

Classificação de Incidentes

TAXONOMIA

Classe Incidente	Tipo Incidente
Código Malicioso	Sistema Infetado
	Distribuição de Malware
	Servidor C2
	Configuração de Malware
Disponibilidade	Negação de Serviço
	Negação de Serviço Distribuída
	Configuração incorreta
	Sabotagem
	Interrupção
Recolha de Informação	Scanning
	Sniffing
	Engenharia Social
Intrusão	Compromisso de Conta Privilegiada
	Compromisso de Conta Não Privilegiada
	Compromisso de Aplicação
	Arrombamento
Tentativa de Intrusão	Exploração de Vulnerabilidade
	Tentativa de Login
	Nova assinatura de ataque
Segurança da Informação	Acesso não autorizado
	Modificação não autorizada
	Perda de dados
Fraude	Utilização indevida ou não autorizada de recursos
	Direitos de autor
	Utilização ilegítima de nome de terceiros
	Phishing
Conteúdo Abusivo	SPAM
	Discurso Nocivo
	Exploração sexual de menores, racismo e apologia da violência

Vulnerabilidade	Criptografia fraca
	Amplificador DDoS
	Serviços acessíveis potencialmente indesejados
	Revelação de informação
	Sistema vulnerável
Outro	Sem tipo
	Indeterminado

O CERT.PT utiliza para a sua classificação de incidentes a taxonomia da Rede Nacional de CSIRT. Para mais detalhes/informação acerca da Taxonomia em vigor existe um documento disponível no website da RNCSIRT.

Mais informações: https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf