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 2020 **N. 04/ 2020** **Aprile 2020**

Il 31 dicembre 2019 è stato segnalato un focolaio di casi di polmonite di eziologia sconosciuta a Wuhan, nella provincia di Hubei, in Cina. Il 9 gennaio 2020, il CDC cinese ha riconosciuto come agente causale dell'epidemia un nuovo coronavirus, incluso filogeneticamente nel clade SARS-CoV. Il morbo associato al virus è definito come malattia da nuovo coronavirus 2019 (COVID-19). Il direttore generale dell'Organizzazione Mondiale della Sanità ha dichiarato il COVID-19 una pandemia globale l'11 marzo 2020.

In questo momento di emergenza nazionale l'Associazione ringrazia dal profondo del cuore tutti coloro che con il proprio lavoro e rischio personale si adoperano per la salute di tutti e per le attività essenziali alla vita nazionale. Un pensiero commosso va a coloro che hanno perso la vita nell'adempimento del proprio dovere e a tutte le vittime di questa epidemia, nonché ai loro famigliari.

Associazione Italiana esperti in Infrastrutture Critiche

ATTIVITA' DELL'ASSOCIAZIONE

Rinnovo associativo per l'anno 2020

Si ricorda a tutti i soci che il 31 dicembre 2019 è scaduto il periodo associativo. Invitiamo tutti i soci a rinnovare per tempo l'associazione versando il relativo contributo, ormai inalterato da anni.

La quota per il rinnovo individuale è di euro 40 e può essere versata con bonifico sul c/c presso Banca Intesa Business, Coordinate bancarie IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando "rinnovo socio ordinario nome e cognome anno 2020".

Per i nuovi iscritti l'importo da pagare è di € 60,00 mentre per i soci attuali la quota di rinnovo rimane sempre fissata a € 40,00. Le quote e le modalità di rinnovo per i soci collettivi – così come le indicazioni per chi vuole iscriversi come nuovo socio - sono contenute nel sito AIIC al link (da copiare)
http://www.infrastrutturecritiche.it/new/per-iscriversi/

Ricordiamo che la data limite per il rinnovo annuale, come da regolamento, è fissata al 31 marzo 2020. Dopo questa data, si decade dalla qualifica di socio e sarà necessario procedere ad una nuova iscrizione, versando in più il relativo contributo per le spese di segreteria.

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

Attività del Gruppo di lavoro

Il Gruppo di Lavoro. "**Internet of Things (IoT) in the context of Critical Infrastructures: Cybersecurity and Privacy concerns and possible solutions**" ha iniziato la sua attività ed ha svolto riunioni nei mesi di novembre, dicembre e febbraio 2020. Poi, per l'emergenza Covid 19, i contatti sono proseguiti via e-mail. Il Gdl è coordinato da Sandro Bologna e vede la partecipazione dei soci: Silvano Bari, Glauco Bertocchi, Luigi Carrozzi, Luisa Franchina, Francesco Ressa, Angelo Socal, Alberto Traballesi e sta per concludere l'elaborazione del saggio.

Tutti i soci possono segnalare eventi, fatti e informazioni di possibile interesse comune da inserire, per esempio, in newsletter o nel sito AIIC.
In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o chairman, valutate la possibilità di partecipare a nome AIIC: in tal caso – però – la partecipazione di AIIC ad un evento deve essere decisa dal Consiglio Direttivo, pertanto siete pregati di contattare il CD con ragionevole anticipo, alla mail segreteria@infrastrutturecritiche.it
In caso non fosse possibile la partecipazione a nome AIIC, vi invitiamo ad indicare, nel profilo professionale, la vostra appartenenza ad AIIC.

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 ed autonomi 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.

NEWS E AVVENIMENTI

Per l'Intelligenza Artificiale è l'ora dell'etica – L'obiettivo è ambizioso. Sostenere un approccio etico all'Intelligenza Artificiale e promuovere tra organizzazioni, governi e istituzioni un senso di responsabilità condivisa con l'obiettivo di garantire un futuro in cui l'innovazione digitale e il progresso tecnologico siano al servizio del genio e della creatività umana e non la loro graduale sostituzione. Lo hanno sostenuto **i** primi firmatari del documento "Call for an AI Ethics": Pontificia Accademia per la Vita, Microsoft**,** IBM**,** la FAO e il Governo italiano**.** La cerimonia, svoltasi il 28 febbraio a Roma all'Auditorium della Conciliazione di fronte a San Pietro in Vaticano, ha visto la presenza di Monsignor Vincenzo Paglia, Presidente della Pontificia Accademia per la Vita, che è lo sponsor dell'iniziativa, Brad Smith, President di Microsoft; John Kelly III, Executive Vice President di IBM, Dongyu Qu, Direttore Generale della FAO, e per il Governo italiano Paola Pisano, titolare del Ministero dell'Innovazione tecnologica e la digitalizzazione**.**
https://www.impresacity.it/news/22999/per-l-intelligenza-artificiale-e-l-ora-dell-etica.html
Impresa city *– 02 marzo 2020*

Energy Way: AI e matematica al servizio della sostenibilità aziendale - Migliorare l'efficienza energetica di un'azienda senza rimpiazzare macchinari, né sostituire lampadine, è possibile. Lo dimostra il lavoro di Energy Way, azienda modenese fondata nel 2013. Ha una sede anche ad Haifa, in Israele, grazie al partner locale Ecoprocess. Grazie al nuovo Direttore Generale David Bevilacqua sta per aprire una sede a Milano e ha progetti di forte ampliamento. Il segreto di Energy Way è un'idea originale di partenza, seguita da un'implementazione di alto livello. In un evento con la stampa il fondatore e CEO Fabio Ferrari ha spiegato che l'azienda dispone di un team altamente qualificato di

giovani matematici, ingegneri, fisici, neuroscienziati, economisti, esperti in intelligenza artificiale e altre specializzazioni, che lavorano insieme con l'obiettivo di usare la matematica per descrivere la natura intorno a noi. "*Studiamo i dati di un fenomeno e troviamo le correlazioni deboli, le peculiarità che non si notano e su cui agire per controllare e ottimizzare un sistema. I nostri interlocutori sono responsabili IT, dell'innovazione, del settore energy, per indagare gli elementi per ottimizzare un sistema*".
https://www.impresagreen.it/news/9814/energy-way-ai-e-matematica-al-servizio-della-sostenibilita-aziendale.html
impresa city *– 02 marzo 2020*

Internet of Things sotto attacco, colpite 7 aziende su 10 – Internet of Things**,** aziende impreparate ad affrontare la sfida cybersecurity. Tocca quota 84% il tasso di imprese nel mondo provviste di sistemi IoT, ma solo il 70% rileva attacchi o tentativi di attacco**, e** più della metà non utilizza misure di sicurezza che vanno oltre la semplice password. Emerge dalla ricerca di Extreme Networks, secondo cui le aziende continuano a essere vulnerabili nei confronti degli attacchi portati attraverso IoT nonostante la rapida adozione della tecnologia. Le aziende sottovalutano le minacce interne: il 55% dei professionisti IT ritiene che la maggior parte dei rischi arrivi dall'esterno e più del 70% pensa di avere una visibilità completa sugli apparati all'interno della propria rete, anche se la ricerca Verizon sulle violazioni dei dati nel 2019 afferma che la maggior parte degli incidenti è dovuta a un utilizzo errato dei privilegi di accesso da parte dei dipendenti, che è una delle prime tre cause in senso assoluto.
https://www.corrierecomunicazioni.it/cyber-security/internet-of-things-sotto-attacco-colpite-7-aziende-su-10/
Corcom *– L. O. – 03 marzo 2020*

Crittografia post-quantum, per resistere agli attacchi quantistici: gli scenari – Con l'avvento dei computer quantistici, gli algoritmi di crittografia moderna stanno vivendo un'evoluzione che modificherà notevolmente il loro attuale impiego e, al fine di sostenere la sicurezza di *Internet* e di altre tecnologie basate sulla crittografia, è necessario incrementare le ricerche in campo matematico per costruire la crittografia del domani, resistente agli attacchi quantistici, e che diverrà nota come crittografia *post-quantum* o *quantum-resistant***.**
In tale contesto la maggior parte dei nostri protocolli di comunicazione si basa principalmente su tre funzionalità crittografiche fondamentali: crittografia a chiave pubblica, firma digitale e scambio delle chiavi. Ciascuna di esse è facilmente decodificabile, senza il possesso della chiave, dall'algoritmo di *Shor* (ideato da *Peter Shor* nel 1994) e sono di fatto ritenute insicure con la comparsa dei *computer* quantistici. Se da un lato la crittografia post-quantum (*Post Quantum Cryptography,* PQC) potrebbe giungere nel breve periodo ad uno o più *standard* implementativi, la *Quantum Key Distribution* (QKD) è una realtà in fase di *testing* già da alcuni anni. Si caratterizzata per la presenza di un canale ottico (fibra o *open space*) per l'invio tramite fotoni della chiave codificata e per la non intercettabilità della chiave, garantita dai principi quantistici di *Heisenberg*. Può essere associata ad un canale classico non sicuro, sul quale la chiave prodotta viene usata in modo tradizionale. Entrambe quindi, la PQC e la QKD, possono costituire due strade percorribili, due soluzioni non alternative tra loro, ma complementari e coesistenti in un singolo crittosistema**.**
https://www.cybersecurity360.it/soluzioni-aziendali/crittografia-post-quantum-per-resistere-agli-attacchi-quantistici-gli-scenari/
Cybersecurity 360 *– Mario Raso – 05 marzo 2020*

Machine learning, più facile passare dal modello alla pipeline - Una cosa è creare un modello di machine learning, lavorando dietro schermo e tastiera di un notebook, un'altra è inserirlo all'interno di un più ampio meccanismo che lo renda scalabile e funzionante. Una pipeline, come si dice in gergo**.** Google ha voluto andare incontro alle difficoltà dei programmatori e dei data scientist con Cloud AI Platform Pipelines, una piattaforma in cloud che permette di *"distribuire solide e riproducibili pipeline di machine learning"*, e che include funzionalità di monitoraggio, auditing, tracciamento delle versioni, riproducibilità.
Sarà dunque più semplice creare dei workflow di apprendimento automatico, che non siano solo sperimentazioni ma che risultino utilizzabili all'interno di contesti aziendali. Per semplificare e velocizzare ulteriormente il lavoro, la piattaforma include numerosi componenti di pipeline preconfezionati, oltre a permettere di crearne altri ex novo….
http://www.ictbusiness.it/cont/news/machine-learning-piu-facile-passare-dal-modello-alla-pipeline/44167/1.html#.XoS6QKgzaUk
IctBusiness.it *– Redazione – 12 marzo 2020*

Office network at the European Network of Transmission System Operators for Electricity (ENTSO-E) breached The European Network of Transmission System Operators for Electricity (ENTSO-E) revealed this week that threat actors penetrated its network. ENTSO-E, the European Network of Transmission System Operators, represents 43 electricity transmission system operators (TSOs) from 36 countries across Europe, thus extending beyond EU borders. ENTSO-E was established and given legal mandates by the EU's Third Package for the Internal energy market in 2009, which aims at further liberalising the gas and electricity markets in the EU. ENTSO-E works with TSO on the definition of Europe's energy and climate strategy. According to the organization, the attack only impacted the office network and did not affect any operational TSO system. *"A risk assessment has been performed and contingency plans are now in place to reduce the risk and impact of any further attacks," reads the statement published by the company. "Our TSO members have been informed and we continue to monitor and assess the situation."* Some of the affected TSOs also published security advisories about the security incident and explained that hackers did not breach their networks.*"……..*
https://securityaffairs.co/wordpress/99385/security/entso-e-security-breach.html
Security Affairs - *Pierluigi Paganini March 11, 2020*

DDoS Attack Trends Reveal Stronger Shift to IoT, Mobile. Attackers are capitalizing on the rise of misconfigured Internet-connected devices running the WS-Discovery protocol, and mobile carriers are hosting distributed denial-of-service weapons. Distributed denial-of-service (DDoS) attacks remain a popular attack vector but have undergone changes as cybercriminals shift their strategies. Today's attackers are turning to mobile and Internet of Things (IoT) technologies to diversify and strengthen their DDoS campaigns, research shows. Researchers with A10 Networks, which tracked nearly 6 million DDoS weapons in the fourth quarter of 2019, today published "DDoS Weapons and Attack Vectors" to share the trends in today's DDoS landscape. These include the weapons being used, locations where attacks are launched, services exploited, and techniques attackers are using to maximize damage caused. DDoS weapons are distributed around the world; however, the bulk of attacks start in countries with the most Internet connectivity. China is the origin of the highest

number of DDoS attacks, with 739,223 starting in the country. The United States is second, with 448,169, followed by the Republic of Korea (440,185), India (268,864), Russia (253,609), and Taiwan (199,656).
The SNMP and SSDP protocols, long the top sources for DDoS attacks, continued to take the top spots in the fourth quarter with nearly 1.4 million SNMP weapons and nearly 1.2 million SSDP weapons tracked. The next one was a surprise: Researchers saw a sharp spike in attacks using WD-Discovery; these rose to nearly 800,000 to become the third most common source of DDoS. A10 Networks attributes this change to the growing popularity of attackers leveraging misconfigured IoT devices to amplify their campaigns. As part of this trend, called "reflected amplification," attackers are focusing on the rising number of Internet-exposed IoT devices running the WS-Discovery protocol. WD-Discovery, a multicast UDP-based communications protocol, is used to automatically detect Internet-connected services. It's used in many devices, going back to Windows Vista; video encoders, printers, cameras, DVRs, and some on-prem security systems reply back to researchers' WS-Discovery Internet scans. WD-Discovery does not perform IP source validation, researchers note, so it's easy for attackers to spoof a victim's IP address. Doing this resulted in the victim being flooded with …… DDoS is also going mobile, researchers found. As an example, Groves points to the large number of Android systems with an unprotected diagnostics backdoor. "This is actively being used to place Mirai-like malware on the phone to make it a weapon," he explains. Further, attackers are widely deploying protocols such as COAP, which unlike the backdoor for Android, is an amplification vector that works similarly to WS-Discovery. ……
https://www.darkreading.com/iot/ddos-attack-trends-reveal-stronger-shift-to-iot-mobile/d/d-id/1337318
***Darkreading**- Kelly Sheridan -March, 13-2020*

La difesa delle reti energetiche passa anche dai contatori - Si chiama "Success" il progetto finanziato dalla Commissione Europea nell'ambito di Horizon 2020 a cui partecipano Germania, Italia e altri 7 Paesi. Ha portato alla realizzazione di un software per prevenire, rilevare e agire sugli attacchi informatici ai danni dei contatori intelligenti installati nelle grandi infrastrutture. Si è svolta a Terni la sperimentazione su una nuova generazione di contatori intelligenti.
Ci sono molti motivi per i quali è importante proteggere i contatori. Il primo è che il settore energetico europeo è coinvolto in un'importante trasformazione. È spinta dal cambio di paradigma energetico, che si sta progressivamente spostando dai combustibili fossili alle energie rinnovabili. Questo comporta una rivoluzione di tutto il settore, compreso il modo in cui vengono conteggiati i consumi. Il cambio interessa gli apparecchi residenziali così come quelli presenti presso le infrastrutture. E anche il contatore digitale è possibile obiettivo di attacchi. Ricordiamo infatti che la cyberwarfare, o guerra digitale, è spesso incentrata sugli obiettivi strategici, come le infrastrutture critiche. I contatori intelligenti sono ormai presenti nelle centrali, nelle aziende che generano autonomamente la propria energia da fonti rinnovabili. Nei dispositivi per la ricarica di veicoli elettrici, e ovviamente nelle smart home. Success si è assunto il gravoso compito di garantire la sicurezza informatica di questi dispositivi. I finanziamenti comunitari hanno permesso di progettare soluzioni di sicurezza digitale appositamente studiate.
https://www.securityopenlab.it/news/322/la-difende-delle-reti-energetiche-passa-anche-dai-contatori.html
***SecurityOpenLab** – Redazione – 25 marzo 2020*

Così la Cina fa propaganda in Italia, con i bot. Ecco l'analisi su Twitter di Alkemy per Formiche
Una ricerca di Alkemy per Formiche rivela un'operazione senza precedenti della propaganda cinese sugli aiuti per il coronavirus. Quasi la metà dei tweet con l'hashtag #forzaCinaeItalia è opera di bot. E l'ambasciata cinese... Quasi la metà dei post su Twitter pubblicati tra l'11 e il 23 marzo con l'hashtag #forzaCinaeItalia è opera di bot. Prodotto dei cosiddetti account automatizzati è anche oltre un terzo di quelli con l'hashtag #grazieCina. Secondo un'analisi di Social Data Intelligence realizzata per *Formiche* dal Lab R&D di Alkemy SpA, in collaborazione con Deweave, Luiss Data Lab e Catchy, il 46,3% dei post su Twitter pubblicati tra l'11 e il 23 marzo con l'hashtag #forzaCinaeItalia, quasi la metà, è stata generata da bot, account automatizzati creati con il preciso scopo di fare da cassa di risonanza. Lo stesso vale per un altro popolare hashtag, #grazieCina, che nello stesso arco di tempo ha dato ampia eco all'operazione diplomatica cinese: più di un terzo dei tweet che lo contenevano, il 37,1%, era prodotto da bot.
La propaganda del governo cinese in Italia è entrata dunque in una nuova fase. Il 12 marzo un Airbus A-350 della China Eastern proveniente da Shanghai è atterrato all'Aeroporto di Fiumicino con a bordo nove medici specializzati cinesi dall'Hubei e trenta tonnellate di materiale sanitario. Nei giorni precedenti e successivi all'arrivo, l'account Twitter dell'ambasciata cinese in Italia ha dato ampio resoconto dell'operazione, dallo sbarco al tragitto che ha portato l'équipe medica a Padova, utilizzando l'hashtag #forzaCinaeItalia. I cinguettii con questo hashtag hanno ricevuto un numero di "mi piace" e retweet di gran lunga superiore alla norma.
UN ESERCITO DI BOT
Non si tratta di un caso. L'analisi del gruppo di ricercatori, composto da Luca Tacchetti, Alice Andreuzzi, Nicola Piras, Alessandra Spada e Stefano Vacca, si basa su un campione di 47.821 tweet. Grafici alla mano, il livello di attività, coinvolgimento (retweet + like) e gradimento (like) dell'account Twitter dell'ambasciata cinese a Roma e dei post riguardanti l'operazione di soccorso del governo cinese sembrano fotografare un'operazione premeditata che non ha precedenti in Italia.
Non è un mistero per chi conosce lo spazio cibernetico l'esistenza sui social network dei bot, account creati ad hoc per aumentare, attraverso post, like, retweet, citazioni, la portata e l'efficacia di un preciso messaggio e assumendo la forma di una *eco chamber*. È ormai da tempo acclarata l'esistenza di un vero e proprio mercato dei bot cui attingono frequentemente sia attori privati sia entità statuali.
IL METODO
Nel caso della propaganda cinese intorno all'arrivo di aiuti in Italia, il team di studiosi ha costruito l'analisi sulla base della definizione di bot offerta dall'Oxford Internet Institute (Oii), che suggerisce alcuni indicatori per riconoscere un account automatizzato da uno vero. …….
https://formiche.net/2020/03/cina-propaganda-twitter-bot-alkemy/
Formiche - *Gabriele Carrer e Francesco Bechis -30/03/2020*

Coronavirus: Warning over surge in Zoom security incidents - Cyber criminals are targeting users of popular video conferencing application Zoom as millions of office workers turn to collaboration tools to keep in touch with each other during the Covid-19 coronavirus pandemic.
Check Point's threat research team says it has seen a steady rise in new Zoom domains, with 1,700 created since January, but this has ramped up in the past few days, with 425 new domains registered in the last seven days alone.
Of these, 70 have now been identified as fake sites, which are impersonating genuine Zoom domains with the intention of capturing and stealing personal information. The numbers reinforce a trend for cyber criminals to take advantage of home working via Zoom, which is used

by over 60% of the Fortune 500 and has been downloaded more than 50 million times from the Google Play app store.
Taking into account that 90% of cyber attacks start with a phishing campaign, much of this guidance boils down to adhering to basic security hygiene. This includes being cautious with emails and files from unknown senders, never opening unknown attachments or links claiming to be Zoom links in emails, keeping an eye out for spelling errors in URLs and emails that are usually a giveaway, and being suspicious of everything unexpected.
As a result of this disclosure, Zoom has now added password by default to all future scheduled meetings; made password settings enforceable at the account level and group level by account administrators; removed a feature that automatically indicates if a meeting ID is valid or invalid; and added a feature to block repeated attempts to scan for meeting IDs.
https://www.computerweekly.com/news/252480806/Coronavirus-Warning-over-surge-in-Zoom-security-incidents?asrc=EM_EDA_125549257&utm_medium=EM&utm_source=EDA&utm_campaign=20200331_Coronavirus:%20Warning%20over%20surge%20in%20Zoom%20security%20incidents
ComputerWeekly *– Alex Scroxtron – 30 mar 2020*

Come agisce la propaganda russa in Italia. Report DFRLab Report del DFRLab dell'Atlantic Council: i media pro Cremlino hanno alimentato fake news sugli aiuti per colpire l'Ue e gli Usa. Compare pure Diego Fusaro... Perché pandemia e infodemia hanno trovato terreno fertile in Italia? Se lo chiedono gli esperti del Digital Forensic Research Lab dell'Atlantic Council in un'analisi in tre parti dedicata al nostro Paese. Diciannove governi in tre decenni, l'ascesa del populismo, la delegittimazione delle istituzioni e il malcontento dilagante hanno causato quell'instabilità facilmente permeabile oggi, in tempi di pandemia, dall'infodemia con teorie del complotto sull'origine del virus, *fake news*, *meme* e messaggi antiestablishment.
Non è una questione solo interna, di partiti all'opposizione che cercano di scalzare il governo. Infatti, scrivono gli esperti, "ci sono anche narrazioni ingannevoli alimentate da potenze straniere per l'influenza a lungo termine" sul nostro Paese. L'allarme interferenze straniere in Italia sull'onda della pandemia di coronavirus è stato lanciato anche dal Copasir. E alcuni eurodeputati hanno messo in guardia i vertici comunitari dalla disinformazione russa e cinese. Come abbiamo svelato grazie a un report di Alkemy per *Formiche*, quasi la metà dei post su Twitter pubblicati tra l'11 e il 23 marzo con l'hashtag #forzaCinaeItalia è opera di bot. E proprio dal 23 marzo è iniziata una nuova offensiva, quella dei media e degli organi del Cremlino e dei funzionari russi, dopo che era atterrato a Pratica di Mare il primo aereo con gli aiuti "Dalla Russia, con amore". Ben prima che il cargo arrivasse in Italia, però, notano gli esperti dell'Atlantic Council nella prima parte dell'analisi, il senatore russo Alexey Pushkov aveva twittato dal suo account ufficiale quanto segue: "La Polonia non ha concesso agli aerei russi con aiuti umanitari per l'Italia di passare sul suo spazio aereo", costringendoli a un viaggio molto più lungo sulla Turchia. La smentita è arrivata velocissima dal governo polacco e Pushkov ha rimosso il tweet. Che però era già diventato virale sui notiziari russi e sui social media. "Utilizzando diversi set di parole chiave su Buzzsumo, DFRLab ha trovato dozzine di articoli che riportavano la dichiarazione online. I risultati della ricerca Польша не пропустила (tradotto: la Polonia non [li] ha lasciati passare) sono 15 articoli con 52.681 reazioni registrate in una settimana". Con la piattaforma di monitoraggio Meltwater Explore, DFRLab ha scoperto che "la notizia ha ottenuto la maggiore amplificazione su Twitter, ricevendo oltre 3 milioni di *impression*". L'articolo di Sputnik Italia, pubblicato lo stesso giorno del tweet di Pushkov, ha ricevuto 107.800 *engagement* online in tre giorni. Un video su YouTube di Diego Fusaro dal titolo "La Russia prova ad aiutare l'Italia. Ma qualcuno la sta misteriosamente boicottando?" è prossimo alle 300.000 visualizzazioni e ai 9.000 like. Da una parte i

media russi in lingua russa e inglese, dall'altra gli organi pro Cremlino in Italia. Entrambe hanno alimentato, con gli aiuti, una campagna anti Ue, anti Stati Uniti e anti Nato, rispolverando perfino hashtag come #italexit e #uscITA. Funzionale all'obiettivo di spaccare l'Unione europea attraverso l'Italia è una dichiarazione del presidente Vladimir Putin – "Se l'Italia lasciasse l'Europa, troverebbe nella Russia un alleato fidato" – pronunciata nel 2015 e non in collegata alla pandemia, che però è stata fatta circolare in questi giorni.
https://formiche.net/2020/03/propaganda-russa-coronavirus-dfrlab/
Formiche *- Gabriele Carrer -31/03/2020*

Spallanzani e non solo. Ospedali sotto attacco cyber. L'alert degli 007 L'ospedale Spallanzani di Roma nel mirino degli hacker. Dopo l'annuncio in video-conferenza dell'assessore alla Sanità della Regione Lazio Alessio D'Amato di "un attacco hacker una settimana fa allo Spallanzani, ma senza successo", arriva la conferma dell'intelligence.
Con un comunicato stampa il Sisr (Sistema per l'informazione e la sicurezza della Repubblica) fa sapere che è stata registrata una serie di "attacchi informatici ai danni di strutture italiane di eccellenza attualmente impegnate nel fronteggiare l'emergenza sanitaria in atto relativa al Covid-19". Le offensive cibernetiche sono state al centro di una riunione straordinaria del Nucleo Sicurezza Cibernetica, l'organo, presieduto dal vicedirettore generale con delega al cyber Roberto Baldoni, del Dipartimento delle Informazioni per la Sicurezza (DIS), che si occupa di gestire eventuali crisi cibernetiche e della preparazione e prevenzione in materia di sicurezza informatica. Alla riunione, si legge nel comunicato, hanno partecipato l'Aise, l'Aisi e la Polizia postale (Cnaipic). Gli attacchi cyber, hanno concluso gli esperti, costituirebbero una risposta "fisiologica" alla crisi in corso che, inevitabilmente, ha attirato l'attenzione di diversi attori nel dominio cyber, "per lo più di matrice criminale". Di qui un alert del Nucleo alla rete sanitaria nazionale, che è stata invitata ad aumentare la difesa delle sue infrastrutture. Sull'episodio dell'Ospedale Spallanzani la Procura di Roma ha aperto un'indagine coordinata dal procuratore Michele Prestipino. L'ipotesi di reato è quella di accesso abusivo a sistema informatico. I sabotaggi si inserirebbero in un genere di attacchi hacker che non necessariamente ha l'obiettivo di esfiltrare dati sensibili, e invece spesso ha scopo di lucro, spiega l'intelligence italiana. Più che malware sono dunque "ransomware". Un fenomeno "di portata mondiale", tanto che la stessa rete dei Csirt (Computer Security Incident Response Teams) europei ha innalzato il livello d'allerta per l'aumento di cyber-crimini che, avverte la Polizia postale, fanno leva in questo momento sui timori e la confusione dei cittadini per la pandemia……
https://formiche.net/2020/04/spallanzani-ospedali-attacco-cyber-007/
Formiche *-Francesco Bechis 01/04/2020*

Il virus di Russia e Cina che attacca l'Ue (e Italia). L'analisi della Commissione Cina e Russia continuano a utilizzare la crisi globale del coronavirus per diffondere *fake news* e altra disinformazione online. È quanto emerge dall'ultimo aggiornamento pubblicato oggi dal team East Stratcom del Servizio europeo per l'azione esterna. Al centro della strategia russa così come di quella cinese c'è la campagna per gli aiuti ai Paesi più colpiti. Tra tutti, l'Italia. Obiettivo: controllare la narrazione e minare l'Occidente. Come spiega *Politico Europe* analizzando il report, tali messaggi – alimentati sui social media e promossi dagli organi di informazione russi e cinesi – erano rimasti per lo più all'interno di un pubblico online amico di russi e cinesi, in particolare in Paesi come Italia, Spagna e Grecia. "Ma man mano che la crisi globale cresce, tali sforzi – sia da parte di gruppi sostenuti dall'esterno dagli Stati sia da attori interni all'Unione europea – stanno collegando la pandemia di

coronavirus con temi di disinformazione preesistenti, tra cui le campagne contro i migranti, le minoranze e la credibilità a lungo termine dell'Ue". Con un videomessaggio in tre lingue, la presidente della Commissione europea, Ursula von der Leyen, ha lanciato ieri un avvertimento contro quella ha definito come una "ondata massiccia" di disinformazione e di *fake news* online sul coronavirus invitando i cittadini europei a verificare le notizie e le piattaforme online a monitorare attivamente la veridicità dei contenuti pubblicati: "Chi diffonde disinformazione vi danneggia. La disinformazione può costare la vita. Insieme", ha detto von der Leyen, "possiamo ristabilire la verità".....La presidente von der Leyen ha mandato la palla nel campo dei colossi digitali. Che molto stanno facendo per aumentare la visibilità dell'Organizzazione mondiale della sanità e altri contenuti autorevoli. Tuttavia, si legge nel rapporto, ci sono diverse sfide sulla trasparenza e l'applicazione dei regolamenti. Ma il problema forse più grande è il fatto che "le principali piattaforme continuano a monetizzare la disinformazione e i contenuti dannosi sulla pandemia (compresi i siti di disinformazione pro Cremlino), ospitando per esempio annunci online su pagine che definiscono i migranti la causa del virus, promuovono cure false o diffondono teorie cospirative sul virus.
Un allarme infodemico simile era stato lanciato pochi giorni fa da alcuni eurodeputati e la scorsa settimana dal Copasir, come raccontato da *Formiche.net*. .....
https://formiche.net/2020/04/cina-russia-fake-virus/
Formiche *- Gabriele Carrer* ***-*** *01/04/2020*

Microsoft Alerts Healthcare to Human-Operated Ransomware Microsoft has notified dozens of hospitals with vulnerable gateway and VPN appliances in their infrastructure, which could put them at risk. Microsoft is alerting healthcare organizations to a rise in human-operated ransomware, which has been growing in frequency as attackers continue to take advantage of the COVID-19 crisis. These types of ransomware campaigns typically seek easy entry into target businesses, many of which have transitioned to remote workforces to stop the coronavirus spread. As a result, ransomware operators have begun to target network devices such as gateway and VPN appliances. The healthcare sector is especially vulnerable to these types of attacks, Microsoft reports, and it has identified and alerted "several dozens of hospitals" with vulnerable gateway and VPN tools. Microsoft's Threat Protection Intelligence Team and Threat Intelligence Center report more human-operated ransomware campaigns are exploiting vulnerabilities in network devices to gain a foothold in target organizations. REvil, also known as Sodinokibi, is an example of one campaign doing this. Once on a network, its operators aim to steal credentials, elevate their privileges, and move laterally across a network before installing ransomware or other malware. Data shows an overlap between infrastructure Sodinokibi used last year and infrastructure it used in recent VPN attacks. "This indicates an ongoing trend among attackers to repurpose old tactics, techniques, and procedures (TTPs) for new attacks that take advantage of the current crisis," Microsoft explains in a blog post. While team members haven't seen technical changes, they did notice social engineering techniques designed to exploit people's fears surrounding COVID-19.....
https://www.darkreading.com/vulnerabilities---threats/microsoft-alerts-healthcare-to-human-operated-ransomware/d/d-id/1337463
DARKREADING *Dark Reading Staff 01/04/2020*

Australian state will install home surveillance hardware to make sure if you're in virus isolation, you stay there The State of Western Australia has given itself the power to install surveillance devices in homes, or compel people to wear them, to ensure that those required to isolate

during the coronavirus crisis don't interact with the community. Not all people will be required to use the devices. State Premier [*equivalent to a US governor – ed.*] Mark McGowan said they'll only be used if: "Someone who is directed to self-isolate and fails to comply. "The law enabling the regime, passed yesterday after very brief debate, is the Emergency Management Amendment (COVID-19 Response) Bill 2020 [PDF]. It outlines the monitoring regime, and the fact that the State Emergency Coordinator has the power to require use of surveillance hardware…….Attempts to damage, remove or interfere with the operation of the devices, or refusal to hand one over to authorised officers, can result in a year behind bars, or a fine of AU$12,000 (US$7,400, £5,900). *The Register* has learned of smartphone-based surveillance in aid of coronavirus-crimping in Taiwan, Singapore and Hong Kong, plus the UK is clearing policy roadblocks to make it possible. Russia has used facial recognition and public security
https://www.theregister.co.uk/2020/04/01/west_australia_isolation/
The Register *- Simon Sharwood - 1 Apr 2020*

PROSSIMI EVENTI

A causa dell'emergenza Covid 19 tutti gli eventi sono stati rinviati a data da destinarsi

NOTIZIE D'INTERESSE:

Le indicazioni per chi vuole iscriversi come nuovo socio - sono contenute nel sito AIIC al link (da copiare)
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.

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

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 Email segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	Si informa che AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirti al gruppo è sufficiente copiare questo 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*