CyberStories

PORTAL PARA ESTUDOS DE CASOS EM CIBERSEGURANÇA

Gabriel Wagnitz

gabriel@wagnitz.com.br

Este é CyberStories

Estudos de caso em cibersegurança, um catálogo com estudos sobre episódios famosos da história recente.

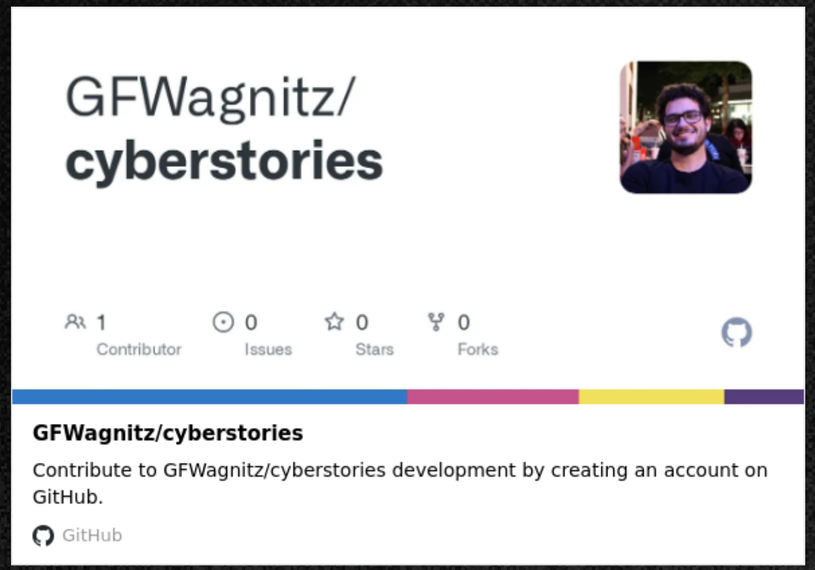
CyberStories - Estudos de caso em cibersegurança

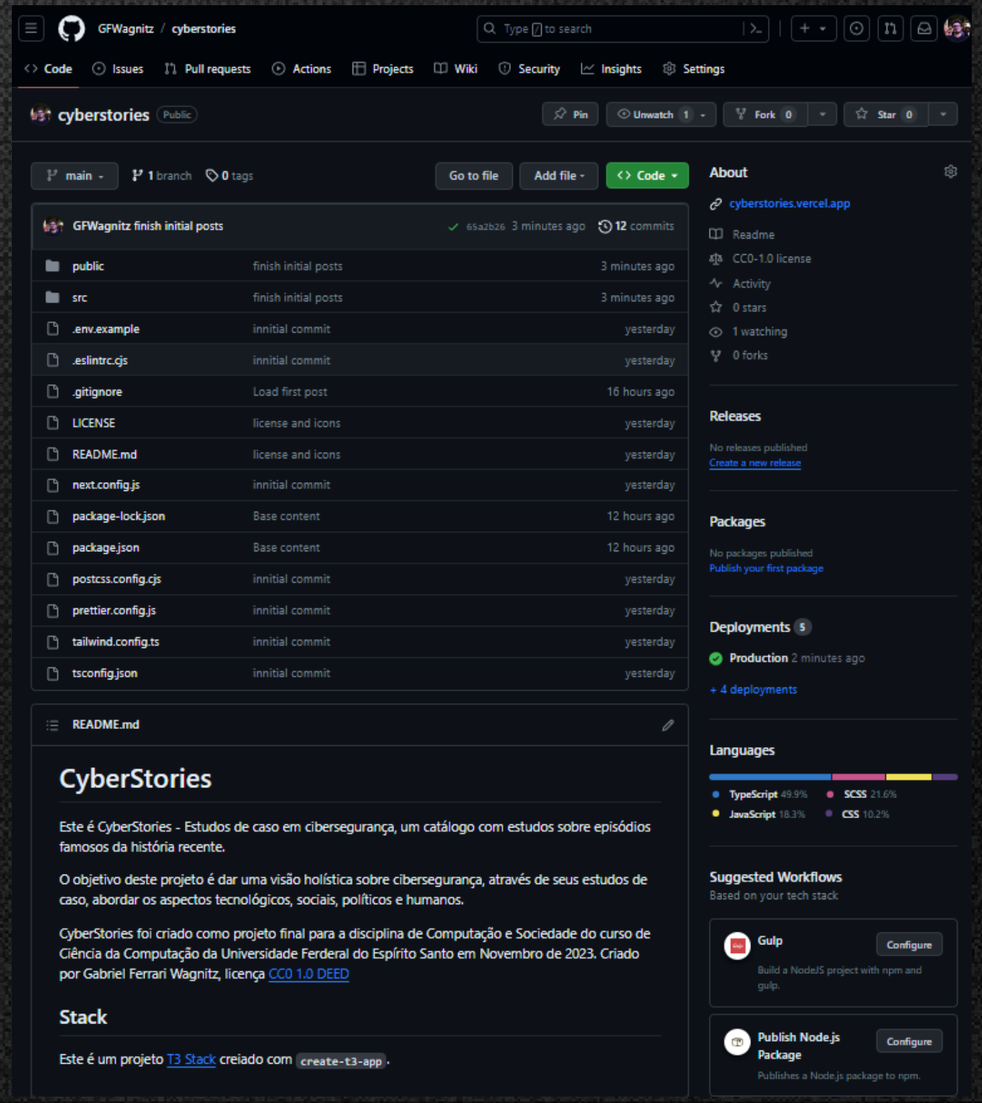
Estudos de caso em cibersegurança

vercel.app

Desenvolvido com T3

NextJS + Typescript





Estudos de caso já lançados

< Voltar

APT1 - Espionagem Internacional

APT1, também conhecida como Unidade 61398 do Exército de Libertação Popular (PLA) da China, foi objeto de um relatório significativo de segurança cibernética em 2013 pela empresa americana de segurança cibernética Mandiant. O relatório revelou muitos detalhes sobre as atividades de espionagem cibernética do APT1.

Alvos e motivação

O APT1 tinha como alvo principal organizações de vários setores em países de língua inglesa, com foco em propriedade intelectual e segredos comerciais. Os motivos pareciam ser o avanço económico e tecnológico das empresas chinesas.

O relatório revelou uma extensa escala de operações, com o APT1 roubando centenas de terabytes de dados de pelo menos 141 organizações em vários setores.

Táticas e técnicas

O APT1 usou uma série de táticas, incluindo e-mails de spear-phishing, malware personalizado e persistência de longo prazo nas redes alvo. Suas técnicas demonstraram altos níveis de sofisticação e persistência.

O relatório detalhou a vasta infraestrutura utilizada pelo APT1, incluindo uma rede de servidores em vários países e uma gama de ferramentas e técnicas para conduzir espionagem cibernética.

Impacto Global

< Voltar

O Episódio Snowden

Os primeiros relatórios sobre as revelações de Edward Snowden sobre programas de vigilância global conduzidos pela Agência de Segurança Nacional dos Estados Unidos (NSA) e seus parceiros internacionais foram publicados em 5 de junho de 2013. Esses relatórios foram baseados em documentos confidenciais que Snowden vazou para os jornalistas Glenn Greenwald, Laura Poitras e Ewen MacAskill. As revelações de Snowden revelaram uma vasta rede de actividades de vigilância, desencadeando um debate global significativo sobre privacidade, segurança e o equilíbrio entre a segurança nacional e os direitos individuais.

Em maio de 2013, Snowden viajou para Hong Kong e forneceu aos jornalistas do The Guardian e do The Washington Post milhares de documentos confidenciais da NSA. Os documentos revelaram numerosos programas de vigilância globais, muitos deles geridos pela NSA e pela Five Eyes Intelligence Alliance, com a cooperação de empresas de telecomunicações e governos europeus.

Táticas e técnicas

Acesso e autorização: A posição de Snowden como administrador de sistemas da empresa contratada pela NSA, Booz Allen Hamilton, deu-lhe autorizações de segurança de alto nível e acesso a informações confidenciais. Essa função proporcionou-lhe acesso mais amplo a vários documentos e sistemas em comparação com outros funcionários que tinham acesso mais limitado e específico à função.

Métodos de coleta de dados: Snowden teria usado seu acesso autorizado para baixar documentos confidenciais. Diz-se que ele usou ferramentas cotidianas disponíveis para administradores de sistema, como baixar arquivos em unidades USB. Seu profundo conhecimento das redes e sistemas da NSA permitiu-lhe navegar e extrair informações sem disparar alarmes de segurança.

Snowden afirmou que selecionou e revisou cuidadosamente os documentos para evitar a divulgação de informações que pudessem prejudicar

Melhorias futuras

OWASP Foundation, the Open Source Foundation for Application Security | OWAS...

OWASP Foundation, the Open Source Foundation for Application Security on the main website for The OWASP...

owasp.org

Cybersecurity Skills Paths & Job Role Paths

Guidance on which HTB Academy Modules to study to obtain specific practical skills necessary for a specific cybersecurity job role.

hackthebox.com /