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. 9/ 2023** **ottobre 2023**

Guerra Palestina-Israele, aumentano gli attacchi cyber

I recenti sviluppi nella guerra informatica evidenziano una crescente minaccia cibernetica contro Israele, vittima di attacchi informatici mirati. Tali attacchi non solo mettono in pericolo la sicurezza delle informazioni, ma anche la stabilità delle infrastrutture critiche del Paese. Il gruppo Killnet e la maggior parte degli hacker pro-Russia hanno annunciato, attraverso i canali social, una nuova fase nella loro guerra informatica, questa volta prendendo di mira Israele. Il vertice di Killnet, noto come KillMilk, ha recentemente condiviso un comunicato che ha catturato l'attenzione delle formazioni alleate. Nel messaggio, KillMilk imputa al governo israeliano la responsabilità principale della violenza nella regione e ha promesso un forte sostegno alla campagna anti-Israele condotta da Anonymous Sudan, un gruppo hacker musulmano noto per le sue azioni contro soggetti ed entità ritenute colpevoli di offese all'Islam, specialmente in Occidente. Complessivamente, oltre 35 gruppi di hacker pro-Palestina hanno avviato una serie di attacchi contro diversi obiettivi israeliani. Questi gruppi, che difendono gli interessi palestinesi, mantengono un alto grado di segretezza; il loro numero esatto e le loro identità devono ancora essere confermati. Gli attacchi informatici, principalmente di tipo DDoS (Distributed Denial of Service), sono stati diretti contro infrastrutture critiche israeliane[1]. Tali attacchi mirano principalmente al governo e alle istituzioni israeliane, ma potrebbero estendersi a tentativi di compromissione dei sistemi di allerta-missile, come è già avvenuto recentemente per mano di Anonymous Sudan. Certamente lo stato di Israele è pronto ad affrontare tali scenari avversi e, dunque, è lecito attendersi un aumento degli attacchi, soprattutto a fronte dell'intensificarsi degli scontri con la Palestina[2]. Questo scenario dimostra quanto sia cruciale la sicurezza cibernetica per Israele, poiché il Paese deve prepararsi e proteggersi da attacchi informatici che potrebbero compromettere la sua stabilità e sicurezza nazionale. Come accennato, il conflitto tra Hamas e Israele si protrae anche sulla rete Internet. Come ha rivelato il caporedattore del Jerusalem Post, il giornale ha dovuto affrontare un aumento degli attacchi informatici al suo sito web, che lo hanno reso inaccessibile da quando Hamas ha lanciato l'attacco su vasta scala contro Israele. "Siamo stati bersaglio di una serie di devastanti attacchi informatici da quando la guerra è iniziata ieri mattina", ha scritto Avi Mayer, l'editore, in una e-mail. "Abbiamo cercato di contrastarli, ma ci hanno colpiti più volte." Mayer ha dichiarato che il giornale aveva degli "indizi" su chi fosse responsabile degli attacchi e sulla loro posizione, ma ha preferito non approfondire ulteriormente "per evitare di dare loro una pubblicità non meritata o di incentivare ulteriormente la loro motivazione a attaccare noi o chiunque altro"[3]. Inoltre, gruppi come "Ghosts of Palestine" sono riusciti con successo a rendere inaccessibili i siti web del Ministero dell'Istruzione israeliano e del Ministero degli Affari Esteri. Gli attacchi informatici non si sono limitati ai siti governativi e ai giornali online, ma si sono estesi anche ai canali social, come dimostra il recente attacco

[1] https://thecyberexpress.com/israel-palestine-conflict-cyber-warfare-risk/
[2] https://www.difesaesicurezza.com/difesa/cyber-warfare-gli-hacker-pro-russia-dichiarano-guerra-a-israele/
[3] https://www.thedailybeast.com/jerusalem-posts-website-taken-down-by-cyberattacks-day-after-hamas-strikes-israel

al canale Telegram del Presidente Isaac Herzog. Secondo un'indagine preliminare condotta dall'agenzia di sicurezza Shin Bet, l'attacco sembra essere di natura criminale piuttosto che legato al terrorismo. Non sono stati compromessi dati e l'account è stato successivamente ripristinato, come riportato dall'Agenzia per la Sicurezza Israeliana. Gilad Leibovitch, direttore accademico di diversi corsi di studio in materia di sicurezza informatica presso il Technion-Israel Institute of Technology di Haifa, ha dichiarato al Jerusalem Post che gli hacker probabilmente cercavano di ottenere informazioni di alto livello. Lo scorso anno, un ex addetto alle pulizie impiegato presso la casa dell'allora Ministro della Difesa israeliano Benny Gantz si è dichiarato colpevole di aver assistito hacker che Gerusalemme ha affermato essere affiliati al regime iraniano[4]. È evidente che Israele sta affrontando una crescente sfida nella dimensione cibernetica e deve adottare misure significative per proteggere le sue infrastrutture da futuri attacchi, che potrebbero prendere di mira obiettivi sempre più sensibili. La collaborazione internazionale nella lotta contro la minaccia cibernetica è essenziale per affrontare questa crescente sfida e garantire la sicurezza e la stabilità della nazione.

Gianluca Cipriani Ha conseguito la laurea in "Scienze Politiche" presso l'Università degli Studi "Roma Tre" e si è specializzato in "Relazioni Internazionali" presso l'Università degli Studi "Roma Tre" con un percorso incentrato sulla strategia militare e sicurezza internazionale. Dopo anni di esperienza come analista di geopolitica, attualmente svolge attività di consulenza in materia di cybersecurity.

Marco Raul Massoni Laureato in "Scienze della Politica" presso l'Università degli Studi di Macerata. Ha conseguito un master in Protezione Strategica del Sistema Paese: Cyber Intelligence, Big Data e Sicurezza delle Infrastrutture Critiche presso la Società Italiana per l'Organizzazione Internazionale (SIOI). Attualmente svolge attività di consulenza in materia di cybersecurity.

[4] https://www.israelhayom.com/2023/10/06/shin-bet-probes-hack-of-israeli-president-herzogs-telegram-account/

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' 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.

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.

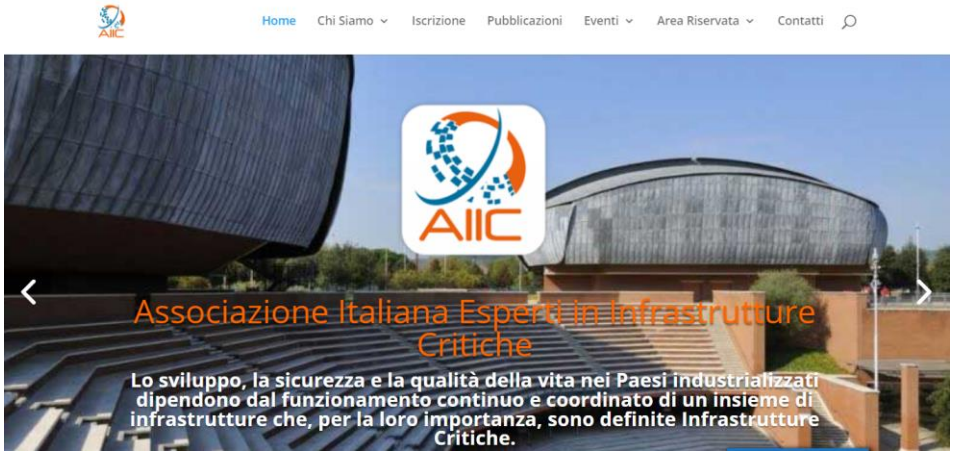
È invece raccomandato indicare, nel proprio profilo professionale, l'appartenenza ad AIIC, Associazione Italiana esperti in Infrastrutture Critiche, in qualità di socio.

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.

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

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*



WORKSHOP SU "GESTIONE DEL RISCHIO NELLA PROSPETTIVA DEI CAMBIAMENTI CLIMATICI" – Roma, 14 novembre 2023, ore 9.30

il Consiglio Direttivo di AIIC è lieto di informarvi che, nell'ambito del processo di formazione e informazione dei propri associati, i soci e i simpatizzanti di AIIC potranno partecipare ad un workshop sponsorizzato da AIIC sul tema

GESTIONE DEL RISCHIO NELLA PROSPETTIVA DEI CAMBIAMENTI CLIMATICI

Martedi' 14 Novembre 2023,
Aula Conferenze, Università di Roma Tre, Via Vito Volterra 62, Roma

Il workshop intende identificare una nuova agenda per la gestione delle Emergenze e di quella del Rischio quotidiano in una prospettiva di cambiamenti climatici che tenderanno ad imporre una maggiore attenzione nella gestione delle Infrastrutture e degli Asset strategici. La nuova Agenda, introdotta da una serie di iniziative legislative (recepimento della Direttiva Europea 2022/2557 relativa a "Critical Entity Resilience" da parte degli Stati Membri) ma anche quelle nazionali (D.L. Morandi), necessiterà di un utilizzo sempre maggiore di nuovi approcci che hanno necessità di essere integrati nei protocolli di Analisi del Rischio e dispiegate per la gestione delle Emergenze. Il Workshop mira a fornire una visione delle differenti componenti del Rischio nel nostro Paese, sia quelle endemiche che quelle che si aspetta avranno un impatto maggiore nei prossimi decenni alla luce delle nuove sfide legate ai cambiamenti climatici.

Tra i relatori è prevista la partecipazione del dott. Sandro Bologna, componente del Consiglio Direttivo di AIIC e coordinatore del Gruppo di Studio AIIC su "Resilienza delle Infrastrutture

Critiche e cambiamenti climatici" che sta terminando i lavori con la pubblicazione di un apposito report.

AGENDA
09:30 *Welcome*
Stefano Panzieri (Università di Roma Tre)
09:40 *Presentazione degli obiettivi del Workshop*
Simona Cavallini (TIEMS Italia e Progress Consulting)
09:50 *L'Evoluzione della Gestione delle Emergenze Nazionali e i Cambiamenti Climatici*
Guido Parisi (già Capo del Corpo Nazionale dei Vigili del Fuoco)
10:10 *Analisi eventi dell'alluvione in Romagna del Maggio 2023*
Massimo Bosi (Comune di Faenza)
10:30 *Cambiamenti Climatici e Resilienza delle Infrastrutture Critiche*
Sandro Bologna (TIEMS Italia e AIIC)
10:50 *Il rischio incendi: nuove prospettive*
Sergio Pirone (TIEMS Italia e Formont)
11:10 *Il rischio idrogeologico degli impianti industriali*
Fabrizio Paolacci (Università di Roma Tre)
11:30 *Osservazione dallo Spazio: interferometria e dati multispettrali per il monitoraggio del territorio e degli asset*
Salvatore Stramondo (Osservatorio Nazionale Terremoti, INGV)
11:50 *I servizi climatici*
Gianmaria Sannino (ENEA, Centro Ricerche Casaccia)
12:10 *Nuovi strumenti per l'Analisi del Rischio e l'Emergency Management*
Maurizio Pollino (ENEA)
12:30 Q&A e Chiusura
Vittorio Rosato (TIEMS Italia e EISAC.it)

La partecipazione all'evento è gratuita, previa registrazione.
Per ulteriori informazioni sul workshop:
info@tiems-ic.it
http://www.tiemsitalianchapter.it/

NEWS E AVVENIMENTI

Companies Explore Ways to Safeguard Data in the Age of LLMs
Generative AI models are forcing companies to become creative about how they keep employees from giving away sensitive data.
Large language models (LLMs) such as ChatGPT have shaken up the data security market as companies search for ways to prevent employees from leaking sensitive and proprietary data to external systems. Companies have already started taking dramatic steps to head off the possibility of data leaks, including banning employees from using the systems, adopting the rudimentary controls offered by generative AI providers, and using a variety of data security services, such as content scanning and LLM firewalls. The efforts come as research reveals that leaks are possible, bolstered by three high-profile incidents at consumer device maker Samsung and studies that find as much as 4% of employees are inputting sensitive data.

In the short term, the data security problem will only get worse — especially because, given the right prompts, LLMs are very good at extracting nuggets of valuable data from training data. Technical solutions will be important, says Ron Reiter, co-founder and CTO at Sentra, a data life cycle security firm.
"Data loss prevention became much more of an issue because there's suddenly ... these large language models with the capability to index data in a very, very efficient manner," he says. "People who were just sending documents around ... now the chances of that data landing into a large language model are much higher, which means it's going to be much easier to find the sensitive data."
Until now, companies have struggled to find ways to combat the risk of data leaks through LLMs. Samsung banned the use of ChatGPT in April, after engineers passed sensitive data to the LLM, including source code from a semiconductor database and minutes from an internal meeting. Apple restricted its employees from using ChatGPT in May to prevent workers from disclosing proprietary information, although no incidents were reported at the time. And financial firms, such as JPMorgan, have put limits on employee use of the service as far back as February, citing regulatory concerns. (continua…)
https://www.darkreading.com/dr-tech/companies-explore-ways-to-safeguard-data-in-the-age-of-llms
Dark Reading *-Robert Lemos -September* 18, 2023

Gestione del rischio idraulico e previsione dell'evoluzione delle onde di esondazione in tempo reale - La descrizione di nuovi strumenti che permettono di descrivere e analizzare gli eventi alluvionali, attraverso lo studio di eventi passati, la modellazione idraulica 2D attuando così misure di mitigazione dei rischi e la corretta gestione delle emergenze.
Rischio idraulico: gli strumenti di analisi degli eventi alluvionali
Tra le più frequenti manifestazioni di fragilità del territorio italiano c'è sicuramente quella legata al rischio idraulico.
Negli ultimi anni sono stati sviluppati nuovi strumenti che permettono una descrizione e una analisi più accurata degli eventi alluvionali. Tali strumenti consentono di intervenire in tre diverse fasi distinte:
Nella ricostruzione di eventi passati,
Nella progettazione di misure di mitigazione del rischio idraulico,
Nella gestione delle emergenze.
L'analisi dei dati territoriali per la modellazione idraulica 2D
L'avanzamento negli ultimi vent'anni delle tecniche di rilevamento della superficie terrestre ha permesso di ottenere rilievi di dettaglio in cui sono descritte con accuratezza tutte le forme del territorio che influiscono nell'evoluzione delle onde di esondazione su una piana alluvionale. (continua…)
https://www.ingenio-web.it/articoli/gestione-del-rischio-idraulico-e-previsione-dell-evoluzione-delle-onde-di-esondazione-in-tempo-reale
Ingenio *– Giovanni Moretti, 26.9.2023*

China APT Cracks Cisco Firmware in Attacks Against the US and Japan
Sophisticated hackers are rewriting router firmware in real time and hiding their footprints, leaving defenders with hardly a fighting chance.
An old Chinese state-linked threat actor has been quietly manipulating Cisco routers to breach multinational organizations in the US and Japan.

"BlackTech" (aka Palmerworm, Temp.Overboard, Circuit Panda, and Radio Panda) has been replacing device firmware with its own malicious version, in order to establish persistence and pivot from smaller, international subsidiaries to headquarters of affected organizations. Those organizations have thus far spanned government, industrial, technology, media, electronics, and telecommunication sectors, and include "entities that support the militaries of the U.S. and Japan," according to a new joint cybersecurity advisory from the National Security Agency (NSA), FBI, and Cybersecurity and Infrastructure Security Agency (CISA), as well as Japanese national police and cybersecurity authorities.

The advisory does not detail any specific CVE affecting Cisco routers. Instead, it explains, "this TTP is not solely limited to Cisco routers, and similar techniques could be used to enable backdoors in other network equipment."

Cisco has not yet responded to Dark Reading's request for comment.

According to Tom Pace, former Department of Energy head of cyber and now CEO of NetRise, it speaks to a more endemic problem in edge security. "If we get our hands on a firmware image from Cisco, Juniper, Huawei, Arista — it doesn't matter who it is," he says. "The same problems persist across all device manufacturers and all verticals."

How BlackTech Breaches Networks

Cisco routers have been subject to compromise and IP theft ever since the company first helped China build its national Internet censorship apparatus — the so-called "Great Firewall" — at the turn of the century. BlackTech, around since 2010, has taken the tradition a step further.

The group possesses 12 different custom malware families for penetrating and staking a foothold inside of Windows, Linux, and FreeBSD operating systems. They are lent an air of legitimacy by code-signing certificates and are constantly updated in order to evade antivirus detection.(continua…)

https://www.darkreading.com/threat-intelligence/china-apt-cracks-cisco-firmware-attacks-against-us-japan

Dark Reading - *Nate Nelson -September 27, 2023*

Building more cyber-resilient satellites begins with a strong network.

In the current global cyber cold war, nation-states prioritize taking control of another nation's satellite infrastructure and destroying it or rendering it useless. Shutting down a competing nation's satellites stops real-time communications, cuts off situational awareness of operating units across militaries and halts navigation. Today, denying a competing nation's access to space is quickly becoming the most dangerous weapon in the stealth world of cyber warfare.

Satellites and access to space are essential for national security. By 2030, there will be an average of 1,700 satellites launched per year and governments will continue to fund 75% of satellite manufacturing and launching. The global satellite communication (SATCOM) market size was estimated at $77B in 2022 and is expected to grow at a compound annual growth rate (CAGR) of 9.7% from 2023 to 2030.

Why satellites are strategic targets

The U.S. Defense Intelligence Agency writes in its 2022 Challenges to Security in Space report: "Space is being increasingly militarized. Some nations have developed, tested and deployed various satellites and some counter-space weapons. China and Russia are developing new space systems to improve their military effectiveness and reduce any reliance on U.S. space systems."

The agency cites known physical and cyberattacks on ground-infrastructure, space situational awareness sensors that can monitor and target satellites and attempts at jamming navigation and communication satellites. Directed energy weapons that can blind imagery satellites, anti-satellite weapons (ASAT) missiles that can destroy low earth orbit (LEO) satellites and create dangerous debris

and orbital weapons that can damage or tamper with satellites either are in development or have been deployed.
Chinese cyber attackers have long been targeting U.S. satellites and the disruption of NOAA satellite data is are example. Nation-state attackers continue to fine-tune their tradecraft in an attempt to disrupt ground control stations, jam or spoof satellite communication links, deliver malware into satellite control systems and use AI to find new attack patterns that will go undetected.
"Hybrid satellite networks (HSNs) are increasingly becoming a target for cyberattacks because they offer unique challenges for attackers," Jeff Hall, principal security consultant and North American aerospace lead at NCC Group, told VentureBeat.
The National Institute of Standards and Technology (NIST) explains that "the space sector is transitioning towards HSN, which is an aggregation of independently owned and operated terminals, antennas, satellites, payloads or other components that comprise a satellite system."
NIST framework required to reduce threat surfaces and close gaps
With competing nations stepping up their efforts to control access to space, it's timely that NIST's National Cybersecurity Center of Excellence has released its most recent report designed to guide the wide spectrum of space stakeholders who all contribute to the security posture of HSNs.
NIST's interagency report NIST IR 8441, Cybersecurity Framework Profile for Hybrid Satellite Networks provides a cross-functional framework for improving infrastructure security, hardening security for assets, data and systems, and reducing the cyber risks to HSNs. (continua…)
https://venturebeat.com/security/building-more-cyber-resilient-satellites-begins-with-a-strong-network/
VentureBeat -*Louis Columbus -October 2, 2023*

Laudate Deum: Papa Francesco lancia un appello urgente per l'azione climatica - Dal "Laudato Si'" al "Laudate Deum" - Il Papa Francesco ha rilasciato un appello urgente per affrontare la crisi climatica nel suo nuovo documento, l'Esortazione Apostolica "Laudate Deum." Questo nuovo documento segue l'Enciclica "Laudato si'" e ribadisce l'importanza cruciale di proteggere il nostro pianeta.
Ormai sono passati otto anni dalla pubblicazione dell'Enciclica "Laudato si'", quando Papa Francesco ha condiviso le sue preoccupazioni per la cura della nostra casa comune con il mondo. Tuttavia, con il passare del tempo, emerge con chiarezza che le nostre azioni non sono state sufficienti.
Il mondo che ci circonda è in pericolo, e i segnali di un'imminente catastrofe diventano sempre più evidenti. Gli effetti del cambiamento climatico colpiscono la vita di milioni di persone in termini di salute, lavoro, accesso alle risorse, abitazioni e migrazioni forzate.
Il Papa sottolinea che il cambiamento climatico non è solo una questione ambientale ma una sfida sociale globale che minaccia la dignità umana. I vescovi degli Stati Uniti hanno chiarito che la cura per la terra è intimamente legata alla cura per gli altri esseri umani. Il cambiamento climatico è una delle principali sfide della società globale, con effetti particolarmente gravi per le persone più vulnerabili.
Questo nuovo documento di Papa Francesco riflette sugli sviluppi degli ultimi otto anni e sottolinea l'urgenza di agire. Le pagine di "Laudate Deum" ci invitano a rinnovare il nostro impegno per la salvaguardia del nostro pianeta e a riconoscere che il cambiamento climatico è un dramma che colpisce tutti noi." L'Esortazione Apostolica "Laudate Deum" di Papa Francesco richiama l'attenzione sulle sfide climatiche che affrontiamo e ci esorta a unire gli sforzi per proteggere il nostro mondo.
Mentre "Laudato Si'" era un trattato completo di 180 pagine, la "Laudate Deum" si distingue per la sua brevità di soli 12 pagine. Questa scelta suggerisce un desiderio di comunicare in modo diretto e incisivo l'urgenza della situazione climatica. Tuttavia, la sua efficacia potrebbe essere amplificata dalla sua semplicità, rendendolo più accessibile a un pubblico più ampio.

Il contenuto della "Laudate Deum" (continua).
https://www.ingenio-web.it/articoli/laudate-deum-papa-francesco-lancia-un-appello-urgente-per-l-azione-climatica/
INGENIO *– Andrea Dari, 4.10.2023*

Cyberattack against Johnson Controls sparks downstream concerns.
Worries mounted quickly after the attack on the building automation and industrial control systems vendor, which works extensively with multiple federal agencies.
A September cyberattack against Johnson Controls International remains under investigation, but concerns linger about potential downstream impacts that may hit the company's customers.
The company, which was founded in Milwaukee but now headquartered in Ireland, does extensive business with U.S. federal agencies and the defense industrial base sector and first disclosed the incident in a Sept. 27 filing with the Securities and Exchange Commission. Concerns escalated days later.
Johnson Controls, which manufactures industrial control systems, physical security alarm systems and facility-related technology and infrastructure, is responding to what security experts described as a ransomware attack that disrupted some internal IT infrastructure and applications.
The company declined to share new details about the incident or its ongoing investigation and referred back to its SEC filing.
Senior officials in the Department of Homeland Security, which has contracts with Johnson Controls, were trying to determine if the attack compromised sensitive physical security information, including agency building floor plans, CNN reported Friday.
"We are assessing the potential impacts of this incident and implementing additional safeguards to our layered security model," a DHS spokesperson told Cybersecurity Dive. "This was not a breach of any DHS network or system." The Cybersecurity and Infrastructure Security Agency is "coordinating closely with Johnson Controls to understand impacts from this incident and provide assistance as necessary," a spokesperson said.(continua…)
https://www.cybersecuritydive.com/news/johnson-controls-cyberattack-downstream-impact/695675/
Cybersecuritydive -*Matt Kapko- Published Oct. 5, 2023*

La progettazione ambientale residenziale per la prevenzione della criminalità - Tutti gli architetti coinvolti nella progettazione di centri residenziali debbono prestare attenzione alla norma ISO 22344-2 - Linee guida per la prevenzione della criminalità attraverso la progettazione ambientale degli insediamenti residenziali. L'esperienza insegna che la progettazione di misure di sicurezza, prima della realizzazione di un sito residenziale, comporta un aumento dei livelli di sicurezza e un risparmio sui costi. Ecco il motivo per cui questa norma è oltremodo importante per chiunque sia coinvolto nella progettazione di insediamenti residenziali.
Ecco il titolo completo della edizione 2023:
ISO/CD 22344-2:2023 -Security and resilience — Protective security — Guidelines for crime prevention through environmental design for residential facilities (Linee guida per la prevenzione della criminalità attraverso la progettazione ambientale degli insediamenti residenziali)
Il documento offre ai progettisti una linea guida per individuare delle strategie generali e specifiche, che possono prevenire o ridurre il crimine, ed anche il timore del crimine, in un insediamento residenziale, composto da un singolo edificio o da più edifici.

Il documento raccomanda di avviare una completa analisi di rischio, preferibilmente secondo le indicazioni della norma ISO 31000, e successivamente applicare misure di mitigazione o prevenzione, che possono essere differenziate in funzione della destinazione specifica dell'area residenziale. (continua…)
https://www.puntosicuro.it/criminalita-C-105/la-progettazione-ambientale-residenziale-per-la-prevenzione-della-criminalita-AR-23715/
PuntoSicuro - *Adalberto Biasiotti, 6.10.2023*

IoT: l'indispensabile connessione tra sicurezza fisica e digitale
La sfera dell'information technology e quella della physical security sono sempre più interdipendenti, eppure il disallineamento e la mancata integrazione tra questi due settori restano piuttosto evidenti. Ecco gli elementi di criticità
La sempre più ampia presenza di tecnologia internet of things, quindi di oggetti connessi in rete, sta facendo apparentemente **sfumare i confini tra realtà fisica e digitale.**
In questo contesto **l'attività di security** va sempre più indirizzata alla protezione di sistemi complessi e non più di singole tipologie di asset.
Indice degli argomenti
- *Sicurezza fisica baluardo degli asset virtuali*
- *Costruire un legame tra sicurezza fisica e cyber*
- *Evitare la disconnessione tra sicurezza fisica e digitale*
- *Conclusioni*

Sicurezza fisica baluardo degli asset virtuali
Del resto, il bisogno di protezione degli asset informativi digitali dovuto alle esigenze di continuità operativa dei servizi erogati e finalizzato a garantirne disponibilità, integrità e riservatezza è sempre più pregnante nel tessuto socioeconomico odierno ed è pertanto diventato prioritario sostenere investimenti e sviluppi organizzativi finalizzati a elevare i livelli di sicurezza informatica. Questo è ancora più vero se facciamo una analisi dello scenario geopolitico attuale. (continua..)
https://www.agendadigitale.eu/sicurezza/iot-lindispensabile-connessione-tra-sicurezza-fisica-e-digitale/
Agenda Digitale- *Stefano Piroddi - 6 ott 2023*

RANSOMWARE ATTACK ON MGM RESORTS COSTS $110 MILLION
Hospitality and entertainment company MGM Resorts announced that the costs of the recent ransomware attack costs exceeded $110 million**.**
In September the hospitality and entertainment company MGM Resorts **was hit by a ransomware attack** that shut down its systems at MGM Hotels and Casinos.
The incident affected hotel reservation systems in the United States and other IT systems that run the casino floors.
The company now revealed that the costs from the ransomware attack have exceeded $110 million. The company paid third-party experts $10 million to clean up its systems.
A few days later, an affiliate of the BlackCat/ALPHV ransomware group known as Scattered Spider claimed responsibility for the attack.
"The Company believes that the operational disruption experienced at its affected properties during the month of September will have a negative impact on its third quarter 2023 results, predominantly in its Las Vegas operations, and a minimal impact during the fourth quarter. The Company does not expect

that it will have a material effect on its financial condition and results of operations for the year. Specifically, the Company estimates a negative impact from the cyber security issue in September of approximately $100 million to Adjusted Property EBITDAR for the Las Vegas Strip Resorts and Regional Operations, collectively." reads the 8-K report filed with SEC. "The Company has also incurred less than $10 million in one-time expenses in the third quarter related to the cybersecurity issue, which consisted of technology consulting services, legal fees and expenses of other third party advisors."
The Company states that its cybersecurity insurance will cover the financial losses and future expenses, however, the full scope of the costs and related impacts has yet to be determined. (continua…)
https://securityaffairs.com/152077/cyber-crime/mgm-resorts-ransomware-attack.html
Security Affairs - *Pierluigi Paganini- October 06, 2023*

Operation Behind Predator Mobile Spyware Is 'Industrial Scale'
The Intellexa alliance has been using a range of tools for intercepting and subverting mobile and Wi-Fi technologies to deploy its surveillance tools, according to an investigation by Amnesty International and others.
The recent surge in Predator spyware is the result of a widespread and entrenched grey-area commercial operation that trades surveillance operations "at industrial scale."
That's according to an analysis by Amnesty International's Security Labs of data gathered by the European Investigative Collaboration (EIC) media network, which has unearthed new information on how the actors behind the shadowy Predator mobile surveillance tool deliver it to target Android and iOS devices.
The analysis is contained in a recent report entitled the Predator Files, and is focused largely on Intellexa — an alliance of intelligence systems providers that the US Commerce Dept. and many others have identified as the main purveyor of Predator. It describes how Intellexa has been using a wide range of supporting products from alliance partners to intercept and subvert mobile networks and Wi-Fi technologies — sometimes in collaboration with Internet service providers (ISPs).
Predator Spyware: A Pervasive & Dangerous Threat
"Intellexa alliance's products have been found in at least 25 countries across Europe, Asia, the Middle East and Africa, and have been used to undermine human rights, press freedom, and social movements across the globe," Amnesty International said. "The 'Predator Files' investigation shows what we have long feared: that highly invasive surveillance products are being traded on a near industrial scale and are free to operate in the shadows without oversight or any genuine accountability."
Just this week, Sekoia reported on a campaign where Madagascar's government dropped Predator — a tool that can extract practically everything and listen to everything on a target device — on mobile devices belonging to target individuals in the country. Google's Threat Analysis Group in September released a report describing how Intellexa had developed an exploit chain for three iOS zero-day vulnerabilities that was later used in an attack on Egyptian organizations. (continua…)
https://www.darkreading.com/endpoint/operation-behind-predator-mobile-spyware-industrial-scale
Dark Reading *-Jai Vijayan- October 09, 2023*

HACKTIVISTS IN PALESTINE AND ISRAEL AFTER SCADA AND OTHER INDUSTRIAL CONTROL SYSTEMS
Both pro-Israeli and pro-Palestinian hacktivists have joined the fight in the cyber realm. Industrial control systems (ICS) seem to be one of the most lucrative targets for them, and there are hundreds exposed.

After Hamas gunmen killed hundreds of Israelis and took an unknown number of people hostage, Israel has now retaliated with airstrikes on Gaza.
Some people took to social media to, for example, show support for Israel by adding the country's flag to their profile pictures. Thousands marched on the streets to express support for the Palestinian side. Others turned to cyber weapons to voice their opinion and sow chaos. Hacktivists are already launching attacks on various systems amid a grave escalation of the Israeli-Palestinian conflict.
We've already reported on a multitude of attacks, mostly distributed denial of service (DDoS), against Israel. Hacktivists have targeted the Israeli government and media, among other organizations.
Some threat actors, such as ThreatSec, haven't claimed any allegiance and are boasting about attacking both sides alike.
"As you might know, we don't like Israel, but… We also don't like War! Soooo, as we have attacked Israel in the past, we now attack the Gaza region, where many of the Hamas fighters are located!" the gang wrote on Telegram, claiming that it had shut down nearly every server owned by Alfanet.ps – including Quintiez Alfa General Trading, which is one of the biggest ISPs (internet service providers) in the Gaza Strip.
ThreatSec is part of the "Five Families" – notorious and highly organized gangs (the others are GhostSec, Stormous, Blackforums, and SiegedSec) that collaborate on launching big cyberattacks.
Mantas Sasnauskas, head of the Cybernews research team, highlighted that many hacktivists go after various ICSs in an attempt to disrupt critical infrastructure and draw international attention.
Since a cyberattack on critical infrastructure can have serious repercussions, including operational disruptions, safety hazards, economic costs, and reputational damage, cybersecurity should be a top priority in the organizations that administer them. (continua…)
https://securityaffairs.com/152224/hacktivism/hacktivists-palestine-israel-after-scada-ics.html
Security Affairs- *Pierluigi Paganini - October 10, 2023*

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.