

BOLETIM IAR

Inteligência Aberta de Rádio

Boletim de Escuta Semanal

Panorama de notícias militares, de inteligência, terrorismo e cibercrime, resultante da escuta de programas de rádio ao redor do mundo. Este Boletim é enviado com exclusividade aos assinantes do Velho General.

Destaques desta edição:

EUA supostamente usando spyware israelense Pegasus para monitorar telefones no México (Pág. 2)

Documentos militares secretos dos EUA divulgados em redes sociais (Pág. 3)

Nas Filipinas, quatro novas bases militares disponíveis para uso dos militares dos EUA (Pág. 4)

Aumento na produção de munição sul-coreana elogiado pelo secretário-geral da OTAN (Pág. 6)

Finlândia deve comprar sistema de defesa aérea israelense (Pág. 6)

Mais de 100 prisões após operação policial contra maior plataforma hacker do mundo (Pág. 7)

REDAÇÃO DOS ARTIGOS

Os textos são registros de escuta de rádio; o texto é, portanto, o da mídia citada, apenas com ajustes da tradução para o português. Os títulos, por outro lado, são nossos.

Pyongyang anuncia novo teste de drone subaquático c/ capacidade nuclear

A Coreia do Norte afirma ter realizado novo teste de drone de ataque subaquático com capacidade nuclear esta semana. A edição de sábado do jornal governista do Partido dos Trabalhadores disse que um instituto de pesquisa científica de defesa nacional conduziu o teste por quatro dias até sexta-feira. A reportagem disse que o drone submersível Haeil-2 entrou na área de teste na província oriental de South Hamgyong na terça-feira. Ele disse que o drone passou cerca de 71 horas viajando uma distância virtual de 1.000 km antes de atingir um alvo simulado e detonar com precisão uma ogiva de teste. Esta é a segunda vez que a Coreia do Norte anuncia um teste de sua nova arma, chamada Haeil, que significa tsunami em coreano. O país disse que testou o drone pela primeira vez no mês passado e afirmou que poderia desencadear um tsunami radioativo capaz de destruir navios e portos inimigos.

(Rádio Japão Internacional, 08-04-2023)

CIA teria ficado surpresa com restabelecimento das relações diplomáticas entre Irã e Arábia Saudita

O diretor da CIA, William Burns, expressou frustração com a decisão de Riad de restaurar laços com Teerã e Damasco, já que observadores apontam o declínio da influência dos EUA no Oriente Médio. De acordo com o *Wall Street Journal*, Burns fez uma visita não anunciada a Riad esta semana para conversar sobre cooperação de inteligência com autoridades sauditas. Em reunião com o príncipe herdeiro saudita Mohammad bin Salman, ele reclamou que Washington se sentiu pego de surpresa pelos movimentos de Riad para restaurar os laços com Irã e Síria, ambos sob sanções ocidentais. Ele expressou a frustração dos EUA por ter sido deixado de fora dos acontecimentos na região.

Primeiro helicóptero Viper AH-1Z prestes a ser entregue aos tchecos

Produzido nos EUA, o primeiro helicóptero de combate Viper AH-1Z deve ser entregue em breve ao exército tcheco. O helicóptero deve ser primeiro transferido pelo fabricante ao governo dos EUA e depois ao exército tcheco. Os primeiros devem chegar à República Tcheca até maio, disse o Ministério da Defesa. No total, o país está comprando oito helicópteros Venom UH-1Y e quatro AH-1Z dos EUA. Os militares tchecos também receberão mais seis Viper mais velhos e dois Venom americanos em troca de ajuda à Ucrânia. Devem substituir o Mi-24V/35 soviético usado até agora.

(Rádio Internacional de Praga, 03-04-2023)

... TERRORISMO ...

Blogueiro pró-Putin morto em ataque a bomba em um café em São Petersburgo

"Hoje, um dispositivo de natureza desconhecida explodiu em um café no centro de São Petersburgo", anunciou em comunicado o Comitê de Investigação da Rússia, responsável pelas principais investigações no país. "Uma pessoa morreu e 25 ficaram feridas, 19 das quais estão hospitalizadas", disse o governador de São Petersburgo, Alexander Beglov, no Telegram. Segundo os investigadores, que abriram uma investigação criminal por "assassinato por meios perigosos", a vítima é o blogueiro militar conhecido pelo pseudônimo de Vladlen Tatarski. Os arredores do edifício foram isolados com cerca de 20 carros da polícia, seis ambulâncias e carros de bombeiros, notou um jornalista da AFP. Provavelmente uma garota trouxe o engenho explosivo, segundo fonte citada pela agência noticiosa *Ria Novosti*. "Havia uma estatueta na caixa: um presente destinado ao Sr. Tatarski", acrescentou esta fonte. "Ela a deu a ele e depois, de repente, houve uma explosão", disse à AFP Alissa Smotrova, uma mulher presente. Outra fonte, também citada pela *Ria Novosti*, precisou que a pessoa em causa era conhecida do blogueiro e que se tinham cruzado em eventos, sem dar mais detalhes. De acordo com o Ministério do Interior da Rússia, às 18h13 (15h13 GMT), a polícia do distrito de Vasileostrovsky recebeu relatos de que uma explosão ocorreu em um café no aterro Universitetskaya no número 25. A explosão ocorreu no Café Street Food Bar No. 1 localizado ao longo do Neva, não muito longe do centro histórico de São Petersburgo. "Todas as medidas necessárias estão sendo tomadas para identificar os envolvidos", acrescentou o Comitê Investigativo Russo.

(A voz da Turquia, 03-04-2023)

Líder do Estado Islâmico é morto em ataque dos EUA na Síria

Khaled Aydd Ahmad Al-Jabouri, líder do grupo jihadista Estado Islâmico responsável por ataques na Europa, foi morto em ataque dos EUA na Síria na terça-feira, anunciou o CENTCOM, o comando militar dos EUA para o Oriente Médio enfatizando que sua morte interromperia temporariamente a capacidade da organização de encenar ataques no exterior.

(Voz da América, 04-04-2023)

Pelo menos 30 mortos após novos ataques das ADF no nordeste da República Democrática do Congo

Novos ataques do ADF ceifaram mais de 30 vidas na RDC, de acordo com a ONU. Esses assassinatos ocorreram em Ituri, no nordeste do país, nos dias 2 e 3 de abril. As ADF são rebeldes filiados ao grupo Estado Islâmico, que os apresenta como seu ramo na África central.

(Rádio Vaticano, 07-04-2023)

... ATIVIDADES DOS SERVIÇOS DE INTELIGÊNCIA ...

EUA supostamente usando spyware israelense Pegasus para monitorar telefones no México

Washington teria celebrado um contrato secreto com a empresa israelense NSO Group poucos dias depois de anunciar o estabelecimento de medidas retaliatórias contra ela, segundo uma investigação publicada segunda-feira no *New York Times*. Como parte do acordo, o NSO Group supostamente deu ao governo dos EUA acesso ao seu software Pegasus, uma ferramenta de rastreamento geográfico capaz de rastrear secretamente telefones celulares sem o conhecimento de seus usuários. Segundo o jornal americano, o contrato foi finalizado em 8 de novembro de 2021 por meio de uma empresa de fachada que servia de fachada para o governo dos EUA e a subsidiária americana de uma notória empresa de hackers israelenses. Um encobrimento que decorre do fato de que cinco dias antes o governo Biden havia anunciado uma ação contra a NSO, cujas ferramentas de hacking são usadas há anos por governos de todo o mundo para espionar dissidentes políticos, ativistas de direitos humanos e jornalistas. Em 3 de novembro, a Casa Branca colocou a NSO em uma lista negra do Departamento de Comércio, declarando a empresa israelense uma ameaça à segurança nacional e instando as empresas americanas a pararem de fazer negócios com ela. O contrato secreto, que viola a política pública do governo Biden, parece estar ativo. De acordo com o *New York Times*, que pôde revisar o acordo, ele permitiu especificamente que o governo testasse, avaliasse e até implantasse o spyware contra alvos de sua escolha

no México. Quando questionados sobre este contrato, os funcionários da Casa Branca disseram que não tinham ouvido falar dele. "Não temos conhecimento deste contrato e qualquer uso deste produto seria motivo de grande preocupação", disse um alto funcionário do governo Biden sob condição de anonimato.

(I24News, 03-04-2023)

Vários documentos militares secretos dos EUA divulgados nas redes sociais

A Rússia ou elementos pró-Rússia provavelmente estão por trás do vazamento de vários documentos militares americanos classificados há um mês sobre a guerra na Ucrânia, datados de um mês, publicados nas mídias sociais na sexta-feira, disseram três autoridades dos EUA à *Reuters*, enquanto o Departamento de Justiça disse que estava investigando o vazamento. Os documentos parecem ter sido alterados para reduzir o número de baixas sofridas pelas forças russas, disseram autoridades americanas, acrescentando que suas avaliações foram informais e separadas da investigação sobre o vazamento em si. Autoridades dos EUA falaram sob condição de anonimato devido à sensibilidade do assunto e se recusaram a discutir os documentos em detalhes. Um primeiro lote de documentos, datado de 1º de março e marcado como "Secreto" e "Top Secret" circulou no *Twitter* e no *Telegram* na sexta-feira, antes de um novo lote de documentos aparecer para detalhar os segredos de segurança nacional americanos relativos, em particular, à Ucrânia, Oriente Médio e a China, apareceu nas mídias sociais, informou o *New York Times*. O Departamento de Justiça dos EUA disse que está em contato com o Departamento de Defesa e abriu uma investigação sobre o vazamento e se recusou a comentar mais. "Estamos cientes dos relatos de postagens nas redes sociais e o Departamento de Defesa está analisando o assunto", disse a porta-voz do Pentágono, Sabrina Singh. Um dos documentos vazados indica que entre 16.000 e 17.500 membros das forças russas foram mortos desde que a Rússia invadiu a Ucrânia em 24 de fevereiro de 2022, o que está muito longe das estimativas oficiais dos EUA, que contavam cerca de 200.000 russos mortos e feridos. Em Kiev, uma autoridade presidencial ucraniana disse que o vazamento continha uma grande quantidade de informações falsas e parecia uma operação de desinformação russa com o objetivo de lançar dúvidas sobre a contraofensiva planejada pela Ucrânia.

(I24News, 08-04-2023)

... MILITAR ...

Nova intrusão de navios chineses em águas territoriais japonesas

A Guarda Costeira Japonesa diz que navios do governo chinês entraram em águas territoriais japonesas perto das Ilhas Senkaku, no Mar da China Oriental. Eles ficaram lá por 80 horas e 36 min. É a mais longa intrusão de tais embarcações em águas territoriais japonesas desde que o governo japonês comprou algumas das ilhas de um proprietário privado japonês em 2012. A guarda costeira diz que quatro embarcações do governo chinês entraram em águas próximas às ilhas de Minamikojima e Uotsurijima logo depois das 11h00 de quinta-feira. Elas pareciam estar seguindo três barcos de pesca japoneses. Segundo a guarda costeira, uma das embarcações chinesas deixou a área na noite de sábado, depois que um dos barcos de pesca fez o mesmo. Eles acrescentam que os outros navios chineses também deixaram a área às 19h44 de domingo. A guarda costeira permanece em alerta máximo e avisa os navios chineses para não reentrar em suas águas territoriais. O Japão controla as ilhas e China e Taiwan as reivindicam. O governo japonês sustenta que não há questão de soberania.

(Rádio Japão Internacional, 03-04-2023)

Detecção de forte atividade dentro da instalação nuclear norte-coreana de Yongbyon

Ao norte do paralelo 38, foi detectado alto nível de atividade no site nuclear de Yongbyon. A *38 North* fez o anúncio no último sábado, com base em imagens de satélite obtidas em 3 e 17 de março. Segundo o site americano especializado em arquivos norte-coreanos, um reator experimental de água leve (ELWR) parece estar em fase de conclusão e prestes a entrar em operação. Com fotos públicas que revelam a ativação do reator e a construção de um novo prédio que começou nas proximidades, ele também afirmou que foram observadas descargas de água no sistema de resfriamento do ELWR. Também indicou que foram iniciadas novas obras que provavelmente ampliarão as capacidades

da usina de enriquecimento de urânio. Ainda segundo o *38 North*, estes movimentos parecem seguir ordens do líder Kim Jong-un, que sublinhou, em 27 de março passado, a importância de aumentar a produção de materiais nucleares para o desenvolvimento do arsenal do país.

(KBS World Radio, 03-04-2023)

Pyongyang continuaria a produzir material nuclear militar

A Coreia do Norte ainda não se atreve a realizar um novo teste atômico, mas parece continuar produzindo material nuclear militar. Trata-se de uma análise do comitê de monitoramento da ONU sobre as sanções impostas ao país comunista. Ele compartilhou isso em novo relatório publicado por seu painel de especialistas. Ele especifica que em 2022, o regime de Kim Jong-un lançou seus mísseis balísticos um total de 73 vezes, incluindo oito ICBMs. Esses especialistas também se referem ao fato de que o Norte testou um motor de foguete de alto impulso com o objetivo de desenvolver um novo ICBM de combustível sólido e que ameaçou um ataque nuclear preventivo. Sobre o principal financiamento do desenvolvimento de armas atômicas, o documento o vincula ao roubo de criptomoedas. Especificamente, no ano passado, grupos de hackers associados ao regime comunista roubaram cerca de um trilhão de won, ou quase 700 milhões de euros, um recorde. Ainda de acordo com o painel de especialistas, Pyongyang continua a contornar as sanções da ONU por via marítima. Na verdade, importa ilegalmente produtos petrolíferos refinados ou carvão a bordo de navios. Vale ressaltar que o relatório foca principalmente nas violações ocorridas no segundo semestre do ano passado, a maioria já conhecida.

(KBS World Radio, 06-04-2023)

Exercícios militares conjuntos das marinhas dos EUA, Japão e Coreia do Sul

Coreia do Sul, EUA e Japão iniciaram seu exercício marítimo conjunto em águas internacionais ao sul da ilha de Jeju, no sul, nesta manhã por dois dias. De acordo com o Ministério da Defesa sul-coreano, participará o porta-aviões americano de propulsão nuclear USS *Nimitz*, que chegou à base naval de Busan. Para a Marinha da Coreia do Sul, destróieres, como *Yulgok Yi*, *Choe Yeong* e *Daejoyeong*, foram implantados. O treinamento se concentrará na guerra antissubmarina hoje e na busca e resgate de acidentes no mar amanhã. Esta manobra surge apenas seis meses depois da última, sugerindo que os três parceiros têm partilhado a ideia de que a provocação norte-coreana atingiu um nível alarmante. O ministério sul-coreano disse que pretende aumentar a capacidade de resposta das três nações contra as crescentes ameaças do regime de Kim Jong-un relacionadas a mísseis balísticos estratégicos mar-superfície (MSBS). Ao longo deste evento, Seul, Washington e Tóquio estarão atentos às atividades dos países vizinhos, especialmente porque um navio de coleta de inteligência chinês foi detectado no mar próximo, durante o exercício realizado no outono passado. Diante dessa mobilização, é muito provável que Pyongyang protagonize uma nova bravata. A *KCNA*, a agência noticiosa norte-coreana, já ontem criticou este treino marítimo, dizendo que se as três nações realizarem tal atividade hostil, o regime norte-coreano fará uma escolha correspondente. O cenário mais plausível é que a Coreia do Norte lance um míssil de longo alcance a pretexto de testar um satélite artificial. Depois de lançar dois mísseis balísticos de alcance intermediário em 18 de dezembro de 2022, disse que concluirá os preparativos para seu primeiro satélite de reconhecimento militar este mês.

(KBS World Radio, 03-04-2023)

Nas Filipinas, quatro novas bases militares podem ser utilizadas pelo exército americano

A guerra de influência entre os EUA e a China é parcialmente travada no arquipélago filipino. Manila anunciou ontem a localização de quatro novas bases militares que podem ser usadas pelos EUA: uma muito perto do disputado Mar da China Meridional e outra não muito longe de Taiwan. Os quatro locais foram cuidadosamente selecionados e podem ser usados para o posicionamento de tropas americanas na região. No início de fevereiro, os dois países anunciaram um acordo para permitir que soldados americanos acessem bases adicionais localizadas no arquipélago. Washington e Manila são aliados de segurança há várias décadas, notadamente ligados por um tratado de defesa e um acordo de cooperação reforçada assinado em 2014, que permite que soldados americanos acessem bases filipinas, mas também armazenem ali materiais e equipamentos militares. No total, os EUA poderiam ocupar dez bases nas Filipinas, incluindo a base naval de Santa Ana, localizada

a apenas 400 km de Taiwan. O novo governo filipino de Ferdinand Marcos Junior deseja fortalecer sua parceria com Washington, impulsionado pelas reivindicações de Pequim em relação a Taiwan e a construção de bases chinesas no Mar da China Meridional.

(Rádio Vaticano, 04-04-2023)

Um porta-aviões chinês teria sido implantado no Oceano Pacífico

O Ministério da Defesa do Japão disse ter confirmado na quarta-feira a presença de três navios de guerra chineses, incluindo o porta-aviões *Shandong*, no Oceano Pacífico ao sul da província de Okinawa. O primeiro porta-aviões construído na China foi implantado em dezembro de 2019. Esta é a primeira vez que o navio foi avistado no Oceano Pacífico. Na quinta-feira, o ministério disse que as Forças de Autodefesa Marítimas avistaram o *Shandong*, uma fragata e outro navio na noite de quarta-feira enquanto se dirigiam para o leste em águas cerca de 300 km ao sul da ilha de Hateruma. Uma foto divulgada pelo ministério mostra vários caças e helicópteros estacionados no convés do *Shandong*. Na quarta-feira, o Ministério da Defesa taiwanês acrescentou que o mesmo porta-aviões cruzou o Canal Bashi, localizado entre Taiwan e as Filipinas. Atualmente, dois porta-aviões são operados pela Marinha Chinesa: *Shandong* e *Liaoning*. O *Liaoning* realizou exercícios de decolagem e pouso no Oceano Pacífico em dezembro e janeiro passados. Para funcionários do Ministério da Defesa do Japão, a China está buscando melhorar as capacidades operacionais de seus porta-aviões. O *Shandong* foi visto antes da reunião da presidente taiwanesa, Tsai Ing-wen, com o presidente da Câmara dos Representantes dos EUA, Kevin McCarthy. O ministério japonês disse que estará em alerta máximo e monitorará de perto a situação.

(Rádio Japão Internacional, 06-04-2023)

Exercícios militares chineses em torno de Taiwan

A China iniciou três dias de patrulhas de prontidão de combate e exercícios militares em torno de Taiwan no sábado. Os militares chineses disseram que a principal prioridade é testar sua capacidade de controlar rotas marítimas e aéreas. De acordo com o Comando de Teatro Oriental do Exército de Libertação do Povo, os exercícios estão ocorrendo no Estreito de Taiwan e áreas no norte, sul e leste da ilha. Os exercícios são vistos como resposta à recente reunião entre a presidente de Taiwan, Tsai Ing-wen, e o presidente da Câmara dos Representantes dos EUA, Kevin McCarthy. O comando disse que o exército, a marinha e a força aérea, entre outros, se mobilizaram rapidamente para as áreas de exercício designadas após receberem ordens para fazê-lo. Ele disse que os exercícios de sábado visam testar a capacidade dos militares de assumir o controle das rotas aéreas e marítimas. O comando acrescentou que outro objetivo era testar a capacidade do exército de posicionar tropas para cercar e cercar Taiwan. Separadamente, o Ministério da Defesa de Taiwan disse que avistou 71 aeronaves militares chinesas, incluindo caças, em torno de Taiwan entre 07h00 e 17h00 de sábado, horário local. Ele disse que 45 deles cruzaram a linha do meio do estreito ou entraram na Zona de Identificação de Defesa Aérea do Sudoeste de Taiwan.

(Rádio Japão Internacional, 09-04-2023)

... NOTÍCIAS DO MERCADO DE ARMAS ...

A República Tcheca ainda seria capaz de fornecer equipamento militar à Ucrânia

A República Tcheca ainda possui reservas de equipamento militar que poderia enviar à Ucrânia para ajudá-la na luta contra a Rússia. Isso foi afirmado pela ministra da Defesa, Jana Cernochova, na televisão tcheca no domingo. Nos próximos dias, Cernochova e o chefe do Estado-Maior do Exército, Karel Rehka, se encontrarão com o presidente da República, Petr Pavel, que disse na semana passada que a República Tcheca não tem mais muitas opções para apoiar a Ucrânia em armamentos. O Ministro pretende fornecer ao Chefe de Estado uma lista de equipamentos que poderão ser disponibilizados à Ucrânia. Jana Cernochova esclareceu que, juntamente com Karel Rehka, foi estabelecido um cronograma e uma lista da ajuda que ainda pode ser prestada a Kiev. "Ainda há coisas em nossos armazéns que garantimos que nunca serão usadas pelo nosso exército e que hipoteticamente podemos enviar para a Ucrânia se eles estiverem interessados", disse ela.

(Rádio Internacional de Praga, 03-04-2023)

Aumento na produção de munição sul-coreana elogiado pelo secretário-geral da OTAN

O Secretário-Geral da Organização do Tratado do Atlântico Norte (OTAN) acolheu calorosamente o aumento da produção de munições da Coreia do Sul. Também elogiou esse suprimento militar sul-coreano indireto para a Ucrânia. O anúncio foi feito ontem por Jens Stoltenberg durante conferência de imprensa no final da reunião ministerial da Aliança Atlântica realizada em Bruxelas com quatro países parceiros da Ásia-Pacífico, nomeadamente Coreia do Sul, Austrália, Nova Zelândia e Japão. Questionado se o possível fornecimento de armas de Seul para Kiev foi discutido, o secretário-geral respondeu que a Terra da Luz da Manhã, grande produtor de munição, estava intensificando a fabricação, o que preencheria estoques dos países membros da OTAN. No entanto, Stoltenberg disse que não poderia detalhar a forma de abastecimento e o destinatário da munição sul-coreana, antes de destacar que a Ucrânia será o país mais ajudado de forma regular por meio do arsenal à disposição da organização internacional. Por sua vez, um membro da delegação sul-coreana também confirmou que nenhum apoio militar direto da Coreia do Sul foi mencionado durante a reunião. Após os comentários favoráveis da OTAN, depois dos EUA, sobre o aumento da produção de munição sul-coreana, os observadores contam com a possível demanda explosiva desses produtos fabricados na Coreia.

(KBS World Radio, 06-04-2023)

A Finlândia deve comprar o sistema de defesa aérea israelense David's Sling

O Ministério da Defesa da Finlândia anunciou na quarta-feira que seu país comprará o sistema de defesa aérea David's Sling de Israel por 316 milhões de euros. Em comunicado, o ministério disse que o sistema melhorará significativamente as capacidades de defesa da Finlândia e permitirá que as forças interceptem alvos a grande altitude. "Ao mesmo tempo, estamos buscando o desenvolvimento ambicioso e de longo prazo da capacidade de defesa da Finlândia em um novo ambiente de segurança", disse o ministro da Defesa, Antti Kaikkonen. O sistema David's Sling, fabricado pela israelense Rafael Advanced Defense Systems, é capaz de interceptar foguetes e mísseis à distância de 40 a 300 km. A declaração disse que a altitude mínima de voo exigida pela Finlândia para o sistema foi fixada em 15.000 metros. O ministério da defesa do país disse ainda que o acordo prevê ainda a possibilidade de compras adicionais no valor de 216 milhões de euros. O anúncio ocorre um dia depois que Helsinque ingressou na aliança militar da OTAN, que desferiu um golpe no presidente russo, Vladimir Putin. A Finlândia adotou neutralidade após sua derrota para os soviéticos na Segunda Guerra Mundial, mas seus líderes expressaram o desejo de ingressar na OTAN depois que a Rússia invadiu a Ucrânia. "A era do não-alinhamento em nossa história chegou ao fim, uma nova era está começando", disse o presidente Sauli Niinistö antes que a bandeira azul e branca de seu país fosse hasteada do lado de fora da sede da OTAN.

(I24News, 06-04-2023)

... CIBERESPAÇO ...

Onda de ciberataques contra Israel reivindicada pelo Anonymous Sudan

Os sites de várias das principais universidades israelenses foram atacados na terça-feira por um grupo de hackers autodenominado Anonymous Sudan. Os sites da Universidade de Tel Aviv, Universidade Hebraica de Jerusalém, Universidade Ben-Gurion do Negev, Universidade de Haifa, Instituto Weizmann de Ciências, Universidade Aberta de Israel e Universidade Reichman estavam entre os sites inacessíveis. O grupo postou comunicado no Telegram, listando os sites atacados. "Infraestrutura: Universidades – o setor educacional israelense foi abandonado pelo que fizeram na Palestina", dizia. O grupo também acrescentou que este não foi o ataque principal, que acontecerá em 7 de abril. A empresa de segurança cibernética Radware disse que ataques cibernéticos em larga escala contra Israel ocorreram todos os anos nessa data na última década. Na terça-feira, a empresa também identificou ataques contra sites de hospitais, jornais e até refinarias. Em fevereiro passado, o site do Technion foi hackeado, informações foram roubadas e os hackers exigiram resgate de vários milhões de shekels. Na sequência, sistemas informáticos do instituto foram desligados e a data de vários exames adiada. O National Cyber Array disse que o Irã estava por trás do ataque cibernético.

(I24News, 04-04-2023)

O grupo de hackers Anonymous Sudan atacou na manhã de quarta-feira os sites de vários meios de comunicação israelenses, incluindo o do *I24NEWS*, por quase duas horas. Os outros meios de comunicação atacados foram *Kan*, *Jerusalem Post* e *Channel 12*. Este ataque cibernético ocorre um dia depois de um hack que teve como alvo várias universidades do país, incluindo Tel Aviv, Jerusalém, Beer Sheva, Haifa, instituto Weizmann, Israel Open University e Universidade Reichman (IDC). O Anonymous Sudan também conseguiu hackear a empresa israelense de segurança cibernética Checkpoint, bem como a organização United Hatzalah. Os ataques fazem parte da Operação anual OPIsrael, uma operação de hackers pró-palestinos que visa instituições israelenses por uma semana para punir o Estado judeu por suas ações na Cisjordânia. O grupo deu a entender que esses ataques continuariam na sexta-feira sem dar detalhes.

(I24News, 05-04-2023)

Mais de cem prisões após operação policial contra a maior plataforma hacker do mundo

Chama-se Genesis Market e é a maior plataforma hacker do mundo. Esta plataforma vendeu os dados e identificadores de milhões de pessoas na internet. Mais de cem pessoas foram presas, 200 propriedades foram revistadas. Investigadores de mais de vinte países estiveram envolvidos nesta operação. As ações ocorreram principalmente na Austrália, Canadá, EUA e uma dezena de países europeus.

(Deutsche Welle, 05-04-2023)

A polícia europeia anunciou na quarta-feira o fechamento de uma das maiores plataformas de hackers do mundo, que vendia credenciais de contas roubadas, inclusive no Canadá. Uma operação policial sem precedentes envolvendo 17 países levou ao desmantelamento do Genesis Market, um dos mercados mais perigosos do mundo, informou a agência Europol em comunicado. Ações coordenadas também foram tomadas em todo o mundo contra os usuários desta plataforma. Eles levaram a 119 prisões e 208 buscas, quatro das quais ocorreram no Canadá. Essa repressão internacional foi liderada pelo FBI nos EUA, Politie na Holanda e Europol, que coordenou o trabalho dos agentes envolvidos em todo o mundo. No Canadá, o Serviço de Investigação de Crimes Cibernéticos da Sûreté du Québec (SQ) trabalhou nisso em colaboração com o FBI, a Comissão Canadense de Radiotelevisão e Telecomunicações (CRTC) e a Real Polícia Montada do Canadá (RCMP). Um total de 28 departamentos de polícia de costa a costa estiveram envolvidos neste dia de ação global sequencial, disse a RCMP. A investigação teve repercussão em Quebec, onde seis pessoas foram presas na terça-feira em conexão com este caso de repercussão internacional. Os suspeitos, quatro homens e duas mulheres com idades entre 21 e 37 anos, podem ser acusados, entre outras coisas, de uso não autorizado de um computador e posse de dispositivo que permite o uso não autorizado de um computador. As buscas resultaram na apreensão de equipamentos de informática e equipamentos utilizados na produção de documentos falsos. Nesta operação, o SQ se encarregou da pesquisa direcionada aos usuários mais ativos do Genesis Market em Quebec. A força policial provincial coordenou com 11 serviços policiais de Quebec, bem como a reunião de aproximadamente 59 assuntos de interesse, todos usuários do Genesis Market, explicou em comunicado à imprensa. A maioria dos suspeitos identificados no Canadá durante a operação vive em Quebec. A principal *commodity* do Genesis Market eram as identidades digitais. Este mercado vendia bots (robôs) que já haviam infectado os dispositivos das vítimas por meio de malware ou ataques de aquisição de contas, informou a agência em comunicado. O Genesis Market tinha 1,5 milhão de robôs em sua posse no momento da ação internacional concertada. Ao comprar um bot, os criminosos tinham acesso a todos os dados coletados por ele, como impressões digitais, *cookies*, *logins* salvos e informações de preenchimento automático (formulários eletrônicos, por exemplo). Essas informações eram coletadas em tempo real, ou seja, os compradores eram avisados sobre qualquer alteração de senha, por exemplo.

(Rádio Canadá internacional, 06-04-2023)

Aumento dramático nos roubos de criptomoedas por supostos hackers norte-coreanos

Um relatório das Nações Unidas indica que, em 2022, a Coreia do Norte roubou mais ativos de criptomoeda do que em qualquer outro ano, usando técnicas cada vez mais avançadas. A ONU recomenda uma sanção contra o chefe da agência norte-coreana responsável. O Conselho de Segurança da ONU, que estabelece sanções contra Pyongyang, divulgou um relatório na quarta-feira cobrindo o período do final de julho ao final de janeiro. De acordo com o documento, uma empresa de segurança cibernética estimou que o cibercrime norte-coreano acumulou

criptomoedas no valor de mais de US\$ 1 bilhão em 2022. Os criptoativos roubados pela Coreia do Norte seriam usados para financiar seus programas nuclear e de mísseis. O relatório acrescenta que o país tem utilizado técnicas cibernéticas cada vez mais sofisticadas, dificultando o rastreamento da origem dos ativos. Os autores do relatório dizem que os hackers responsáveis pela maioria dos ataques são membros do Bureau Geral de Reconhecimento. A comissão recomenda adicionar o chefe do escritório, general Ri Chang Ho, à lista de indivíduos alvo de sanções. Exorta novamente os Estados-Membros a reforçarem as suas medidas de segurança.

(Rádio Japão Internacional, 06-04-2023)

Pyongyang diversificaria seus meios para roubar criptomoedas

A Coreia do Norte parece estar diversificando as formas de roubar criptomoedas para financiar seu programa de armas de destruição em massa. Foi revelado desta vez que também usa finanças descentralizadas, abreviadas como DeFi. Em seu primeiro relatório sobre a avaliação global de risco de finanças ilícitas DeFi, publicado ontem, o Tesouro dos EUA estima que hackers norte-coreanos estão transferindo e lavando dinheiro roubado usando este sistema desenvolvido na esteira do mercado de criptoativos, graças às funcionalidades do blockchain. Segundo o departamento dos EUA, o regime de Kim Jong-un, sob sanções dos EUA e da ONU, está aumentando a captação ilegal de recursos usando o sistema em questão e a VASP, uma provedora de serviços de ativos virtuais. O notório Lazarus Group, apoiado pelo Norte, por exemplo, apreendeu ativos digitais no valor total de US\$ 720 milhões, atacando o videogame online Axie Infinity em 2022 e a empresa de criptomoedas Harmony em 2020. Também de acordo com o Tesouro dos EUA, hackers ligados ao reino eremita estão também envolvidos nos ataques de ransomware. E muitos milhares de trabalhadores de TI norte-coreanos em todo o mundo também estão por trás das atividades cibernéticas ilícitas.

(KBS World Radio, 07-04-2023)

*O **Boletim de Escuta Semanal - Inteligência Aberta no Rádio** traz um panorama de notícias militares, de inteligência, terrorismo e cibercrime, resultante da escuta de programas de rádio ao redor do mundo. Trata-se de um informe e não de uma análise: é o registro de escuta das rádios e a redação é, portanto, a da mídia citada.*

Este monitoramento regular é um excelente barômetro da evolução da situação política internacional e oferece notícias que de outro modo poderiam passar despercebidas.

O boletim é produzido por Alain Charret, ex-oficial da força aérea francesa que serviu em vários centros de escuta na França, especialmente na Alemanha antes da queda da URSS, e é traduzido para português pelo Velho General.



velhogeneral.com.br

[Assine o Velho General](http://velhogeneral.com.br)