Taxonomia Comum da Rede Nacional de CSIRT

Dezembro 2023

Taxonomia Comum da Rede Nacional de CSIRT

Versão:

20231215

(ENISA / TF-CSIRT RSIT WG v.1003)

Autor:

Grupo de Trabalho 1 - Taxonomia

Revisão:

Grupo de Trabalho 1 - Taxonomia

Dezembro de 2023

Classificação	Data	Versão do documento
TLP:CLEAR	Dezembro 2023	3.3

Título
Taxonomia Comum da Rede Nacional de CSIRT

Origem
Rede Nacional de CSIRT – Grupo de Trabalho Taxonomia

Histórico de Versões			
Versão	**Data**	**Revisor**	**Comentários/Notas**
2.5	Dezembro 2012		
3.0	Dezembro 2019	Grupo de Trabalho – Taxonomia	Revisão e Atualização da Taxonomia
3.3	Dezembro 2023	Grupo de Trabalho – Taxonomia	Revisão e alinhamento com a RSIT v1003

ÍNDICE

1. INTRODUÇÃO

Este documento descreve a taxonomia comum para a classificação de incidentes de segurança informática, na Rede Nacional de CSIRT.

Esta taxonomia foi revista durante o ano de 2019 tendo originado a versão 3.0 deste documento. Como base para a revisão, o Grupo de Trabalho (GT) teve em consideração a Taxonomia de Referência do Working Group – RSIT WG .

O documento foi novamente revisto no decorrer do ano 2023, tendo originado a versão 3.3. A passagem direta da versão 3.0 para 3.3 faz-se no sentido de alinhar a minor release com a versão 1.3 (1003) da RSIT WG.

2. CLASSIFICAÇÃO DE INCIDENTES

A classificação de incidentes deverá ser efetuada com base em dois vetores – "Tipo de Incidente" e "Tipo de Evento". No modelo de classificação de incidentes adotado foi ainda decidida uma divisão dos vários Tipos específicos de incidentes por Classes genéricas que agrupam conjuntos de incidentes com resultados ou objetivos semelhantes. Para além das Classes e Tipos de incidentes, foi ainda identificado um conjunto de eventos associados a cada Tipo de incidente. A tabela seguinte elenca, de forma não exaustiva, os tipos de eventos presentes na Taxonomia Comum da Rede Nacional de CSIRT.

Tipo de Evento	**Descrição**
Sistema(s) infetado(s) com *malware* conhecido	Detetado num sistema a presença de qualquer um dos tipos de *malware*.
Disseminação de *malware* através de e-mail	*Malware* anexo a mensagem ou presença de link para URL malicioso em mensagem de correio eletrónico.
Disseminação de *malware* através de *QRCode*	URI codificado em *QRCode*, para download de *malware*
Alojamento de *malware* em página *web*	Página *web* que se encontra a disseminar um dos vários tipos de *malware*.
Alojamento de servidor C2	Sistema que é usado como ponto de controlo de uma *botnet*. Também se inclui neste campo os sistemas que servem como ponto de recolha de dados furtados através de *botnets*.
Replicação e disseminação de *worm*	Sistema comprometido com um *worm* que tenta comprometer outros sistemas.
Ligação a porto(s) suspeito(s), associado(s) a um determinado *malware*	Sistema que efetua tentativas de acesso a um porto geralmente associado a um determinado tipo de *malware*.

Ligação a sistema(s) suspeito(s) associado(s) a um determinado *malware*	Sistema que efetua tentativas de acesso a um endereço IP ou URL geralmente associado a um determinado tipo de *malware* como por exemplo, C2 ou página para distribuição de componentes associados a uma determinada *botnet*.
Flood de pedidos	Envio massivo de pedidos (pacotes de rede, e-mails, etc.), a partir de uma única fonte, a um determinado serviço com o objetivo de afetar o seu funcionamento.
Exploit ou ferramenta para esgotamento de recursos (rede, capacidade de processamento, sessões, etc.)	Utilização, a partir de uma única fonte, de software especialmente concebido para afetar o funcionamento de um determinado serviço através da exploração de uma vulnerabilidade no mesmo.
Flood distribuído de pedidos	Envio massivo de pedidos (pacotes de rede, e-mails, etc.), a partir de várias fontes, a um determinado serviço com o objetivo de afetar o seu funcionamento.
Exploit ou ferramenta distribuídos para esgotamento de recursos	Utilização, a partir de várias fontes, de software especialmente concebido para afetar o funcionamento de um determinado serviço através da exploração de uma vulnerabilidade no mesmo.
Vandalismo	Atividades lógicas e físicas que não tenham como objetivo premeditado danificar a informação ou evitar a sua transmissão entre sistemas, mas que tenham essa consequência.
Disrupção intencional de mecanismos de transmissão e tratamento de dados	Atividades lógicas e físicas que tenham como objetivo premeditado de corromper a informação ou evitar a sua transmissão entre sistemas.
Disrupção não intencional de mecanismos de transmissão e tratamento de dados	Acontecimentos que tenham como consequência não prevista a corrupção da informação ou impossibilidade de transmissão entre sistemas.
Probe a sistema	*Scan* a um único sistema à procura de portos abertos ou serviços a responderem nesses portos.
Scan de rede	*Scan* a uma rede de sistemas, com o objetivo de identificar sistemas que estejam ativos nessa mesma rede.

Transferência de zona DNS	Transferência não autorizada de uma determinada zona de DNS.
Wiretapping	Interceção, lógica ou física, de comunicações.
Disseminação de e-mails de *phishing*	Envio massivo de e-mails com o objetivo de recolher dados para efeitos de *phishing* das vítimas.
Alojamento de *websites* de *phishing*	Alojamento de *websites* para efeitos de *phishing*.
Agregação de informação recolhida em esquemas de *phishing*	Recolha de dados resultantes de ataques de *phishing* através de páginas *web*, contas de correio eletrónico, etc.
Tentativa de utilização de *exploit*	Utilização, sem sucesso, de uma ferramenta que explora uma determinada vulnerabilidade no sistema.
Tentativa de SQL *Injection*	Tentativa, sem sucesso, de manipulação ou leitura de dados em base de dados, através da técnica de SQL *Injection*.
Tentativa de XSS	Tentativa, sem sucesso, de ataques recorrendo a técnicas de *cross-site scripting*.
Tentativa de *file inclusion*	Tentativa, sem sucesso, de inclusão de ficheiros no sistema alvo através de técnicas de *file inclusion*.
Tentativa de ataque *brute-force*	Tentativa de *login*, sem sucesso, em sistema através da utilização sequencial e consecutiva de credenciais de acesso.
Tentativa de password *cracking*	Tentativa de descoberta de credenciais de acesso através da quebra dos mecanismos criptográficos que as protegem.

Tentativa de ataque dicionário	Tentativa de *login*, sem sucesso, em sistema através da utilização de credenciais de acesso pré-carregadas em dicionário.
Utilização de *exploit* local ou remoto	Utilização, com sucesso, de uma ferramenta que explora uma determinada vulnerabilidade no sistema.
SQL *Injection*	Manipulação ou leitura de dados em base de dados, através da técnica de SQL *Injection*.
XSS	Ataques recorrendo a técnicas de *cross-site scripting*.
File inclusion	Inclusão de ficheiros no sistema alvo através de técnicas de *file inclusion*.
Bypass sistema controlo	Acesso indevido a sistema ou componente contornando um sistema de controlo de acesso existente.
Furto de credenciais de acesso	Acesso indevido a sistema ou componente através da utilização de credenciais de acesso furtadas.
Furto de credenciais de acesso privilegiado	Acesso indevido a sistema ou componente através da utilização de credenciais de acesso privilegiado furtadas.
Acesso indevido e sistema	Acesso não autorizado a um sistema ou componente.
Acesso indevido à informação	Acesso não autorizado a um conjunto de informações.
Exfiltração de dados	Acesso e partilha não autorizados de um determinado conjunto de informações.

Modificação de informação	Alteração indevida de um determinado conjunto de informações.
Eliminação de informação	Eliminação indevida de um determinado conjunto de informações.
Utilização indevida ou não autorizada de recursos	Utilização de recursos da instituição para fins diferentes daqueles para que os mesmos foram afetos.
Utilização ilegítima de nome da instituição ou de terceiros	Utilização de nome da instituição sem autorização da mesma.
Flood de e-mails	Envio de número anormalmente elevado de mensagens de correio eletrónico.
Envio de mensagem não solicitada	Envio de mensagem de correio eletrónico não solicitada ou não pretendida pelo destinatário.
Distribuição ou partilha de conteúdos protegidos por direitos de autor	Distribuição ou partilha de conteúdos protegidos por direitos de autor e direitos conexos.
Disseminação de conteúdos proibidos por lei (crimes públicos).	Distribuição ou partilha de conteúdos ilegais como pornografia de menores, glorificação da violência, e outros conteúdos proibidos por lei.

Tabela 1 - Classificação de Eventos

Numa fase posterior o incidente deve ser classificado por tipo, segundo a tabela 2, abaixo.

3. TAXONOMIA DE REFERÊNCIA PARA INCIDENTES DE SEGURANÇA [V3.3]

REFERENCE SECURITY INCIDENT TAXONOMY [1003]

Classe de Incidente ***Classification***	**Tipo de Incidente** ***Incident Examples***	**Descrição / Exemplos** ***Description / Examples***
Conteúdo Abusivo Abusive Content	Spam Spam	Spam ou "e-mail em massa não solicitado", significa que o destinatário não concedeu permissão verificável para o envio da mensagem e que a mensagem é enviada como parte de uma coleção maior de mensagens, todas com conteúdo funcionalmente comparável. Este IOC refere-se a recursos da infraestrutura de spam, tais como verificadores e/ou coletores de endereços, URLs em e-mails de spam, etc. *Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content. This IOC refers to resources, which make up spam infrastructure, for example, harvesters like address verification, URLs in spam emails, etc.*
	Discurso Nocivo Harmful Speech	Perseguição ou discriminação de alguém, p. ex., através de ciber perseguição, racismo ou ameaças, contra um ou mais indivíduos. *Bullying, harassment or discrimination of somebody, e.g., cyber stalking, racism or threats against one or more individuals.*
	Exploração Sexual de Menores, Racismo e Apologia da Violência	Exploração Sexual de Menores, conteúdo sexual, glorificação da violência, e outros conteúdos proibidos por lei.

	(Child) Sexual Exploitation/Sexual/Violent Content	*Child Sexual Exploitation (CSE), Sexual content, glorification of violence, etc.*
Código Malicioso Malicious Code	Sistema Infetado Infected System	Sistema infetado com *malware*, p. ex., PC, smartphone ou servidor infetados com um *rootkit*. Na maioria das vezes, refere-se a ligações a um servidor de comando e controlo "*sinkholed*". *System infected with malware, e.g., PC, smartphone or server infected with a rootkit. Most often this refers to a connection to a sinkholed command and control server.*
	Servidor C2 C2 Server	Servidor de comando e controlo contactado por *malware* em sistemas infetados. *Command and control server contacted by malware on infected systems.*
	Distribuição de *Malware* Malware Distribution	URI usado para distribuição de *malware*, p. ex., um URL para download incluído em faturas falsas distribuídas via *spam* de *malware* ou *exploit-kits* (em *websites*). *URI used for malware distribution, e.g., a download URL included in fake invoice malware spam or exploit kits (on websites).*
	Configuração de *Malware* Malware Configuration	URI de alojamento de ficheiro de configuração de *malware*, p. ex., código web para injeção de *trojans* bancários. *URI hosting a malware configuration file, e.g., web injects for a banking trojan.*

Recolha de Informação Information Gathering	Scanning Scanning	Ataques baseados em pedidos realizados a um sistema com o intuito de descobrir pontos fracos. Também inclui processos de teste para recolha de informações sobre sistemas, serviços e contas. Inclui *fingerd*, consultas DNS, ICMP, SMTP (EXPN, RCPT, etc.) e *scanning* de portos. *Attacks that send requests to a system to discover weaknesses. This also includes testing processes to gather information on hosts, services and accounts. This includes fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, etc) port scanning.*
	Sniffing Sniffing	Observação e/ou gravação de tráfego de rede (*wiretapping*). *Observing and recording of network traffic (wiretapping).*
	Engenharia Social Social Engineering	Recolha de informações de um ser humano através de meios não técnicos (p. ex., mentiras, truques, subornos ou ameaças). *Gathering information from a human being in a non-technical way (e.g., lies, tricks, bribes, or threats).*
Tentativa de Intrusão Intrusion Attempts	Exploração de Vulnerabilidade Exploitation of Known Vulnerabilities	Tentativa de comprometer um sistema ou corromper um serviço, através da exploração de vulnerabilidades com um identificador padronizado, como o CVE (p. ex., usando *buffer overflow*, *backdoor*, *cross-site scripting*) *An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g., using buffer overflow, backdoor, cross site scripting)*

	Tentativa de *Login* Login Attempts	Múltiplas tentativas de *brute-force login* (incluindo adivinha ou quebra de passwords). Este IOC refere-se a um recurso que foi observado a executar ataques *brute-force* sobre um determinado protocolo aplicacional. *Multiple brute-force login attempts (including guessing or cracking of passwords). This IOC refers to a resource, which has been observed to perform brute-force attacks over a given application protocol.*
	Nova Assinatura de Ataque New Attack Signature	Ataque que usa a exploração de uma vulnerabilidade desconhecida. *An attack using an unknown exploit.*
Intrusão Intrusions	Comprometimento de Conta Privilegiada Privileged Account Compromise	Comprometimento de um sistema em que o atacante ganhou privilégios de administração. *Compromise of a system where the attacker gained administrative privileges.*
	Comprometimento de Conta Não Privilegiada Unprivileged Account Compromise	Comprometimento de um sistema usando uma conta (utilizador/serviço) não privilegiada. *Compromise of a system using an unprivileged (user/service) account.*
	Comprometimento de Aplicação Application Compromise	Comprometimento de uma aplicação através da exploração de vulnerabilidades (des)conhecidas, p. ex., *SQL injection*. *Compromise of an application by exploiting (un)known software vulnerabilities, e.g., SQL injection.*

	Comprometimento de Sistema System Compromise	Comprometimento de um sistema p. ex., *logins* ou execução de comandos não autorizados. Inclui tentativas de comprometimento de sistemas *honeypot*. *Compromise of a system, e.g., unauthorised logins or commands. This includes attempts to compromise honeypot systems.*
	Arrombamento Burglary	Intrusão física, p. ex., no edifício ou centro de dados corporativos. *Physical intrusion, e.g., into corporate building or data centre.*
Disponibilidade Availability	Negação de Serviço Denial of Service	Ataque de Negação de Serviço, p. ex., envio de pedidos especialmente concebidos para uma aplicação web que causam falha ou lentidão. *Denial of Service attack, e.g., sending specially crafted requests to a web application which causes the application to crash or slow down.*
	Negação de Serviço Distribuída Distributed Denial of Service	Ataque distribuído de negação de serviço, p. ex., ataques *SYN-Flood* ou de reflexão/amplificação UDP. *Distributed Denial of Service attack, e.g., SYN-Flood or UDP-based reflection/amplification attacks.*
	Configuração Incorreta Misconfiguration	Configuração incorreta de software que resulta em problemas de disponibilidade de serviço, p. ex., um servidor DNS com a DNSSEC KSK da zona raiz, desatualizada. *Software misconfiguration resulting in service availability issues, e.g., DNS server with outdated DNSSEC Root Zone KSK.*

	Sabotagem Sabotage	Ações maliciosas intencionais que ameaçam, tentam ou concretizam danos a um sistema ou componente com o objetivo de interromper a disponibilidade de um serviço. Estas podem ser de natureza lógica ou física, desde regras maliciosas numa firewall que impedem todo o tráfego, a corte de cabos, ameaça de bomba ou fogo posto. *Intentional actions maliciously threatening to, attempting to or actually damaging a system or component with the aim of disrupting the availability of a service. These can happen both at logical and physical levels, from malicious firewall rules dropping all traffic, to wire-cutting, bomb threats or arson.*
	Interrupção Outage	Interrupção provocada p. ex., por falha de ar condicionado ou desastre natural. *An outage caused, for example, by air conditioning failure or natural disaster.*
Segurança da Informação Information Content Security	Acesso Não Autorizado Unauthorised Access to Information	Acesso não autorizado à informação, p. ex., abusando credenciais furtadas para acesso a um sistema ou aplicação, interceção de tráfego ou obtenção de acesso a documentos físicos. *Unauthorised access to information, e.g., by abusing stolen login credentials for a system or application, intercepting traffic or gaining access to physical documents.*
	Modificação Não Autorizada Unauthorised Modification of Information	Modificação não autorizada de informação, p. ex., um atacante usar credenciais roubadas para acesso a um sistema ou aplicação, ou a encriptação de dados resultante de *ransomware*. Inclui *defacements*. *Unauthorised modification of information, e.g., by an attacker abusing stolen login credentials for a system or application, or a ransomware encrypting data. Also includes defacements.*

	Perda de Dados Data Loss	Perda de dados causada por, p. ex., falha de disco ou furto/roubo físico. Loss of data caused by, for example, hard disk failure or physical theft.
	Exfiltração de Informação Leak of Confidential Information	Exfiltração de informação, p. ex., credenciais, dados pessoais, informação interna e/ou classificada. *Leaked confidential information, e.g., credentials or personal data.*
Fraude Fraud	Utilização Indevida ou Não Autorizada de Recursos Unauthorised Use of Resources	Utilização de recursos da instituição para fins diferentes daqueles para que os mesmos foram afetos, incluindo para fins lucrativos, p. ex., o uso de e-mail para participar na obtenção de lucros ilegais através de correntes de e-mails ou esquemas de pirâmide. *Using resources for unauthorised purposes including profit-making ventures, e.g., the use of email to participate in illegal profit chain letters or pyramid schemes.*
	Direitos de Autor Copyright	Distribuição ou instalação de software comercial não licenciado ou outros conteúdos protegidos por direitos de autor (também conhecido como *Warez*). *Offering or Installing copies of unlicensed commercial software or other copyright protected materials (also known as Warez).*
	Utilização Ilegítima de Nome de Terceiros Masquerade	Tipo de ataque no qual uma entidade usa ilegalmente a identidade de outra para seu benefício. *Type of attack in which one entity illegitimately impersonates the identity of another in order to benefit from it.*

	Phishing Phishing	Entidade que se tenta passar por outra de modo a persuadir o utilizador a revelar credenciais privadas. Este IOC normalmente é um URL usado para *phishing* de credenciais do utilizador. *Masquerading as another entity in order to persuade the user to reveal private credentials. This IOC most often refers to a URL, which is used to phish user credentials.*
Vulnerabilidade Vulnerable	Criptografia Fraca *Weak Cryptography*	Serviços publicamente acessíveis permitindo criptografia fraca, p. ex., servidores *web* suscetíveis a ataques POODLE/FREAK. *Publicly accessible services offering weak cryptography, e.g., web servers susceptible to POODLE/FREAK attacks.*
	Amplificador DDoS DDoS Amplifier	Serviços publicamente acessíveis, passíveis de serem abusados para ataques DDoS de reflexão/amplificação, p. ex., servidores DNS *open-resolvers* e servidores NTP com *monlist* ativo. *Publicly accessible services that can be abused for conducting DDoS reflection/amplification attacks, e.g., DNS open-resolvers or NTP servers with monlist enabled.*
	Serviços Acessíveis Potencialmente Indesejados Potentially Unwanted Accessible Services	Serviços publicamente acessíveis eventualmente indesejados, p. ex., Telnet, RDP ou VNC. *Potentially unwanted publicly accessible services, e.g., Telnet, RDP or VNC.*
	Revelação de Informação Information Disclosure	Serviços publicamente acessíveis eventualmente revelando informação sensível, p. ex., SNMP ou Redis. *Publicly accessible services potentially disclosing sensitive information, e.g., SNMP or Redis.*

	Sistema Vulnerável Vulnerable System	Um sistema vulnerável a certos ataques, p. ex., má configuração de definições de cliente proxy (tal como WPAD), sistemas operativos desatualizados/descontinuados ou vulnerabilidades *cross-site scripting*. *A system which is vulnerable to certain attacks, e.g., misconfigured client proxy settings (such as WPAD), outdated operating system version, or cross-site scripting vulnerabilities.*
Outro Other	Sem tipo Uncategorised	Todos os incidentes que não se encaixam num dos tipos especificados devem ser colocados nesta classe, ou o incidente não é classificado. *All incidents which don't fit in one of the given categories should be put into this class or the incident is not categorised.*
	Indeterminado Undetermined	A classificação do incidente é desconhecida/indeterminada. *The categorisation of the incident is unknown/undetermined.*
Teste Test	Teste Test	Destinado a testes *Meant for testing.*

Tabela 2 - Classificação de Incidentes

4. CORRELAÇÃO ENTRE EVENTOS E INCIDENTES

Porque poderá ser necessário aplicar mecanismos de classificação automática de incidentes, apresenta-se como referência o seguinte modelo relacional (não exaustivo) entre "Tipo de Evento" e "Tipo de Incidente" (Tabela 3). Importa no entanto que esta associação não é necessariamente exclusiva (um-para-um), podendo um determinado "Tipo de Evento" estar associado a vários "Tipo de Incidente".

Tipo de Evento	Tipo Incidente	Classe de Incidente
Flood de e-mails	SPAM	Conteúdo Abusivo
Envio de mensagem não solicitada		
Publicação de informação com o objetivo de intimidar ou coagir outrem	Discurso Nocivo	
Disseminação de conteúdos proibidos por lei (crimes públicos)	Exploração Sexual de Menores, Racismo e Apologia da Violência	
Sistema(s) ou software(s) infetado(s) com *malware* permitindo acesso remoto, monitorização de atividades do sistema e recolha de informações	Sistema Infetado	Código Malicioso
Alojamento de servidor de comando e controlo	Servidor C2	
Disseminação de *malware* através de vários canais de comunicação	Distribuição de *Malware*	

Probe a sistema	Scanning	Recolha de Informação
Scan de rede		
Transferência de zona DNS		
Observação de tráfego de rede	Sniffing	
Gravação de tráfego de rede		
Ataques do tipo *CEO Fraud*	Engenharia Social	
Informação obtida através de meios não técnicos passível de ser usada em ataques futuros, p. ex., falsos telefonemas de suporte técnico (*call center support scam*)		
Tentativa de utilização de *exploit*	Exploração de Vulnerabilidade	Tentativa de Intrusão
Tentativa de SQL *Injection*		
Tentativa de XSS		
Tentativa de *File Inclusion*		
Tentativa de *brute-force*	Tentativa de *Login*	
Tentativa de password *cracking*		
Tentativa de ataque dicionário		
Tipo de ataque/*exploit* não conhecido	Nova Assinatura de Ataque	

Acesso indevido a uma interface de administração através da utilização de credenciais com acesso privilegiado	Comprometimento de Conta Privilegiada	Intrusão
Acesso indevido a uma interface de utilizador através da utilização de credenciais sem acesso privilegiado	Comprometimento de Conta Não Privilegiada	
Acesso indevido a uma rede *WiFi* usando uma conta temporária		
Acesso indevido a uma aplicação ou plataforma online	Comprometimento de Aplicação	
Execução de comandos não autorizados num sistema	Comprometimento de Sistema	
Tentativas de comprometimento de *honeypot*		
Entrada não autorizada em instalações físicas	Arrombamento	
Exploit ou ferramenta para esgotamento de recursos (rede, capacidade de processamento, sessões, etc.)	Negação de Serviço	Disponibilidade
Flood de pedidos		
Flood distribuído de pedidos	Negação de Serviço Distribuída	
Exploit ou ferramenta distribuídos para esgotamento de recursos		
Vandalismo	Sabotagem	

Disrupção intencional de mecanismos de transmissão e tratamento de dados		
Disrupção não intencional de mecanismos de transmissão e tratamento de dados	Interrupção	
Acesso indevido a sistema	Acesso Não Autorizado	Segurança da Informação
Acesso indevido à informação		
Modificação de informação	Modificação Não Autorizada	
Avaria de disco e outros suportes magnéticos	Perda de Dados	
Comprometimento de informação de caráter confidencial	Exfiltração de Informação	
Exfiltração de dados		
Comprometimento de credenciais ou dados pessoais		
Utilização indevida ou não autorizada de recursos	Utilização Indevida ou Não Autorizada de Recursos	Fraude
Distribuição ou partilha de conteúdos protegidos por direitos de autor	Direitos de Autor	
Utilização ilegítima de nome da instituição ou de terceiros	Utilização Ilegítima de Nome de Terceiros	

Disseminação de e-mails de *phishing*	Phishing	
Receção de e-mails que mascarem a sua identidade		
E-mails que visem persuadir o utilizador a efetuar uma ação p. ex., abrir um ficheiro anexo ou clicar num *link*		
E-mails que contêm *links* para sites que influenciam o utilizador a revelar informação pessoal ou credenciais		
E-mails relacionados com a disseminação de *malware*		
Agregação de informação recolhida em esquemas de *phishing*		
Utilização de mecanismos de cifra considerados inseguros	Criptografia fraca	Vulnerabilidade
Servidor NTP configurado com *monlist*	Amplificador DDoS	
Servidor DNS configurado para responder a pedidos do tipo ANY/ALL		
Serviços inadvertidamente expostos, p. ex., RDP, SSH, Telnet, FTP, etc.	Serviços acessíveis potencialmente indesejados	
Documentos internos acessíveis em partilha pública	Revelação de Informação	
Sistema com atualizações/correções de segurança em falta	Sistema vulnerável	

Tabela 3 - Relação não exaustiva entre Tipos de Evento e Tipos de Incidente

5. MÚLTIPLAS CLASSIFICAÇÕES

Um evento pode dar origem a um ou mais incidentes suscetíveis de se enquadrarem em uma ou várias classificações. Por exemplo, um incidente pode envolver várias tentativas de login ("Tentativa de Intrusão - Tentativa de login") com o objetivo primário de obter acesso não autorizado à informação ("Segurança da Informação - Acesso não autorizado").

A ordenação das Classes/Tipos de incidentes, na tabela 2, não reflete qualquer prioridade na sua utilização em casos de múltiplas classificações possíveis.

Quando várias classificações são aplicáveis, a classificação primária de um incidente é a intenção do atacante (objetivo primário), enquanto a classificação secundária pode ser o meio, ou o mecanismo de transporte, usado para concretizar o ataque (objetivos secundários). Para o exemplo acima, o "Acesso não autorizado" é a classificação primária (objetivo primário) e "Tentativa de login" seria a classificação secundária (objetivo secundário).

Fazendo a ponte com a Unified Kill Chain[1], a classificação primária será a ação sobre os objetivos. As classificações secundárias serão os objetivos secundários (e não todos os TTP identificados) para materializar o acesso inicial ou para movimentações laterais/propagação na rede.

A interpretação acima não invalida que, caso se justifique, o evento ou report dê origem a vários incidentes, onde cada incidente trata cada uma das diferentes etapas, seja porque a ferramenta não suporte múltiplas classificações ou porque se considere importante registar os dois incidentes em separado.

De igual forma, as equipas que não consigam introduzir múltiplas classificações poderão optar pela reclassificação durante a investigação sendo que o valor final no encerramento deverá ser relativo à intenção do atacante (objetivo primário).

Para manter coerência na Rede, sobre as estatísticas produzidas, a classificação final de um incidente que envolva mais que um Membro, deverá ser consistente entre os Membros envolvidos, devendo o Membro que alterar a classificação, comunicar essa alteração aos restantes (envolvidos no tratamento desse incidente).

[1] https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

6. ILÍCITOS CRIMINAIS

A notificação de incidentes ao Centro Nacional de Cibersegurança não se substitui à comunicação às autoridades judiciais ou aos órgãos de polícia criminal competentes, quando esses incidentes configuram também um ilícito cujo procedimento penal implique ou obrigue a queixa ou dependa de acusação particular.

Registe-se que nos casos em que o incidente possa configurar um crime público, as entidades policiais e os funcionários públicos estão obrigados a denunciá-los sempre que tenham conhecimento destes no exercício de funções[2].

[2] https://www.ministeriopublico.pt/faq/o-que-e-um-crime-publico

7. LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

- **C2** - Command and Control
- **CNCS** - Centro Nacional de Cibersegurança
- **CSIRT** - Computer Security Incident Response Team
- **DoS** - Denial of Service
- **DDoS** - Distributed Denial of Service
- **DNSSEC** - Domain Name System Security Extensions
- **FREAK** - Factoring RSA Export Keys
- **FINGERD** - Finger user information protocol daemon
- **FTP** - File Transfer Protocol
- **ICMP** - Internet Control Message Protocol
- **IOC** - Indicator of compromise
- **KSK** - Key signing key
- **NTP** - Network Time Protocol
- **POODLE** - Padding Oracle On Downgraded Legacy Encryption
- **RDP** - Remote Desktop Protocol
- **SMTP** - Simple Mail Transfer Protocol
- **SNMP** - Simple Network Management Protocol
- **SPAM** - Sending and Posting Advertisement in Mass
- **SSH** - Secure Shell

- **TELNET** - Teletype Over Network Protocol
- **UDP** - User Datagram Protocol
- **URI** - Uniform Resource Identifier
- **URL** - Uniform Resource Locator
- **WPAD** - Web Proxy Autodiscovery Protocol

8. LISTA DE TERMOS

- **evento** - ocorrência identificável, com um efeito potencialmente adverso na segurança das redes e dos sistemas de informação.
- **incidente -** um evento com um efeito adverso real na segurança das redes e dos sistemas de informação.
- **Log** - um registo da atividade que ocorre nos sistemas de informação e comunicação, de uma organização.
- **malware** - software ou firmware destinado a executar um processo não autorizado que terá um impacto adverso na confidencialidade, integridade ou disponibilidade de um sistema de informação.
- **monlist** - comando que permite recolher informação de monitorização de tráfego do serviço NTP
- **proxy** - software que recebe um pacote de rede de um cliente e envia o mesmo em nome do cliente para o destino desejado.
- **syslog** - um protocolo que especifica um formato geral de introdução e um mecanismo de transporte de logs.
- **timestamp** - uma sequência de caracteres ou informações codificadas que identificam quando um determinado evento ocorreu, fornecendo geralmente a data, a hora do dia, e por vezes são precisas até à fração de segundo.
- **warez** - termo cultural global referente a software pirateado que é distribuído pela Internet.
- **exploit kit** - ferramenta usada para implantar e comandar a exploração automática de vulnerabilidades em sistemas remotos. Os exploit kits permitem a um ator malicioso disseminar malware sem necessidades de conhecimentos avançados sobre as vulnerabilidades em exploração.
- **CSIRT** - Computer Security Incident Response Team (também, por vezes, referenciado como CERT - Computer Emergency Response Team) é uma unidade organizacional especializada, responsável pela resposta a incidentes de cibersegurança. Estas equipas são responsáveis pela

deteção, análise, mitigação e resolução de ameaças e incidentes de segurança de acordo com a sua missão.

9. AGRADECIMENTOS

Esta revisão da Taxonomia Comum da Rede Nacional de CSIRT, é resultado dos trabalhos desenvolvidos pelo Grupo de Trabalho da Taxonomia instituído pela Rede para a revisão da taxonomia. Elaborado com base num documento prévio, importa atribuir os devidos agradecimentos aos autores desse documento e de outros que eventualmente lhes tenham antecedido.

É também reconhecida a disponibilidade dos Membros do Grupo de Trabalho, que através do empenho dos seus representantes, permitiram incorporar valiosos contributos nos trabalhos e atingir com sucesso os resultados propostos.

O Grupo de Trabalho da Taxonomia, que produziu o presente documento, era constituído pelos Membros (por ordem alfabética):

- **COORDENAÇÃO:**
  - CSIRT.UMINHO
- **MEMBROS**:
  - CERT.PT
  - COCIBER - EMGFA
  - CSIRT.UPORTO
  - EDP CSIRT
  - EURONEXT CSIRT
  - LAYER8 CSIRT
  - RCTS CERT
  - OUTSYSTEMS CSIRT