraina conferma che sempre più spesso i conflitti coinvolgono anche operazioni ibride caratterizzati da attacchi informatici mirati alle infrastrutture critiche, specialmente nei settori dell'energia e dei servizi finanziari. Ecco quali sono le minacce e le possibili misure di contrasto.

La guerra in Ucraina è uno dei tanti conflitti che coinvolgono operazioni ibride e che includono attacchi informatici ai danni di infrastrutture critiche altamente vulnerabili, specialmente nei settori dell'energia e dei servizi finanziari che archiviano, gestiscono e trasferiscono enormi volumi di dati personali.

Questo è stato particolarmente chiaro durante l'ondata di attacchi avvenuta all'inizio del 2022.

Infatti, in seguito all'invasione dell'Ucraina il 24 febbraio e alle conseguenti sanzioni imposte a Mosca nei giorni successivi, si sono moltiplicati gli allarmi per possibili attacchi informatici contro tali infrastrutture in risposta alle azioni intraprese dall'Occidente e dai suoi alleati nei confronti del Cremlino.

Uno degli obiettivi più indicati come possibile bersaglio di questo tipo di azioni sono gli istituti bancari. Secondo un rapporto pubblicato dalla Banca d'Italia nel marzo 2022 intitolato "Cyber resilience per la continuità di servizio del sistema finanziario", benché la minaccia cyber sia per sua stessa natura trasversale, il settore finanziario è un obiettivo privilegiato degli attacchi in quanto i target includono un variegato numero di attori come banche centrali, banche commerciali, fornitori di sistemi di pagamento, money transfer, società per lo scambio di criptovaluta, altre organizzazioni finanziarie nonché utenti.

Gli attacchi in ambito finanziario sono sempre più mirati allo sfruttamento di specifiche vulnerabilità e caratteristiche delle singole organizzazioni.

Indice degli argomenti

La risposta dell'Europa
Le vulnerabilità dell'ecosistema energetico globale
(continua)
https://www.cybersecurity360.it/nuove-minacce/cyber-crime-le-minacce-al-sistema-bancario-e-al-settore-energetico
***Cybersecurity360** - Davide Agnello, Valeria Rosati - 14 Mar 2022*

Mobilità e sostenibilità mettono una marcia in più grazie alle missioni spaziali - Le auto a guida autonoma saranno un aggregato di tecnologie nate per lo spazio, altre sono già negli smartphone e al nostro fianco nella sfida contro il climate change. Dalle sfide più estreme per spingere l'esplorazione dell'universo sempre più avanti, nascono soluzioni che stanno rivoluzionando la mobilità e molti altri settori. Il problema resta il trasferimento tecnologico: secondo Patrizia Caraveo (Inaf) più che tanti uffici servirebbero continui contatti tra ricerca e industria. Altrimenti le grandi scoperte resteranno soluzioni a problemi non (ancora) noti.
Sesta al mondo per spese spaziali in rapporto al PIL, terza contribuente dell'ESA con quasi 600 milioni di euro e dotata di agenzia spaziale con budget a 9 zeri, l'Italia investirà nello spazio anche 1,49 miliardi del PNRR. Queste cifre vanno moltiplicate per 5 per ottenere il valore che la filiera industriale può ricavare dalle tecnologie nate nello Spazio se saprà "metterle a terra".
A sottolinearlo è l'astrofisica dirigente di ricerca dell'Istituto Nazionale di Astrofisica (Inaf) Patrizia Caraveo, raccontando il contributo dell'astrofisica nel campo della mobilità e della sostenibilità terrestri. "I soldi spesi nello spazio non sono investimenti a fondo perduto, anzi: sono sempre più redditizi. Basta chiedersi da dove sono nate molte delle tecnologie oggi utilizzate nel quotidiano oppure quelle che compongono le auto a guida autonoma".
Indice degli argomenti
Più sicurezza a terra con GPS e sensori lidar dallo spazio
Per imparare a riciclare basta chiedere agli astronauti
Prossima missione spaziale: avvicinare ricerca e industria
(continua)
https://www.zerounoweb.it/cio-innovation/mobilita-e-sostenibilita-mettono-una-marcia-in-piu-grazie-alle-missioni-spaziali/
***ZEROUNOWEB** - Marta Abba' - 15 Mar 2022*

La forza rivoluzionaria di IoT nel settore finanziario - Internet of Things è uno dei principali abilitatori di trasformazione digitale del settore finanziario, con applicazioni efficaci soprattutto in ambito di sicurezza, efficienza e customer experience. Dai sistemi antifrode ai servizi innovativi di risparmio e investimento, ma senza dimenticare le polizze più flessibili, IoT è e resterà un trend dominante nel prossimo futuro
Nell'analizzare il rapporto tra i servizi finanziari e l'universo dell'Internet of Things, qualche anno fa Deloitte fece notare il fascino del collegamento tra un mondo nativamente tangibile, come quello degli oggetti connessi, e uno che di tangibile non ha più nulla, neanche il denaro. Eppure, IoT rappresenta uno dei più potenti abilitatori di trasformazione digitale del settore finanziario, con straordinarie previsioni di crescita: secondo Fortune Business Insight, parliamo di un CAGR del 26,5% fino al 2026, laddove il suo valore nel mercato BFSI (banking, financial services, insurance) sarà di 116,27 miliardi di dollari.
Ancor più interessante il fatto che gli attori del mercato stiano investendo in media 117,4 milioni USD/anno, ovvero lo 0,4% dei propri ricavi, in soluzioni IoT rivolte ai tre macrocosmi della sicurezza,

della customer experience e dell'efficienza operativa. Alla base delle rosee previsioni ci sarebbe un incremento di consapevolezza dei benefici di IoT nell'online banking e in ambito assicurativo.

Indice degli argomenti

Sfruttare i benefici dell'IoT in ambito finanziario
IoT e finance: gli use case più significativi
Fraud detection
Transazioni e pagamenti innovativi
Perfezionamento della customer experience
Sviluppo di prodotti innovativi
Smart Contract basati sull'IoT
(continua)

https://www.zerounoweb.it/trends/la-forza-rivoluzionaria-di-iot-nel-settore-finanziario/

ZEROUNOWEB *- Emanuele Villa - 14 Mar 2022*

Giornata Mondiale Acqua - Perdite idriche, 900 milioni per digitalizzare le reti - Fa leva sulle nuove tecnologie il piano da 3,8 miliardi del Mims per mettere in sicurezza le strutture primarie del Paese e ridurre le inefficienze nella distribuzione. Il ministro Giovannini: "Investimenti programmati anche con l'obiettivo di colmare il divario Nord-Sud"

Per ridurre le perdite di acqua nelle reti di distribuzione il Ministero delle Infrastrutture e della Mobilità Sostenibili (Mims) ha previsto interventi per una cifra di poco inferiore a 1,4 miliardi di euro: 900 milioni dal Pnrr, utilizzati anche per la digitalizzazione e il monitoraggio delle reti, e 482 milioni dal programma europeo React Eu attraverso il Piano Operativo Nazionale (Pon) Infrastrutture e Reti.

Indice degli argomenti

Ambrosetti: pesa la scarsa digitalizzazione delle infrastrutture
Gli investimenti complessivi del Mims
Gli interventi sulle infrastrutture idriche primarie
(continua)

https://www.corrierecomunicazioni.it/digital-economy/perdite-idriche-900-milioni-per-digitalizzare-le-reti/

Corriere Comunicazioni *- Domenico Aliperto - 22 Mar 2022*

Cybersecurity in sanità: minacce, scenari e prospettive concrete - Aumentano le minacce cyber contro la sanità digitale, un effetto collaterale della forte accelerazione digitale del settore. Le sfide riguardano l'estrema complessità dei sistemi, lo sviluppo di nuovi modelli di assistenza connessa e la crescita dell'IoT. Come vincerle? Ripensando i paradigmi di sicurezza.

Avviata da tempo, la trasformazione digitale in sanità ha subito con la pandemia una vera e propria accelerazione verticale. E per quanto si debbano ancora affrontare diverse sfide nel percorso verso nuovi modelli di cura e di assistenza, non vi è dubbio che le prospettive – complice anche in PNRR – siano interessanti.

Il rovescio della medaglia, comune a tutti i percorsi di digitalizzazione, è la crescita di valore degli asset digitali e, quindi, l'aumento dell'attività cyber criminale attorno ad essi. Secondo il Rapporto Clusit 2021, sono stati 1.871 gli incidenti cyber registrati nel 2020, di cui 215 in area sanitaria. La crescita nell'healthcare è stata del 5,9% e l'area attrae il 12% di tutti gli attacchi registrati.

La tendenza è inevitabilmente in crescita e si concretizza soprattutto in attività di cyber crime, con una particolare frequenza dei malware (45%), dell'Account Cracking (14%) e degli attacchi di phishing e di social engineering (9%). È corretto sottolineare che, nonostante le attività di cybercrime volte alla

sottrazione dei dati siano il 94% del totale, il settore deve farei conti anche con attività di spionaggio (4%), soprattutto in tema di vaccini anti-covid.
Secondo lo IBM Security, l'healthcare detiene da 11 anni il primato di verticale con il più alto costo per data breach, che passa dai 7,13 milioni di dollari del 2020 ai 9,23 milioni del 2021, con un incremento del 29,5%. Dato ancor più interessante quello di Ponemon Institute, che dà una stima del tempo medio di rilevazione degli attacchi: in Italia è di 203 giorni. Ciò significa che le capacità di monitoraggio dei sistemi sono fortemente migliorabili.
Indice degli argomenti
Attività Cyber in aumento: quali le sfide da affrontare
Come approcciare la sicurezza nella sanità 2.0
(continua)
https://www.zerounoweb.it/techtarget/searchsecurity/cybersecurity-in-sanita-minacce-scenari-e-prospettive-concrete/
ZEROUNOWEB *- Emanuele Villa - 23 Mar 2022*

Cyber security ed energia: ecco i rischi e i nuovi scenari di guerra ibrida - Il settore energetico non è immune agli attacchi hacker e, a quanto pare, tra il 2012 e il 2018 sono stati 135 i Paesi colpiti dai cyber criminali a livello globale. L'accusa americana ha puntato il dito su quattro funzionari russi: a rischio le energie rinnovabili. Ecco i possibili scenari.
Il settore energetico non è immune agli attacchi hacker: ne sanno qualcosa la Colonial Pipeline, la Saudi Arabian Oil Co., la Petroleos Mexicanos e tante altre società che hanno subito grandi attacchi negli ultimi anni, che le hanno costrette a interrompere i loro servizi.
Indice degli argomenti
Cyber security ed energia: i sospetti
Cyber security ed energia: le accuse
I rischi per le energie rinnovabili
(continua)
https://www.cybersecurity360.it/nuove-minacce/cyber-security-ed-energia-ecco-i-nuovi-scenari-di-guerra-ibrida/
Cybersecurity360 *- Marco Santarelli - 28 Mar 2022*

CISA and DoE warns of attacks targeting UPS devices. The US CISA and the Department of Energy issued guidance on mitigating attacks against uninterruptible power supply (UPS) devices.The US Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy published joint guidance on mitigating cyber attacks against uninterruptible power supply (UPS) devices. The US agencies warn of threat actors gaining access to a variety of internet-connected uninterruptible power supply (UPS) devices by exploiting default credentials. UPS devices provide clean and emergency power in a variety of applications when normal input power sources are interrupted for various reasons. The guidance recommends organizations immediately enumerate all UPSs and similar systems and ensure they are not accessible from the internet. In the case where a UPS device must be accessible online, organizations are recommended to implement the following controls:

- Ensure the devices are accessible through a virtual private network.
- Enforce multifactor authentication.
- Use strong passwords or passphrases in accordance with National Institute of Standards and Technology guidelines (for a humorous explanation of password strength, see XKCD 936)

(continua)
https://securityaffairs.co/wordpress/129620/security/cisa-doe-warn-attacks-ups.html
SecurityAffairs *– Pierluigi Paganini - March 30, 2022*

Riconoscimento facciale - Sorveglianza biometrica nuova arma nella cyber guerra, dall'Afghanistan all'Ucraina: usi e scenari - A livello mondiale, la proliferazione di tecnologie invasive di riconoscimento facciale rappresenta una strategia non del tutto nuova, spesso utilizzata – soprattutto in epoche recenti – anche per finalità militari. Il precedente dell'Afghanistan, gli usi nel conflitto ucraino, le ripercussioni sulla sicurezza di tutti.
Anche l'Ucraina starebbe iniziando a puntare sulla tecnologia di riconoscimento facciale per scansionare i volti dei soldati russi e identificare le migliaia di persone che hanno perso la vita in occasione dei bombardamenti pianificati dal Cremlino, sfruttando le potenzialità – ancora ritenute non del tutto affidabili – della controversa piattaforma Clearview AI (ove sono raccolte oltre 2 miliardi di immagini estrapolate, tra l'altro, anche dai più noti e popolari social media russi).
Questo nell'ottica di predisporre un database aggiornato e completo in grado di selezionare e processare le foto caricate e indicizzate sul web, anche per verificare la presenza di eventuali infiltrati russi, riconoscere i soldati senza bisogno di impronte digitali e intensificare la lotta alla disinformazione mediante la supervisione centralizzata del flusso comunicativo che circola online.
Indice degli argomenti
L'uso del riconoscimento facciale in zone di guerra
L'uso di tecnologie invasive a livello globale
Il patrimonio informativo Usa nelle mani dei talebani
La tecnologia HIIDE
Ripercussioni etiche sulla sicurezza e sulla tutela della privacy
Le linee guida di Human Rights First
Conclusioni
(continua)
https://www.agendadigitale.eu/sicurezza/sorveglianza-biometrica-nuova-arma-nella-cyber-guerra-dallafghanistan-allucraina-usi-e-scenari/
AGENDA DIGITALE - *Angelo Alù - 01 Apr 2022*

Qbot malware switches to new Windows Installer infection vector The Qbot botnet is now pushing malware payloads via phishing emails with password-protected ZIP archive attachments containing malicious MSI Windows Installer packages. This is the first time the Qbot operators are using this tactic, switching from their standard way of delivering the malware via phishing emails dropping Microsoft Office documents with malicious macros on targets' devices. Security researchers suspect this move might be a direct reaction to Microsoft announcing plans to kill malware delivery via VBA Office macros in February after disabling Excel 4.0 (XLM) macros by default in January.
Microsoft has begun rolling out the VBA macro autoblock feature to Office for Windows users in early April 2022, starting with Version 2203 in the Current Channel (Preview) and to other release channels and older versions later.
"Despite the varying email methods attackers are using to deliver Qakbot, these campaigns have in common their use of malicious macros in Office documents, specifically Excel 4.0 macros," Microsoft said in December.

"It should be noted that while threats use Excel 4.0 macros as an attempt to evade detection, this feature is now disabled by default and thus requires users to enable it manually for such threats to execute properly."
This is a significant security improvement towards protecting Office customers since using malicious VBA macros embedded in Office documents is a prevalent method to push a large assortment of malware strains in phishing attacks, including Qbot, Emotet, TrickBot, and Dridex.
What is Qbot?
Qbot (also known as Qakbot, Quakbot, and Pinkslipbot) is a modular Windows banking trojan with worm features used since at least 2007 to steal banking credentials, personal information, and financial data, as well as to drop backdoors on compromised computers and deploy Cobalt Strike beacons. (continua…)
https://www.bleepingcomputer.com/news/security/qbot-malware-switches-to-new-windows-installer-infection-vector/
BleepingComputer - *Sergiu Gatlan - April 11, 2022*

No plain sailing: modern pirates hack superyachts' cybersecurity Superyachts are battling anonymous cyberattacks from a new kind of pirate whilst hydrogen-powered boats are on track to replace fossil fuels. These themes and more dominated this year's 28th edition of the Dubai International Boat Show.
Returning for the first time since the arrival of COVID, the Dubai International Boat Show is a highlight on the annual calendar for luxury boat manufacturers. Over 800 companies from more than 50 countries use the event as a platform to showcase and unveil their latest products.
One such company was Sunreef Yachts from Poland, which unveiled their new Sunreef Eco 80 yacht. After falling victim to the delays created by the world's shipping crisis, the Sunreef Eco 80 arrived fashionably late to the event with its show-stopping solar panels. The eco-friendly design aims to make the yacht autonomous from docking or refuelling. (……..)
Pirates hack superyachts' cybersecurity.
Most modern marine vessels are heavily equipped with technology, from GPS and navigation systems to electronic chart displays and information systems (ECDIS). The arrival of this new technology has sailed superyachts into dangerous waters with a new type of pirate.
Owning a superyacht is a luxury for the world's financial elite due to the exorbitant cost of buying and maintaining one. High-tech superyachts with wealthy owners create the perfect combination for bounty-hungry hacking pirates.
Pirates in theatrical movies would sail under a skull and bones flag equipped with a hook and an eye patch. However, realistically today, a pirate can hold a ship at ransom from the comfort of a coffee shop. Cyber security expert Naveen Hemanna explains how the rise of digital banking and cryptocurrencies helps fuel this form of crime. He told Euronews, "The pirates need not be on the boat. (continua….)
https://www.euronews.com/next/2022/04/11/no-plain-sailing-modern-pirates-hack-superyacht-cybersecurity
Euronews *–Evan Bourke - 11/04/2022*

Missili e malware. L'assalto russo alla rete elettrica ucraina *A marzo, pochi giorni dopo l'allaccio della rete elettrica ucraina a quella europea, i servizi segreti del Cremlino hanno tentato – senza successo*

– di fare saltare le centrali di controllo sfruttando un malware noto come Industroyer 2. Ecco cos'è successo. Emergono notizie dal fronte cyber in Ucraina, che finora pareva più quieto di quanto non si aspettassero gli analisti. Martedì sono stati resi noti i dettagli delle operazioni nel quinto dominio, condotte dalla Russia ai danni dell'infrastruttura energetica ucraina. A metà marzo i servizi russi avrebbero provato a far saltare la rete elettrica attaccando diverse centrali, ma non è andata come speravano.

Le informazioni arrivano da un documento stilato dalla Computer Emergency Response Team (Cert) del governo ucraino, condiviso con diversi partner internazionali e visto da alcune testate statunitensi. Si parla di "almeno due tentativi andati a termine"; uno è avvenuto pochi giorni dopo che l'Ucraina si è collegata alla rete energetica europea per ridurre la sua esposizione alla Russia. Quando la notizia è stata resa nota, il vicedirettore della divisione governativa per lo Sviluppo digitale **Victor Zhora** ha definito il documento "preliminare". Questo non ne invalida i contenuti: anzi, l'ufficiale ha riconosciuto l'apporto di squadre internazionali, tra cui il Cybercommand statunitense, e di due aziende, Microsoft ed ESET. Le informazioni condivise da queste ultime hanno permesso di ricostruire quanto avvenuto. Il contesto: l'Ucraina è vittima di una sequela di ciberattacchi russi da almeno otto anni, come ha ricordato Zhora. Ma secondo gli esperti, gli attacchi avvenuti a marzo 2022 ricordano da vicino due istanze, nel 2015 e 2016, in cui gli aggressori – che gli Stati Uniti e altri hanno identificato come Sandworm, ossia l'unità 74455 dei servizi segreti russi – erano riusciti a interrompere le operazioni della rete elettrica russa. In particolare, l'incidente del 2016 fu condotto mediante un codice malevolo soprannominato Industroyer. Un esperto di ESET ha spiegato ad *ABC* che il programma era costruito per accendere e spegnere gli interruttori in una sequenza progettata per causare un blackout, oltre a distruggere i computer. Gli Usa hanno poi accusato sei ufficiali del Gru, e diversi Paesi occidentali hanno incriminato Sandworm, responsabile anche dei disastri causati da un altro malware – NotPetya – nel 2017. Anche lo scorso marzo gli aggressori sono riusciti a penetrare e mettere fuori uso parte del sistema di controllo della rete elettrica ucraina, usando un'iterazione del malware che i ricercatori hanno soprannominato Industroyer 2. (continua----)

https://formiche.net/2022/04/russia-ucraina-attacco-centrali-elettriche-industroyer/

***FORMICHE** - Otto Lanzavecchia - 13/04/2022*

Fuori Kaspersky. La circolare Acn sul software russo

L'Agenzia per la cybersicurezza nazionale (Acn) sta per pubblicare una circolare che spiegherà come sostituire i software di sicurezza russi, annuncia il direttore Baldoni. Tra gli altri nel mirino Kaspersky: dopo la guerra russa in Ucraina il governo Draghi vuole togliere il colosso cyber di Mosca dalla Pa

L'Italia è pronta a sostituire gli antivirus russi dalla Pubblica amministrazione e dalle sue aziende. L'Agenzia per la cybersicurezza nazionale (Acn) sta per diramare una circolare che spiegherà come e quando rimpiazzare i software di origine russa con altri ritenuti più sicuri.

A darne notizia è stato il direttore dell'agenzia **Roberto Baldoni** in audizione alla Commissione Finanze del Senato martedì. Il documento in corso di adozione riguarderà la scelta dei "prodotti per la sicurezza dei dispositivi" e in particolare "di *end-point security*, come anti-virus e *anti-malware* o di protezione delle reti come i firewall", ha spiegato. Un tassello in più nella vicenda che riguarda Kaspersky, il colosso russo degli antivirus fondato da **Eugene Kaspersky** e finito al centro di un caso internazionale dopo l'invasione russa dell'Ucraina e le sanzioni occidentali a Mosca.

Era stata la stessa Acn, inaugurata un anno fa dal governo Draghi per vigilare sulla difesa cibernetica degli asset strategici, a diramare una nota il 15 marzo scorso sottolineando "le implicazioni di sicurezza derivanti dall'utilizzo di tecnologie informatiche fornite da aziende legate alla Federazione Russa" e chiedendo ad aziende e Pa di "procedere urgentemente ad un'analisi del rischio derivante dalle soluzioni di sicurezza informatica utilizzate e di considerare l'attuazione di opportune strategie di diversificazione". La circolare dell'Acn, ha detto Baldoni, sarà stilata "anche sulla base di elementi forniti in sede interistituzionale dal nucleo della cybersicurezza costituito presso l'Agenzia con il dl. 82 del 2021".

Altri Paesi europei sono già intervenuti per chiedere di sostituire Kaspersky. Il rischio segnalato è quello di un'interferenza indebita del governo russo nelle sue aziende e la conseguente esposizione dei dati degli utenti. Accuse sempre rispedite al mittente dall'azienda con sede a Mosca. Oltre all'Acn a metà marzo un alert più esplicito era partito dall'agenzia dei Servizi tedeschi, la Bsi, mettendo in guardia "contro l'uso del software di protezione antivirus del produttore russo Kaspersky".

La parola d'ordine, ha spiegato Baldoni in audizione, è "diversificazione". Per l'Agenzia è necessario cioè diversificare i fornitori di servizi informatici per evitare un'eccessiva esposizione al rischio cibernetico da parte di attori legati a Mosca. Questo perché "durante la crisi in Ucraina il livello di rischio derivante dall'utilizzo di prodotti e servizi legati ad aziende che hanno relazioni con la Federazione russa è mutato". (continua…..)

https://formiche.net/2022/04/kaspersky-acn-software-russo/

***FORMICHE**- Francesco Bechis - | 13/04/2022*

Microsoft Leads Operation to Disrupt Zloader Botnet

The banking Trojan-turned-ransomware-distribution tool has been a potent threat since late 2019.

Researchers from Microsoft and several security vendors have sinkholed 65 domains associated with the prolific Zloader malware distribution botnet.

Another 319 backup domains that Zloader generated via an embedded domain generation algorithm (DGA) have been seized as part of the same operation, which included ESET, Palo Alto Networks, and Black Lotus Labs.

The goal is to disable the infrastructure that the criminal gang behind the Zloader botnet has been using as part of its malware-distribution-as-a-service operation, says Amy Hogan-Burney, general manager of Microsoft's digital crimes unit. It is likely the operators of the botnet will try to revive operations, Hogan-Burney says, so Microsoft and the other entities involved in the takedown will continue to work with each other and with Internet service providers to monitor for and identify any further activity by the group.

Zloader first surfaced on security vendor radars in November 2019 as banking malware modeled along the lines of the notorious Zeus banking Trojan. The malware — which was sold in underground forums under the name "Silent Night" — was designed to steal data associated with online bank accounts, such as account login IDs and passwords.

ESET said its researchers have observed criminal groups using different ways to distribute Zloader, including via exploit kits such as RIG, COVID-19 themed phishing emails, adult sites, and misuse of Google Ads. The malware is designed to take a variety of malicious actions once installed on a system. This includes stealing data from browsers, stealing cryptocurrency wallets, logging keystrokes, enabling remote control, and supporting arbitrary command execution, ESET said.

One feature of the malware — its ability to profile the network and the compromised host — has allowed threat actors to distribute different malicious payloads to infected systems. Recently, this has included various ransomware families such as DarkSide and Ryuk, both of which have been associated with numerous high-profile attacks over the past two years or so.
Microsoft's digital crimes unit led the effort to take down Zloader infrastructure. The company obtained a court order from the US District Court for the Northern District of Georgia that allowed Microsoft's security researchers to take control of 65 Zloader-associated domains and direct traffic to these sites to a Microsoft sinkhole. (continua…)
https://www.darkreading.com/threat-intelligence/microsoft-leads-operation-to-disrupt-zloader-botnet-activity
Darkreading *- Jai Vijayan - April 1*

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.

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 Palestro 95 – 00185 ROMA
Tel. +39 06 64871209
E-mail: segreteria@infrastrutturecritiche.it

Gruppo di user all'interno Si informa che AIIC ha costituito un proprio gruppo di user

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

della community all'interno della community di LinkedIn: per unirti al gruppo è sufficiente usare il seguente 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
ai quali potete inviare suggerimenti e quesiti scrivendo a: segreteria@infrastrutturecritiche.it