EUROPEAN TLD ISAC

Análise do cenário de ameaças a Top-Level Domains

Resumo executivo

ANÁLISE DO CENÁRIO DE AMEAÇAS A TOP-LEVEL DOMAINS EM 2024

SOBRE O TLD ISAC Europeu

O European Top-Level Domain Information Sharing and Analysis Centre (TLD ISAC Europeu) é uma iniciativa de colaboração dedicada a reforçar a postura de cibersegurança dos registries de top-level domain com código de país (ccTLD) em toda a Europa. Funciona como uma plataforma fiável para a partilha de informações sobre ameaças, promovendo as melhores práticas e fomentando a cooperação entre operadores de ccTLD, peritos em segurança e outras partes interessadas. Para mais informações, aceda a https://www.tld-isac.eu.

CONTACTO

Para contactar o TLD ISAC Europeu ou para questões de imprensa sobre este relatório, envie um e-mail para info@tld-isac.eu.

AVISO LEGAL

NOTA DA VERSÃO PORTUGUESA

Este documento é uma tradução para português do documento original publicado pelo TLD ISAC Europeu. A tradução apresentada foi realizada no âmbito do programa de capacitação digital da LusNIC e CDA/ICANN, sendo esta fornecida apenas para fins informativos. Em caso de divergência, inconsistência ou dúvida de interpretação, a versão original prevalece.

A LusNIC agradece ao TLD ISAC Europeu, entidade responsável pelo documento original, pela produção e disponibilização destes conteúdos, que serviram de base à presente tradução para português, realizada com o objetivo de apoiar a capacitação e a partilha de conhecimento entre os membros da comunidade LusNIC.

Resumo executivo

O TLD ISAC Europeu realizou uma Análise do Cenário de Ameaças (TLA) para identificar as ameaças que afetam os operadores de registry de TLD. Um grupo de trabalho do ISAC identificou 55 ameaças relacionadas com o ecossistema de ccTLD. Cada ameaça foi avaliada em termos de impacto e probabilidade por 18 membros efetivos do CENTR (todos ccTLD) em fevereiro e março de 2024. As ameaças foram classificadas por ordem de prioridade com base na perceção do risco, tendo em conta o impacto e a probabilidade. As funções individuais dos inquiridos na organização incluíam CEO, CISO e gestores de segurança.
O resumo executivo é público, ao passo que o acesso aos resultados detalhados do estudo é restrito aos participantes no inquérito CENTR e aos membros do TLD ISAC Europeu.

De forma global, das 55 ameaças analisadas, 5 ameaças resultam num risco "alto", 26 num risco "médio", 17 num risco "baixo" e 7 num risco "muito baixo". Nenhuma das ameaças foi avaliada como um risco "inaceitável ou "muito alto".

As ameaças classificadas como "risco alto" são

TH01 Os cibercriminosos pretendem aceder às informações privadas dos registrants a partir do sistema de gestão dos nomes de domínio.

TH17 Os cibercriminosos pretendem obter as credenciais dos utilizadores internos e dos registrars a partir do sistema de gestão do software de servidores de nomes.

TH35 Os cibercriminosos pretendem aceder a informações confidenciais do registry ccTLD com recurso a phishing.

TH43 Os cibercriminosos pretendem manipular os anúncios de prefixos BGP para sequestrar o tráfego anycast.

TH45 Os cibercriminosos pretendem entrar no ecossistema de registry ccTLD e aí permanecer durante o máximo de tempo possível, aprendendo sobre as suas operações e configuração, divulgando informações.

As 55 ameaças foram todas classificadas segundo a seguinte matriz de risco. O valor do risco é calculado com base no impacto médio, na probabilidade média das respostas agregadas dos inquiridos, e por ID de ameaça única.

Matriz de risco

IMPACTO MÉDIO POR ID DE AMEAÇA

PROBABILIDADE MÉDIA POR ID DE

	MUITO BAIXO	BAIXO	MÉDIO	ALTO	MUITO ALTO
MUITO PROVÁVEL	BAIXO: (0)	MÉDIO: (1) TH11	ALTO: (0)	MUITO ALTO: (0)	INACEITÁVEL: (0)
POUCO PROVÁVEL	BAIXO: (0)	MÉDIO: (2) TH15, TH28	ALTO: (1) TH35	ALTO: (0)	MUITO ALTO: (0)
MODERADO	MUITO BAIXO: (0)	BAIXO: (3) TH18, TH34, TH36	MÉDIO: (13) TH04, TH05, TH10, TH12, TH16, TH23, TH27, TH29, TH31, TH37, TH38, TH46, TH47	ALTO: (4) TH01, TH17, TH43 , TH45	ALTO: (0)
POUCO IMPROVÁVEL	MUITO BAIXO: (0)	MUITO BAIXO: (1) TH26	BAIXO: (12) TH06, TH08, TH09, TH13, TH14, TH22, TH33, TH40, TH41, TH42, TH50, TH51	MÉDIO: (8) TH03, TH07, TH20, TH30, TH32, TH39, TH52, TH53	MÉDIO: (2) TH02, TH19
MUITO IMPROVÁVEL	MUITO BAIXO: (0)	MUITO BAIXO: (0)	MUITO BAIXO: (6) TH24, TH25, TH44, TH48, TH49, TH55	BAIXO: (2) TH21, TH54	BAIXO: (0)

Recomendações

Os resultados desta análise podem ser utilizados para dar prioridade às atividades de mitigação com base nos requisitos de conformidade de uma organização e no nível de aceitação do risco. O quadro seguinte apresenta uma visão geral das 10 ameaças com classificação mais elevada e os valores médios de resposta de impacto e probabilidade. Numa fase seguinte, as organizações podem definir e implementar medidas de mitigação, que normalmente resultam em evitar o risco, reduzir o risco, partilhar o risco ou aceitar o risco. As opções de mitigação relacionadas com a redução ou minimização das 10 principais ameaças identificadas podem ser encontradas nos capítulos sobre as ameaças correspondentes. Após a seleção das opções de mitigação, os resultados devem ser documentados.

ID DA AMEAÇA	DESCRIÇÃO DA AMEAÇA	RISCO	IMPACTO MÉDIO	PROBABILIDADE MÉDIA
TH01	Os cibercriminosos pretendem aceder às informações privadas dos registrants a partir do sistema de gestão dos nomes de domínio.	ALTO	ALTO	MODERADA
TH17	Os cibercriminosos pretendem obter as credenciais dos utilizadores internos e dos registrars a partir do sistema de gestão do software de servidores de nomes.	ALTO	ALTO	MODERADA
TH43	Os cibercriminosos pretendem manipular os anúncios de prefixos BGP para sequestrar o tráfego anycast.	ALTO	ALTO	MODERADA
TH45	Os cibercriminosos pretendem entrar no ecossistema de registry ccTLD e aí permanecer durante o máximo de tempo possível, aprendendo sobre as suas operações e configuração, divulgando informações.	ALTO	ALTO	MODERADA
TH35	Os cibercriminosos pretendem aceder a informações confidenciais do registry ccTLD com recurso a phishing.	ALTO	MÉDIO	POUCO PROVÁVEL
TH02	Os cibercriminosos pretendem controlar o sistema de gestão de nomes de domínio.	MÉDIO	MUITO ALTO	POUCO PROVÁVEL
TH19	Os cibercriminosos pretendem comprometer a integridade total do ficheiro de zona DNS em repouso.	MÉDIO	MUITO ALTO	POUCO PROVÁVEL
TH03	Os cibercriminosos pretendem encriptar a infraestrutura do sistema de gestão de nomes de domínio para chantagear o registry ccTLD e pedir um resgate.	MÉDIO	ALTO	POUCO PROVÁVEL
TH07	Os cibercriminosos pretendem prevenir que o registry ccTLD cumpra os SLA relacionados com a disponibilidade do serviço de gestão de nomes de domínio para os registrars.	MÉDIO	ALTO	POUCO PROVÁVEL
TH20	Os cibercriminosos pretendem comprometer a integridade dos registos DNS, em repouso, da zona DNS que não estão assinados.	MÉDIO	ALTO	POUCO PROVÁVEL

EUROPEAN
TLD ISAC