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 2023 | **n. 1/ 2023** | **Gennaio 2023**

NIS 2: Strategia nazionale e gestione dei rischi

Il 14 dicembre 2022 è stato pubblicato in Gazzetta ufficiale dell'Unione europea il testo relativo alla NIS 2 (https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32022L2555). Tra le diverse novità introdotte dalla direttiva, è utile sottolineare che la NIS2 incorpora una struttura per la segnalazione degli incidenti composta da due fasi. Indipendentemente dalla supervisione proattiva o reattiva, la legislazione impone che qualsiasi incidente significativo venga segnalato entro 24 ore dall'insorgenza, aggiungendo dettagli entro 72 ore. Pertanto, è necessaria un'integrazione contenente maggiori dettagli come misura di follow-on; questa deve essere inviata entro un mese dall'avvenuto un incidente. Questa impostazione ha l'obiettivo di raccogliere rapidamente dettagli relativi all'evento e condividerli - tra i diversi addetti ai lavori – al fine di prevenire eventuali impatti derivanti da attacchi simili e per fornire un'analisi approfondita dell'incidente che sia utile per la pianificazione di nuovi modelli di resilienza.
Con il termine "incidente significativo" di cybersecurity il legislatore intende definire un evento in grado di causare gravi conseguenze operative dei servizi o perdite finanziarie per l'organizzazione. Inoltre, tale evento può avere ripercussioni su persone fisiche o giuridiche causando danni materiali o immateriali considerevoli. Le entità sono, dunque, tenute a indicare se sospettano che l'incidente significativo sia il risultato di attività illecite o dolose e se questo possa avere impatti transnazionali.
Tra i diversi articoli che compongono la direttiva è utile porre l'accendo sull'art. 7 relativo alla necessità per ciascun stato di dotarsi di una strategia di sicurezza e l'art. 21 concernente le misure per la gestione dei rischi.

La Strategia nazionale per la cybersecurity

L'art. 7 impone a ciascuno stato membro dell'UE di adottare una strategia di sicurezza nazionale considerando i seguenti obiettivi strategici:

- Obiettivi e priorità della strategia di cybersecurity dello Stato membro
- Un quadro di governance per raggiungere gli obiettivi e le priorità dichiarati
- Un quadro di governance che chiarisca i ruoli e le responsabilità delle parti interessate degli Stati membri, i punti di contatto istituiti e i tram di risposta agli incidenti di sicurezza informatica (CSIRT)
- Un meccanismo per individuare le attività pertinenti e le valutazioni dei rischi degli Stati membri
- Identificazione delle misure che garantiscono la preparazione, la risposta e la pianificazione della ripresa per includere la cooperazione pubblico-privato
- Un elenco delle autorità e dei portatori di interessi coinvolti nell'attuazione della strategia nazionale per la cybersecurity stabilita dallo Stato membro e per conto dello Stato membro

Inoltre, l'articolo stabilisce politiche di dettaglio che ciascuno Stato membro deve integrare nelle proprie strategie, tra cui considerazioni sulla catena di approvvigionamento delle TIC (Tecnologie dell'Informazione e della Comunicazione), orientamenti per le piccole e medie imprese, gestione delle vulnerabilità, sicurezza di Internet, requisiti per l'adozione di tecnologie e strumenti di condivisione delle informazioni, formazione e istruzione, e piani per migliorare il livello generale di consapevolezza in materia di sicurezza informatica per i cittadini.

Le misure di gestione dei rischi per la cybersecurity

La gestione del rischio di cui all'art. 21 interessa gli aspetti tecnici, operativi e organizzativi relativi alla sicurezza delle reti e dei sistemi informativi su cui le entità fanno affidamento per la fornitura di beni e servizi. La legislazione impone alle entità di valutare la proporzionalità delle attività di gestione del rischio, considerando il loro grado di esposizione ai rischi, le dimensioni, la probabilità di incidenti e la loro gravità, nonché gli impatti sociali ed economici derivanti da potenziali incidenti.

In generale, la NIS 2 promuove l'inclusione delle seguenti misure in ciascun programma di gestione del rischio:

- Politiche sull'analisi dei rischi e sulla sicurezza dei sistemi informativi
- Gestione degli incidenti
- Continuità operativa, ad esempio gestione dei backup e ripristino di emergenza e gestione delle crisi
- Sicurezza della catena di approvvigionamento, compresi gli aspetti relativi alla sicurezza riguardanti le relazioni tra ciascuna entità e i suoi fornitori diretti o prestatori di servizi
- Sicurezza nell'acquisizione, nello sviluppo e nella manutenzione di reti e sistemi informativi, compresa la gestione e la divulgazione delle vulnerabilità
- Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersecurity
- Pratiche di base per la cyber hygiene e formazione sulla sicurezza informatica
- Politiche e procedure relative all'uso della crittografia
- Sicurezza delle risorse umane, politiche di controllo degli accessi e gestione delle risorse
- Uso di soluzioni di autenticazione a più fattori o autenticazione continua

In conclusione, la direttiva risulta essere un fondamentale punto di partenza per indirizzare gli sforzi degli stati membri in ottica di cyber-resilienza e si pone come il primo passo di un più ampio percorso che l'Unione Europea intende affrontare per contrastare le nuove ed emergenti minacce presenti nel panorama della cybersecurity.

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.

Andrea Agostino Fumagalli Laureato in “Giurisprudenza” presso l’Università degli Studi di Milano con tesi in Informatica Giuridica Avanzata, ha maturato diverse esperienze lavorative nell’ambito legale e di compliance, occupandosi di sicurezza delle informazioni. Attualmente svolge attività di consulenza in materia di cybersecurity.

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

ATTIVITA' DI EDUCATION

Sono in corso di programmazione le attività di formazione per soci e simpatizzanti che si svolgeranno nell'anno 2023.

Anzitutto, l'accordo con IsacaRoma consentirà 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 questi eventi, possibilmente – se le condizioni pandemiche lo consentiranno – in modalità mista, presenza e distanza.
Inoltre, stiamo già prendendo accordi per una ripresa delle 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.

VISITA GUIDATA PRESSO LA DIVISIONE AEREA DI SPERIMENTAZIONE AERONAUTICA E SPAZIALE (AEROPORTO DI PRATICA DI MARE) aggiornamento

Come già comunicato negli avvisi precedenti, abbiamo contattato lo Stato Maggiore dell'Aeronautica Italiana che ci ha confermato la disponibilità ad organizzare una visita guidata presso il **Reparto Sperimentale di Volo** della **Divisione Aerea di Sperimentazione Aeronautica e Spaziale (D.A.S.A.S.)**, situato presso l'aeroporto militare "Mario de Bernardi" di Pratica di Mare (Roma).

Il programma di massima prevede:

- presentazione delle principali attività del Reparto Sperimentale di Volo e dei Gruppi componenti, in particolare il Gruppo Gestione Software ed il Gruppo Ingegneria per l'Aerospazio;
- illustrazione delle attività per il biocontenimento dei velivoli per l'emergenza Covid-19;
- le caratteristiche dei velivoli presenti;
- la funzione di Entry Point sanitario nazionale per la gestione delle emergenze epidemiologiche.

Ottenuta l'approvazione dello Stato Maggiore Aeronautica, sono in corso i contatti con il D.A.S.A.S. per definire il programma operativo della visita, che potrebbe essere effettuata nel periodo metà febbraio-marzo 2023, durata prevista 3 ore, luogo di incontro Aeroporto di Pratica di Mare (Roma) da raggiungersi con mezzi propri.

Siamo quindi in attesa delle modalità con cui ottenere i permessi di ingresso in zona militare, a seguire procederemo con l'apertura delle iscrizioni. Vi terremo informati.

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

Attenzione! **La visita è riservata ai soli soci AIIC in regola con il pagamento delle quote sociali.** I signori non-soci che volessero partecipare, possono iscriversi all'Associazione AIIC usufruendo di una quota di associazione minima (euro 50 anno + 10 una tantum).

Le modalità per l'iscrizione si trovano sul sito www.infrastrutturecritiche.it o si possono richiedere inviando una mail a segreteria@infrastrutturecritiche.it

RINNOVO ASSOCIATIVO ANNO 2023

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

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.

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

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

NEWS E AVVENIMENTI

L'evoluzione dei ponti: materiali e schemi strutturali - Nel presente articolo si ripercorre la storia dei ponti con la loro evoluzione sia in termini di materiali che di schemi strutturali.
Ferro e cemento armato hanno reso possibili opere impensabili con legno e muratura
I disastri che negli ultimi anni hanno interessato diverse opere stradali hanno portato all'attenzione dell'opinione pubblica la sicurezza di ponti e viadotti e accresciuta la curiosità a saperne di più di queste opere la cui costruzione affonda le radici nella storia, risalendo al periodo neolitico.
La costruzione di un ponte ha sempre avuto la motivazione di superare, con un percorso carrabile o pedonabile, un ostacolo dovuto alla configurazione del terreno, per esempio una valle o un fiume, e l'obiettivo di facilitare gli spostamenti, i contatti con i popoli vicini, gli scambi, i commerci. L'evoluzione dei ponti ha accompagnato la storia dell'umanità, seguendo e rappresentando i tempi. Ad esempio, mentre i romani furono dei grandi costruttori di ponti avendo bisogno di collegamenti veloci e sicuri per il mantenimento e il controllo dell'impero, alla caduta dell'Impero Romano e fino al IX secolo d.C., invece, l'interesse per i ponti diminuì notevolmente perché le unità politiche si estendevano su superfici

ridotte e, di conseguenza, non potevano affrontare le spese per la costruzione e la manutenzione di opere così impegnative.
Costruire un ponte è sempre stata una sfida contro le forze della natura, accompagnata dalla paura dell'insuccesso e proprio queste difficoltà hanno affascinato i popoli. La disponibilità di nuovi materiali e l'utilizzo di nuove tecnologie hanno rivoluzionato il modo di costruire e di concepire un ponte, anche se l'ammirazione per i ponti antichi, sopravvissuti fino ai nostri giorni, non è minore di quella verso i moderni ponti di grande luce.
Nel presente articolo, che riprende e aggiorna un articolo precedente, si esaminano i materiali e le tipologie utilizzate per superare luci sempre maggiori con costi sempre più sostenibili. La disponibilità di materiali come il ferro e il cemento armato ha offerto nuove possibilità, impensabili con legno e muratura.
Allo stesso tempo, la necessità di adottare sistemi ad arco, che meglio sfruttavano le proprietà della muratura di resistere bene soltanto a compressione, grazie all'utilizzo di acciaio e cemento armato, ha lasciato posto anche a tipologie di più semplice realizzazione, quali i ponti a travata, o caratterizzate da elementi tesi, come i ponti strallati e sospesi.
(continua)
https://www.ingenio-web.it/articoli/i-ponti-monumento-al-progresso-la-loro-storia-e-la-loro-evoluzione
***INGENIO -** Paolo Clemente - 13.12.2022*

Cybersecurity nel 2023 fra metaverso e Intelligenza Artificiale – Le previsioni per il settore evidenziano essenzialmente tre eventualità: *gli attacchi ai processi aziendali, quelli alle identità e quelli alle intelligenze artificiali*.
Nella prima eventualità si annoverano i **supply chain attack** e le assicurazioni informatiche. Il primo tema è suffragato dall'incremento che negli ultimi due anni hanno contraddistinto gli *attacchi alla supply chain digitale*. Con la conseguenza diretta che le aziende sono sempre più preoccupate per la tranquillità dei partner e dei fornitori. Quella delle **assicurazioni informatiche** è invece una questione poco evidenziata. Gli assicuratori hanno iniziato a subire pesanti perdite da quando, per *coprire le estorsioni informatiche*, hanno cominciato a trasferire i relativi costi sui loro clienti.
Per quanto riguarda **le identità** le previsioni riguardano metaverso ed autenticazione a più fattori (MFA).
Il primo attacco del *metaverso* deriverà da una vulnerabilità nelle nuove funzionalità di produttività aziendale**, come il remote desktop.**
Per l'MFA, verranno impiegate tecniche di bypass MFA malevole per attacchi mirati alle credenziali.
L'ultima previsione riguarda i processi di sviluppo e parte dall'assunto che la qualità dell'output sarà in linea con la qualità dei dati che vengono immessi. Con un codice errato o non sicuro, l'uscita dell'AI sarà analoga.
https://www.securityopenlab.it/news/2413/cybersecurity-nel-2023-fra-metaverso-e-intelligenza-artificiale.html
***Redazione SecurityOpenLab**, 16-12-2022*

App malevole con 2 milioni di Download rilevate sul Play Store
Gli analisti Doctor Web riferiscono di aver trovato una nuova serie di applicazioni dannose, di phishing e adware nel Google Play Store, che sono state scaricate **da oltre due milioni di persone in totale**. La maggior parte delle applicazioni rilevate fingeva di essere delle utility e degli ottimizzatori,

mentre in realtà causavano solo malfunzionamenti del dispositivo, mostravano annunci intrusivi e rovinavano la vita agli utenti. Ad esempio, una delle applicazioni scoperte, scaricate più di un milione di volte, era TubeBox. Con il suo aiuto, i proprietari di dispositivi Android potrebbero guadagnare denaro guardando video e pubblicità.
https://www.redhotcyber.com/post/app-malevole-con-2-milioni-di-download-rilevate-sul-play-store/
Red Hot Cyber *– Redazione RHC - 18/12/2022*

Cybersecurity delle infrastrutture critiche – Di fronte alla crescita in Europa delle attività di spionaggio e sabotaggio, è necessario **incrementare la protezione delle infrastrutture critiche**, nel mirino dei cyber criminali per fini prettamente finanziari, ma anche di quelli sostenuti dagli stati nazionali, con lo scopo preminente di provocare disservizi e danni materiali.
È evidente una importante differenza tra difensori e attaccanti, in quanto i difensori, muovendosi di slancio, riescono solo e limitare i danni del potenziale distruttivo degli attacchi. Attacchi che sono sferrati con tecniche vecchie e nuove. Tra le prime il phishing nelle sue varie declinazioni (spoofing, spear phishing, eccetera), incentrato sul fattore umano e seguito nell'attacco dal ransomware. Fra le nuove tecniche, la capacità di aggirare l'antivirus con una serie di impronte digitali incoerenti, il malware fileless.
Il riconoscimento precoce di tentativi di attacco viene effettuata generalmente con **l'analisi di qualsiasi tipo di indicatore di compromissione (IoC)**. Quelli più facili da individuare sono marcatori o pattern di codice maligno, già accertati come dannosi. Quelli più difficili sono quelli deboli, come un movimento laterale e tracce di offuscamento in un file. A prescindere dal tipo di **IoC**, la procedura passa per l'analisi dei log: milioni di dati generati dalle soluzioni per la protezione degli endpoint o perimetrale. La prima conseguenza è che non è possibile un'ispezione manuale nei tempi richiesti, tanto che le aziende si vedono costrette a ricorrere a soluzioni basate su Intelligenza Artificiale e Machine Learning.
In ogni caso, **non si può fare esclusivo affidamento su strumenti e algoritmi**. Gli esperti di security di Stormshield sottolineano che ormai **occorrono metodologie di controllo e protezione che si adattino all'ambiente di lavoro**, combinando il monitoraggio continuo al perfezionamento e alla comprensione dei dati, che vanno condivisi internamente secondo i principi dell'intelligenza collettiva. Per questo il pool migliore di strumenti da usare include SOC, Cyber Threat Hunting e combinazione coerente delle conoscenze acquisite sugli attaccanti.
https://www.securityopenlab.it/news/2457/cybersecurity-delle-infrastrutture-critiche.htm
Redazione SecurityOpenLab*, 19-12-2022*

Attacco informatico al Ministero dell'agricoltura italiano e ad altri siti governativi
Da oggi il sito **www.politicheagricole.it** risulta non raggiungibile. Tutti si chiedevano cosa mai fosse successo, visto che il sito non rispondeva più alle richieste degli utenti. RHC cercando nelle underground ha compreso l'accaduto. Si è trattato di un attacco DDoS svolto da un gruppo di criminali informatici russi "senza nome" che hanno pubblicato poco fa sul loro canale Telegram (frequentato da pochissimi follower, circa 200 nella versione inglese e 12.000 in quella russa) una rivendicazione dell'accaduto.
(*continua*)
https://www.redhotcyber.com/post/attacco-informatico-al-ministero-dellagricoltura-della-sovranita-alimentare-e-delle-foreste-italiano/
Red Hot Cyber – *Redazione RHC - 3/12/2022*

Infrastrutture critiche, cyber-attacchi più che raddoppiati nel 2022

Offensive in crescita del 138% (da 5.434 a 12.947). In aumento anche il numero di persone indagate, gli alert diramati e le richieste di cooperazione internazionale. La ragione? Il contesto geopolitico della guerra in Ucraina. Il rapporto del Servizio Polizia postale e delle comunicazioni, guidato da Ivano Gabrielli

Gli attacchi alle infrastrutture critiche informatizzate del Paese rilevati dal Servizio Polizia postale e delle comunicazioni, guidato da **Ivano Gabrielli**, sono aumentati del 138% nel corso del 2022 rispetto all'anno precedente. È quanto emerge dal Resoconto attività 2022 della Polizia postale e delle comunicazioni e dei Centri operativi sicurezza cibernetica.

La ragione? Le tensioni geopolitiche legate all'invasione russa dell'Ucraina, un elemento centrale nel panorama cyber come ha spiegato nei giorni scorsi **Pierluigi Paganini**, amministratore delegato di Cybhorus, a *Formiche.net*.

Gli attacchi alle infrastrutture critiche nel 2021 erano stati 5.434; nel 2022, invece, 12.947 (dati rilevati il 27 dicembre scorso). In aumento del 78% anche le persone indagate (da 187 a 332); del 2% gli alert diramati (110.524 contro 113.226); del 28% le richieste di cooperazione gestite dall'ufficio del punto di contatto Htc, la "rete" per le emergenze cibernetiche istituita dalla convenzione di Budapest (la più importante struttura di cooperazione internazionale e per il contrasto alle attività criminali). (continua…)

https://formiche.net/2023/01/rapporto-polizia-postale-cyber-attacchi-2022/

***FORMICHE** - Gabriele Carrer - 03/01/2023 –*

Space Race: Defenses Emerge as Satellite-Focused Cyberattacks Ramp Up

Amid escalating cyber activity, two separate cybersecurity frameworks are targeting the satellite arena, highlighting the ease in attacking the infrastructure and the difficulty in defending it.

With cyberattacks becoming a reality against the space sector's infrastructure in 2022, two groups are aiming to get ahead of future attacks by creating framework initiatives.

The goal of the frameworks is to better understand not only potential threats — in terms of the traditional tactics, techniques, and procedures (TTPs) applied to the space sector — but also to help companies and government agencies create countermeasures against attacks targeting satellites and spacecraft.

On Jan. 3, the US National Institute of Standards and Technology (NIST) and the MITRE Corp., which is also a government contractor, released a version of the NIST Cybersecurity Framework tailored to the ground-based portion of the space sector. The NIST publication complements another effort by nonprofit government contractor The Aerospace Corp., which created in October the Space Attack Research and Tactics Analysis (Sparta) matrix, a version of the MITRE ATT&CK framework applied to threats against space-based infrastructure.

Cyberattacks Are Now Targeting Satellites

Early in 2022, the FBI and CISA warned that attacks against satellite ground-based and space-based infrastructure could become a reality — and it soon did. The year saw nation-state operations targeting Viasat and SpaceX's Starlink satellites and forcing governments and aerospace companies to create defenses against the attacks.

In the early days of Russia's invasion of Ukraine, for example, Russia-aligned hackers targeted the ground-based segment of Viasat's satellite communications network, taking Internet modems offline throughout Europe. Soon after, Russia also targeted the distributed satellite Internet service Starlink, according to government officials and SpaceX_CEO Elon Musk, which has been critical for providing the Ukraine war effort with Internet connectivity.

"Starlink has resisted Russian cyberwar jamming & hacking attempts so far, but [attackers are] ramping up their efforts," Musk stated on Twitter last May.
In November, Starlink was in the crosshairs again, with Russia-linked Killnet APT targeting it with a DDoS campaign that made the service inaccessible for several hours. (continua….)
https://www.darkreading.com/ics-ot/space-race-defenses-satellite-cyberattacks
***DARKREADING**- Robert Lemos-January 05, 2023*

From Ferrari to Ford, Cybersecurity Bugs Plague Automotive Safety
Security vulnerabilities plague automakers, and as vehicles become more connected, a more proactive stance on cybersecurity will be required — alongside regulations.
A range of automakers from Acura to Toyota are plagued by security vulnerabilities within their vehicles that could allow hackers to access personally identifiable information (PII), lock owners out of their vehicles, and even take over functions like starting and stopping the vehicle's engine.
According to a team of seven security researchers, whose efforts were detailed on Web application security specialist Sam Curry's blog, vulnerabilities across automakers' internal applications and systems allowed them in a proof-of-concept hack to send commands using only the VIN (vehicle identification number), which can be seen through the windshield outside the car.
In all, the team uncovered serious security issues from automakers such as BMW, Ferrari, Ford, Volvo, and many others, across Europe, Asia, and the United States. It also found issues at suppliers and telematics companies including Spireon, which develops GPS-based vehicle tracking solutions.
A BMW Group spokesperson tells Dark Reading that IT and data security have the "highest priority" for the company and that it is continuously monitoring its system landscape for possible vulnerabilities or security threats.
The spokesperson adds that the vulnerability mentioned in the report has been known since beginning of November and has been processed according to BMW's "security standard operating procedures," e.g., its bug-bounty program.
"The relevant addressed vulnerability issues were closed within 24 hours and we have no indication of any data leaks," the spokesperson says. "No vehicle-related IT systems were affected nor compromised. No BMW Group customers or employee accounts were compromised."
This is only the latest security concern to come to light. In March, telemetry from industrial systems security firm Dragos spotted Emotet command-and-control servers communicating with several automotive manufacturer systems. The malware is commonly used as an initial infection vector to drop ransomware.
In December, at least three mobile apps tailored to allow drivers to remotely start or unlock their vehicles were found to have security vulnerabilities that could allow unauthenticated malicious types to do the same from afar.
Automakers Slow to Recognize Growing Threat (continua…)
https://www.darkreading.com/ics-ot/ferrari-ford-cybersecurity-bugs-automotive-safety
***DARKREADING** - Nathan Eddy - January 06, 2023*

Texas County EMS Agency Says Ransomware Breach Hit 612,000
A municipal ambulance services provider that serves 15 cities in a Texas county has reported to federal regulators a ransomware breach potentially affecting 612,000 individuals, which is equivalent to nearly 30% of the county's 2.1 million population.

Metropolitan Area EMS Authority, a Texas government administrative agency that does business as MedStar Mobile Healthcare, reported the hacking incident to the U.S. Department of Health and Human Services' Office for Civil Rights on Dec. 19. MedStar, which provides ambulance services in Tarrant County, Texas, reported that on Oct. 20, it experienced "issues" with its network systems.
Colman McCarthy, an attorney at law firm Shook, Hardy & Bacon, which represents MedStar, tells Information Security Media Group the breach involved ransomware. MedStar did not pay a ransom but was able to fully restore its systems.
"Access to a portion of MedStar's network was affected. All servers were back online within 48 hours," McCarthy says. "Throughout the incident, MedStar continued to provide emergency medical services to the communities it serves."
MedStar is still determining the full scope of the incident and intends to offer credit monitoring "as required by law and in line with industry practice."
Breach Details
In its breach notification statement, MedStar says an unauthorized third party gained access to a restricted location in MedStar's computer network that contained a number of files, including some containing personal health information.
"We have not been able to confirm that those files were actually accessed by the third party, and therefore cannot say that any personal information in those files was accessed," the statement says.
(continua…..)
https://www.govinfosecurity.com/texas-county-ems-agency-says-ransomware-breach-hit-612000-a-20876
GOVINFOSECURITY *- Marianne Kolbasuk McGee- January 6, 2023*

Impiegato riceve un sollecito per una fattura scaduta ma è un virus: violata privacy dei lavoratori e maxi-sanzione per l'azienda
Deve essere riuscito a farsi odiare sia dall'azienda che dai suoi oltre centomila colleghi quell'ingenuo impiegato che di recente ha abboccato alla classica mail di phishing inviata da un sedicente fornitore che sollecitava il pagamento di una fattura scaduta con tanto di file allegato, che però non conteneva alcun documento amministrativo, bensì un ransomware in grado di crittografare tutti i dati presenti nei server aziendali, compresi appunto quelli del personale.
(*continua*)
https://www.federprivacy.org/informazione/societa/impiegato-riceve-un-sollecito-per-una-fattura-scaduta-ma-e-un-virus-violata-privacy-dei-lavoratori-e-maxi-sanzione-per-l-azienda
Federprivacy *- Nicola Bernardi – 07/12/2022*

Rompere l'algoritmo crittografico RSA con un computer quantistico: facciamo chiarezza
La pubblicazione di un documento in cui un gruppo di ricercatori cinesi afferma di poter violare l'algoritmo crittografico RSA a 2048 bit (sebbene non lo abbia ancora fatto) non ha colto di sorpresa gli addetti ai lavori.
Non è una novità, infatti, che il quantum computing possa diventare un problema di sicurezza: già da tempo gli esperti si interrogano sulle sfide che ci attendono nei prossimi anni per far sì che lo sviluppo di questa tecnologia non avvantaggi in qualche modo il cyber crimine nel mettere fuori gioco gli attuali algoritmi crittografici usati per garantire la sicurezza delle informazioni.
In questo contesto, ad esempio, il NIST (il National Institute of Standards and Technology degli Stati Uniti) lo scorso 5 luglio 2022 ha comunicato di aver selezionato i primi quattro algoritmi crittografici in grado di resistere alla computazione quantistica. Facciamo, dunque, chiarezza sull'argomento perché,

come ha affermato il noto crittografo Bruce Schneier, l'annuncio dei ricercatori cinesi è da "prendere sul serio: potrebbe non essere corretto, ma non è ovviamente sbagliato".

Indice degli argomenti

Cos'è l'algoritmo crittografico RSA

L'algoritmo RSA deve il suo nome a tre matematici americani, R. Rivest, L. Adleman e A. Shamir, che per primi inventarono una funzione matematica per realizzare nella pratica un sistema di crittografia asimmetrica, ovvero basato sui concetti di chiave pubblica e privata.

Il lavoro dei tre matematici prese spunto dall'articolo originale sulla crittografia asimmetrica di Diffie e Hellman del 1976 (continua….)

https://www.cybersecurity360.it/nuove-minacce/rompere-lalgoritmo-crittografico-rsa-con-un-computer-quantistico-facciamo-chiarezza/

***CYBERSECURITY360**- Andrea Razzini- 10 Gen 2023*

ChatGpt usato dai cybercriminali: per scrivere malware e phishing

Criminali cominciano a usare il bot Chatgpt di OpenAi, per aiutarsi nella scrittura del codice. Ma lo si può adoperare anche per compilare mail di phishing. Checkpoint analizza il fenomeno. Siamo solo agli inizi di una nuova minaccia da studiare attentamente

Non sai come scrivere un codice di un **ransomware** ma ti vuoi gettare anche tu in questo fantastico business? Niente paura: ora puoi usare Chatgpt.

Vorresti scrivere anche una mail **phishing** ma soffri della crisi da foglio bianco? Di nuovo, il bot Chatgpt di OpenAi è il tuo migliore alleato.

Se esistesse un Aranzulla dei cybercriminali probabilmente scriverebbe così. Il pericolo esiste davvero, però: i cybercriminali stanno cominciando a usare Chagpt scrive Checkpoint.

Indice degli argomenti

Come usano Chatgpt i cybercriminali

Su un popolare forum di hacking clandestino è apparsa una discussione denominata "ChatGPT – Benefits of Malware". "L'autore del thread ha rivelato che stava sperimentando ChatGPT per ricreare ceppi di malware e tecniche descritte in pubblicazioni di ricerca e scritti su malware comuni. Ad esempio, ha condiviso il **codice** di uno stealer basato su Python che cerca tipi di file comuni, li copia in una cartella casuale all'interno della cartella Temp, li comprime e li carica su un server FTP codificato", scrive Checkpoint.

Scrittura malware, marketplace

Checkpoint ha analizzato lo script e conferma le affermazioni del criminale informatico. "Si tratta effettivamente di uno stealer di base che cerca 12 tipi di file comuni (come documenti MS Office, PDF e immagini) nel sistema. Se vengono trovati file di interesse, il malware copia i file in una directory temporanea, li zippa e li invia sul web. Vale la pena notare che l'attore non si è preoccupato di crittografare o inviare i file in modo sicuro, quindi i file potrebbero finire nelle mani di terze parti", scrive Checkpoint. (continua…)

https://www.cybersecurity360.it/nuove-minacce/chatgpt-usato-dai-cybercriminali-per-scrivere-malware-e-phishing/
Cybersecurity360 *- Alessandro Longo - 10 Gen 2023*

San Fran's BART Investigates Vice Society Data Breach Claims
Vice Society is boasting that it compromised the San Francisco transportation system, while BART maintains operations and mounts an investigation.
The San Francisco Bay Area Rapid Transit System (BART) was listed this week by ransomware group Vice Society as being among its latest victims.
Brett Callow, threat analyst with Emsisoft, flagged the Vice Society BART brag on Jan. 6. However, BART's spokesperson Alicia Trost told Dark Reading there haven't been any service disruptions as a result of a cyberattack and that an investigation is ongoing.
"We are investigating the data that has been posted," Trost told Dark Reading by email. "To be clear, no BART services or internal business systems have been impacted. As with other government agencies, we are taking all necessary precautions to respond."
Vice Society was also behind a recent spate of school breaches in the US and beyond, most recently releasing the personal information stolen from a group of 14 schools in the UK.
https://www.darkreading.com/ics-ot/san-fran-bart-investigates-vice-society-data-breach
Dark Reading -*Dark Reading Staff- January 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.

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

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

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 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.