Cyber Segurança

Projeto Sementes de Futuro em Defesa

Vol. 2 Nº 16

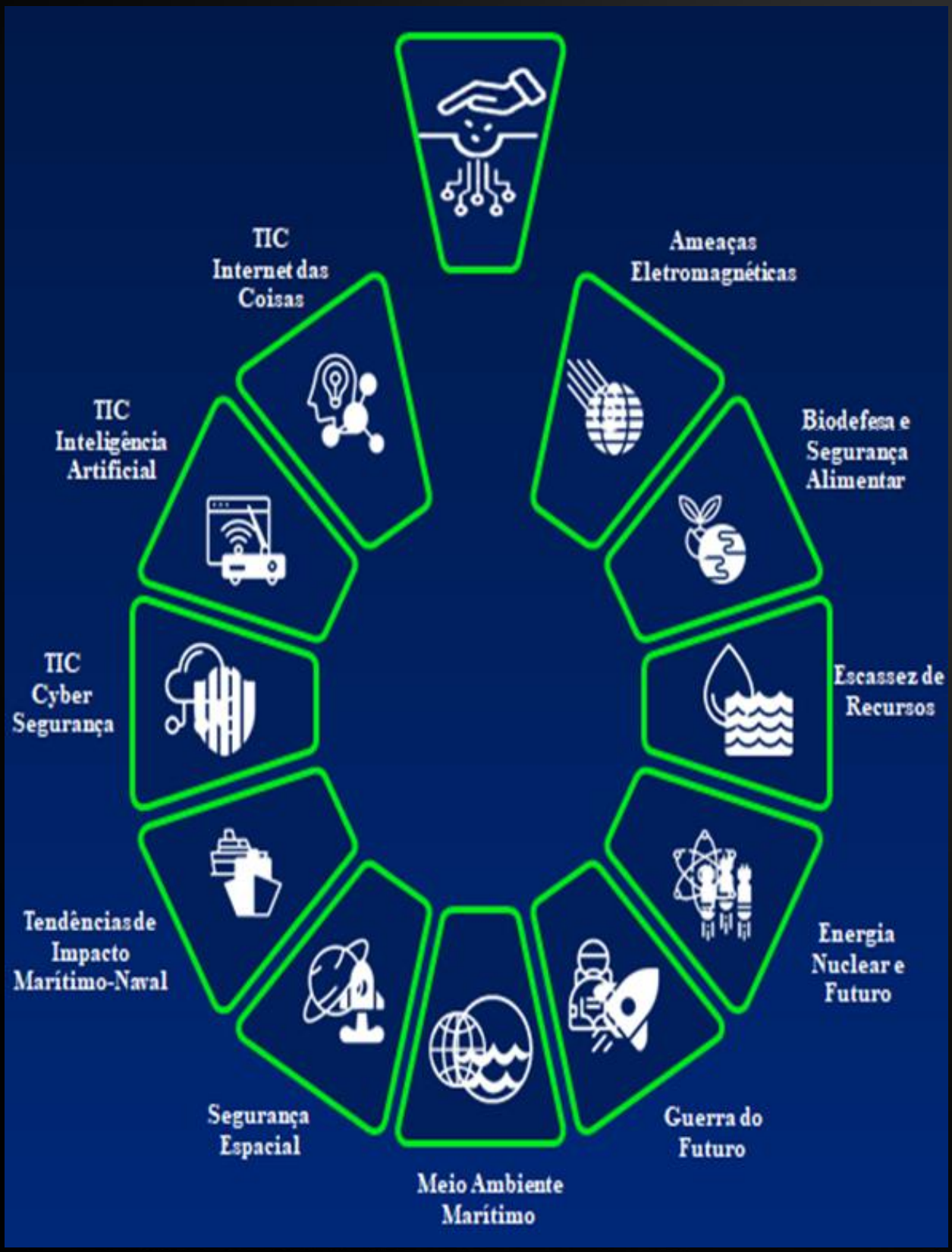
EXPEDIENTE

O Projeto Sementes de Futuro em Defesa faz parte do Programa de Cooperação Acadêmica em Defesa Nacional (PROCAD-DEFESA) “Prospectiva para Segurança e Defesa”, projeto da CAPES e do Ministério da Defesa (MD) liderado pela Escola de Guerra Naval (EGN) com 10 outras IES, Instituições e Empresas, para formar uma rede colaborativa de pesquisa e monitoramento de sementes do ambiente futuro, apoiada em plataforma computacional, análise multicritério, com abrangência nacional, participação social pública e privada, civil e militar para acompanhamento dos cenários prospectivos do Ministério da Defesa e uso dual.

O Sementes de Futuro em Defesa é um produto digital e semanal desenvolvido pelos pesquisadores das Linhas de Pesquisa Cenários Prospectivos de Segurança e Defesa do Laboratório de Simulações e Cenários (LSC) da EGN, cuja divulgação visa estimular e disseminar sementes de futuro para temas estratégicos sobre defesa e segurança, subsidiando análises prospectivas altamente qualificadas para auxiliar as Forças Armadas brasileiras no desenvolvimento de estratégias de longo prazo. As matérias deste informativo não representam o posicionamento institucional de qualquer setor das Forças Armadas.

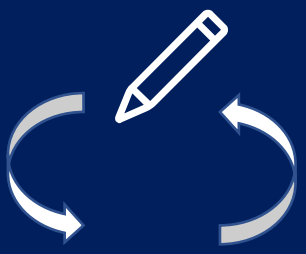
Acompanhe-nos nas Redes Sociais

Laboratório de Simulações e Cenários
Linha de Pesquisa Cenários Prospectivos para Segurança e Defesa
Avenida Pasteur, 480 – Urca, Rio de Janeiro – RJ – Brasil – CEP: 22290-240


TIC
Internet das
Coisas
Ameaças
Eletromagnéticas
TIC
Inteligência
Artificial
Biodefesa e
Segurança
Alimentar
TIC
Cyber
Segurança
Escassez de
Recursos
Tendências de
Impacto
Marítimo-Naval
Energia
Nuclear e
Futuro
Segurança
Espacial
Guerra do
Futuro
Meio Ambiente
Marítimo

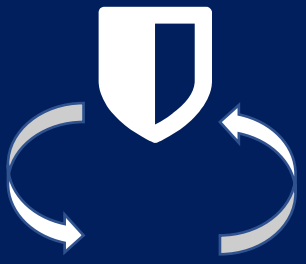
TENDÊNCIA DE PESO	**São eventos cuja direção e sentido são suficientemente consolidados para que se possa admitir sua continuidade no futuro; retratam processos cujo rompimento requer um esforço hercúleo e improvável de apresentar resultados. (LIMA; CURADO, 2017, pp. 16-17)**
FATO PRÉ-DETERMINADO	**São eventos já conhecidos, cuja ocorrência é praticamente certa. No geral, as indicações resultantes não se efetivaram ainda, mas se sabe que o evento irá ocorrer no futuro. (LIMA; CURADO, 2017, p. 17)**
FATO PORTADOR DE FUTURO	**São sinais existentes no ambiente, ínfimos por sua dimensão presente, mas imensos por suas consequências e potencialidades futuras. (MARCIAL, GRUMBACH, 2014, p. 240)**
INCERTEZA CRÍTICA	**São eventos mais incertos e de maior importância à cenarização; tratam-se das variáveis que determinarão a lógica e a ideia-força dos cenários, portanto, suas mudanças críticas possibilitam múltiplos futuros possíveis. (LIMA; CURADO, 2017, p. 17)**
SURPRESA INEVITÁVEL	**São forças previsíveis, pois têm suas raízes em forças que já estão em operação neste momento; entretanto, não se sabe quando irão se configurar, quais suas consequências previsíveis e como afetarão. (MARCIAL, GRUMBACH, 2014, p. 244)**
CORINGAS (WILD CARDS)	**Referem-se a grandes surpresas possuidoras de baixa probabilidade de ocorrência e extremamente difíceis de serem antecipadas; se consolidadas, possuem grande impacto e se materializam rapidamente. (LIMA; CURADO, 2017, p. 18)**
PRINCIPAIS ATORES E SUAS ESTRATÉGIAS	**Indivíduos, grupos ou organizações que influenciam ou recebem influência significativa do sistema; o ator desempenha importante papel, influenciando o comportamento das variáveis com objetivo de viabilizar seus projetos. (MARCIAL, GRUMBACH, 2014, p. 238)**

DATA E FONTE

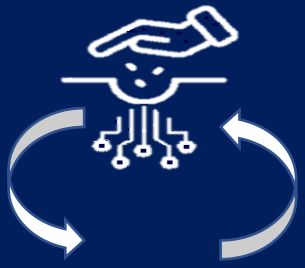


AUTOR

DESCRIÇÃO

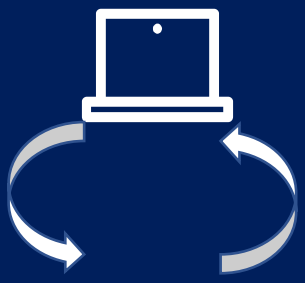


IMPACTOS FUTUROS
EM DEFESA



SEMENTES DE FUTURO
EM DEFESA

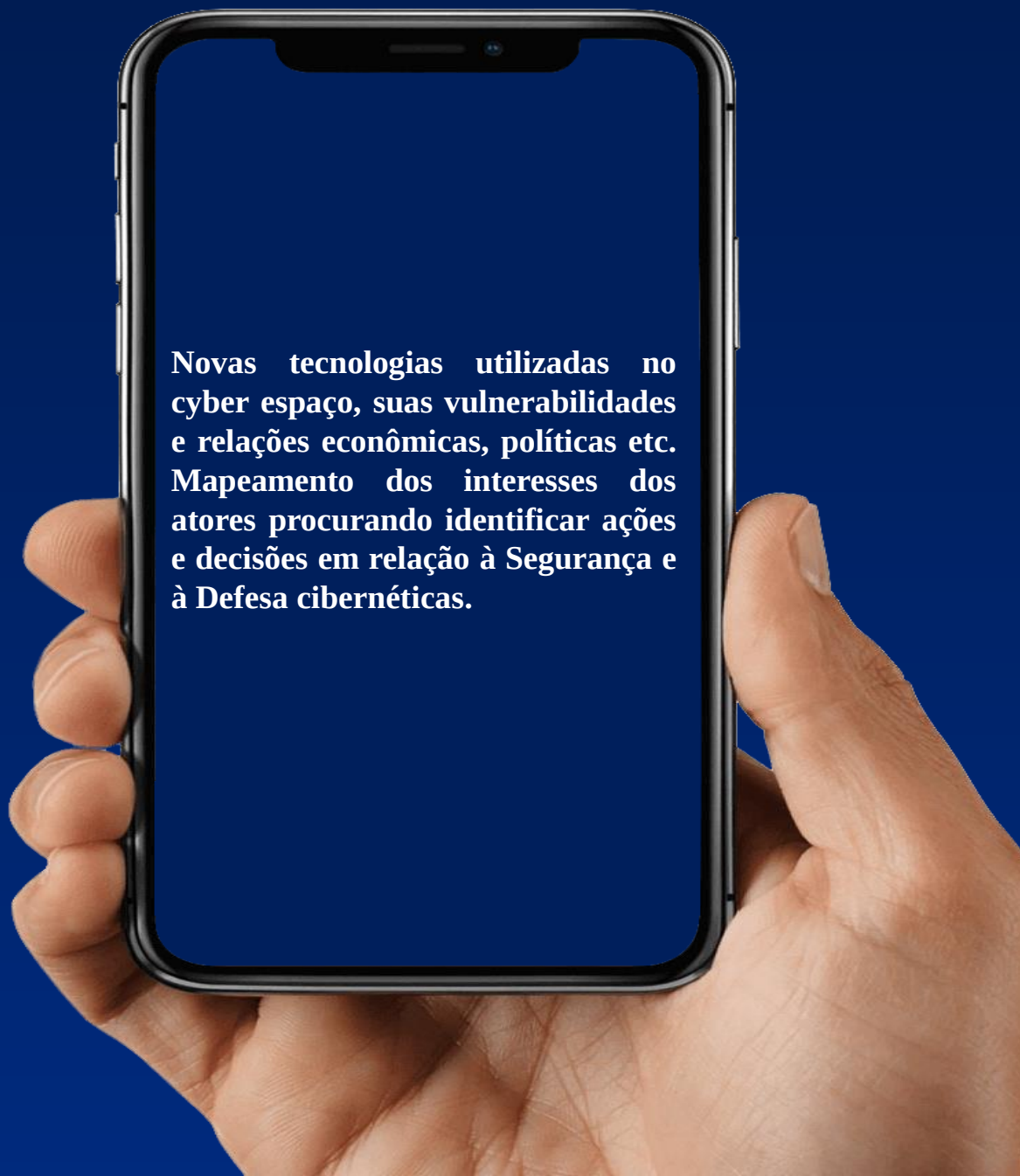
PALAVRAS-CHAVE



LINK DE ACESSO

PESQUISADOR DO LSC

TIC Cyber Segurança



LINGUÍSTICA FORENSE É INSTRUMENTO DE APOIO À INTELIGÊNCIA CIBERNÉTICA

11/03/2021 – Núcleo de Estudos Estratégicos em Defesa e Segurança (NEEDS)

Leonardo Perin Vichi

Desde 2017, o mundo tem visto a disseminação de diversos *malwares* que afetam empresas, órgãos governamentais e pessoas. Nesse jogo complexo, a dificuldade de identificar a autoria está no anonimato dos IPs e no uso de contas *blockchain* nos resgates. Mas uma ferramenta vinda das ciências forenses tem sido utilizada para o perfilamento dos autores: a Linguística Forense. Seu primeiro uso foi em 2018, no ataque ao sistema financeiro com o *malware Karamanak/Pegasus/Ratopak,* no qual foram detectadas em seu código-fonte evidências de que seus autores eram falantes do idioma russo. No ataque com o *Ransomware WannaCry*, o pedido de resgate foi redigido em 28 idiomas diferentes, e pesquisadores de Inteligência Cibernética, ao analisarem os textos, constataram que o nível de correção textual do texto em chinês indicava ter sido redigido por falantes nativos e escritos em teclado do próprio idioma.

A linguística forense vem se apresentando como mais uma ferramenta da inteligência cibernética. Sua utilização visa auxiliar o sistema de defesa nacional, inclusive do Brasil, um dos países do mundo que mais sofrem ataques cibernéticos. Na maioria das investidas, o criminoso utiliza meios diversos para ocultar seus rastros, mas sempre deixa alguma pista onde dados linguísticos podem permitir o perfilamento do atacante visando sua identificação.

Surpresa Inevitável

Ransomware; *malware*; *WannaCry*; *blockchain*; linguística forense.

http://needs.df.ufscar.br/artigos_de_opiniao3/127/leonardo_perin_vichi:_inteligencia_cibernetica_e_a_linguistica_forense_como_ferramenta_-_o_uso_da_analise_linguistica_para_atribuicao_de_autoria_em_ciberataques#linha

Marcelo Andrade de Barros – Pós-Graduado em Administração de Banco de Dados (UNESA)

DEPARTAMENTO DE JUSTIÇA DOS EUA ANUNCIA NOVA POLÍTICA DE ABUSO E FRAUDE CIBERNÉTICA

19/05/2022 – Departamento de Justiça dos Estados Unidos

Escritório de Relações Públicas

O Departamento de Justiça dos EUA anunciou a revisão de sua política em relação à cobrança de violações da Lei de Combate à Fraude Cibernética e Práticas Abusivas (*Computer Fraud and Abuse Act-CFAA*). Pela primeira vez, a política orienta que a pesquisa de segurança baseada em boas práticas não seja taxada ou cobrada legalmente. Estas pesquisas significam acessar um computador exclusivamente para fins de teste de boas práticas (*White Hat*), demonstrando boa-fé do usuário em investigação e/ou correção de uma falha ou vulnerabilidade de segurança. Tal atividade é realizada de maneira projetada para evitar qualquer dano a indivíduos ou ao público, e onde as informações derivadas da atividade são usadas principalmente para promover a segurança ou proteção da classe de dispositivos, máquinas ou serviços *online* à qual o computador acessado pertence, ou daqueles que usam tais dispositivos.

A pesquisa de segurança cibernética é um fator-chave para melhorar a segurança da informação em viés de prática computacional. A nova política promove a segurança cibernética ao fornecer clareza para pesquisadores de segurança em boas práticas, que erradicam vulnerabilidades para o bem comum, promovendo a privacidade e a segurança cibernética, defendendo o direito legal de indivíduos, proprietários de redes, operadores e outras pessoas para garantir a confidencialidade, integridade e disponibilidade das informações armazenadas em seus sistemas de informação. Um estudo mais detalhado desta nova política nos Estados Unidos pode auxiliar nas formulações futuras de pesquisas de segurança baseadas em boas práticas cibernéticas no Brasil.

Fato Pré-Determinado

Crime cibernético; proteção de dados; *compliance*; Política de Segurança da Informação e Comunicação (PSIC); proteção das informações.

https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act

Marcio Auday – Pós-Graduado em Direito e Processo Penal (UCAM-AVM)

NSA E ALIADOS EMITEM AVISO DE SEGURANÇA CIBERNÉTICA EM SETORES FRAGILIZADOS

17/05/2022 – *National Security Agency (NSA)*

Comunicado de Imprensa

A Agência de Segurança Cibernética e Infraestrutura (CISA), a Agência de Segurança Nacional (NSA) e o FBI, juntamente com nações aliadas, publicaram um Aviso de Segurança Cibernética para aumentar a conscientização sobre as configurações de segurança ruins, controles fracos e outras más condutas práticas de "limpeza" de rede que atores cibernéticos mal-intencionados usam para obter o acesso inicial sistêmico de uma vítima. As práticas e controles de segurança fracos explorados rotineiramente para acesso inicial também incluem as melhores práticas que podem ajudar as organizações a fortalecer suas defesas contra essa atividade maliciosa. Ainda segundo o aviso, enquanto essas falhas de segurança existirem, os cibercriminosos maliciosos continuarão a explorá-las. Para o diretor de segurança cibernética da NSA, Rob Joyce, é fundamental encorajar todos a mitigar essas fraquezas implementando as melhores práticas recomendadas.

Alguns dos pontos fracos mais comuns entre entidades internacionais e, inclusive, da gestão nacional no Brasil relacionada à segurança cibernética, incluem não utilizar a autenticação multifator, aplicar privilégios ou permissões incorretamente e erros nas listas de controle de acesso, não mantendo seus softwares atualizados. O referido comunicado recomenda mitigações que controlam o acesso, fortalecem as credenciais e estabelecem o gerenciamento centralizado de *logs*, aumentando o nível operacional de boas práticas em segurança cibernética.

Tendência de Peso

Segurança computacional; cibersegurança; proteção de dados; ataques cibernéticos; Política de Segurança da Informação e Comunicação (PSIC); proteção das informações.

https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3033563/nsa-allies-issue-cybersecurity-advisory-on-weaknesses-that-allow-initial-access/

Marcio Auday – Pós-Graduado em Direito e Processo Penal (UCAM-AVM)

PHISHING CONTINUARÁ SENDO RISCO PARA A SEGURANÇA CIBERNÉTICA

25/02/2021 – *Dark Reading*

Robert Lemos

De acordo com relatórios de ameaças cibernéticas publicados por empresas e instituições do setor, os cibercriminosos e os Estados dobraram e melhoraram os ataques populares, visando empresas com ataques de *ransomware* de dupla extorsão. Este tipo de ataque se trata de uma invasão em que o cibercriminoso não apenas "sequestra" o acesso aos dados e arquivos do computador e pede um resgate para liberá-los, como também cobra para não vazar as informações na internet. Utilizando-se de *phising* (uma técnica de crime cibernético que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais) com o tema COVID-19, e aproveitando o caos da segurança cibernética após a mudança para trabalho remoto, tais práticas vêm se apresentando como um constante alerta para a segurança cibernética no futuro.

Pode-se observar que diante de cenários de caos, ações maliciosas são executadas de forma paralela. Esses ataques demonstraram o quanto pode ser falha a segurança das informações governamentais, primordiais para o trabalho contínuo da máquina administrativa do país, inclusive do Brasil, uma vez que essas vulnerabilidades mapeadas podem ser porta de entrada para ataques futuros e/ou contínuos.

Tendências de Peso

Cybersegurança; ataques cibernéticos; *ransomware*; cyberameaças. *phishing*.

https://www.darkreading.com/threat-intelligence/ransomware-phishing-will-remain-primary-risks-in-2021

Fernanda Carvalho – Graduada em Relações Internacionais (IRID/UFRJ)

“RANSONWARE DAS COISAS” COMEÇA A SEQUESTRAR DISPOSITIVOS INTELIGENTES

05/02/2021 - Inforchannel.com.br

Redação

O *malware ransonware* apareceu em 2017, com a variante *WannaCry*, sequestrando computadores de centenas de empresas pelo mundo e, não parou de evoluir. Segundo pesquisadores da *Check Point*, está ocorrendo uma “mutação” do *malware* para *ransonware* das coisas (*Ransomware-of-Things* ou RoT), começando a sequestrar dispositivos inteligentes diversos, impedindo seu uso ou atrapalhando seu funcionamento. O risco dessa mutação é que os dispositivos de Internet das Coisas (IOT) estão cada vez mais comuns no dia a dia, e afetam diretamente sensores e automações nas linhas de produção, plantas industriais, consultórios médicos, dentre outros. O *ransonware* das coisas mostra como a conectividade é o motor do mundo, assim como os ataques contra dispositivos móveis podem contornar as medidas de segurança tradicionais.

Cada vez mais empresas e instituições públicas utilizam equipamentos IOT, que são rotineiramente produzidos sem preocupações de segurança cibernética. É importante ratificar que as Forças Armadas Brasileiras, no processo licitatório de equipamentos, deveriam deixar explícitos se os equipamentos seguem as boas práticas de segurança da informação em seu desenvolvimento.

Surpresa Inevitável

Ransomware; *smart devices*; *malware*; *WannaCry*; segurança cibernética.

https://inforchannel.com.br/check-point-alerta-sobre-os-principais-riscos-do-ransomware-das-coisas-e-como-funciona/

Marcio Auday – Pós-Graduado em Direito e Processo Penal (UCAM-AVM)

SEMENTES DE FUTURO EM DEFESA

Sinalizar o futuro para defender o presente