Taxonomia Comum da Rede Nacional de CSIRT

Taxonomia Comum da Rede Nacional de CSIRT

Versão:

3.0

(ENISA / TF-CSIRT RSTI WG v.1002)

Autor:

Grupo de Trabalho - Taxonomia

Revisão:

Grupo de Trabalho - Taxonomia

Janeiro de 2020

Classificação	Data	Versão do documento
TLP:WHITE	Janeiro 2020	3.0

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

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 deste documento. Como base para esta revisão este Grupo de Trabalho (GT) teve em consideração a Taxonomia de referência do Working Group – RSIT WG[1] [2].

1 https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force
2 https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/reference-security-incident-taxonomy-working-group-2013-rsit-wg

2 CLASSIFICAÇÃO DE INCIDENTES

A classificação de incidentes deverá ser feita de acordo com 2 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 para a 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 email	Malware anexado a mensagem ou presença de link para URL malicioso em mensagem de correio eletrónico.
Alojamento de malware em página web	Página web que se encontra a disseminar um dos vários tipos de malware.
Alojamento de servidor de 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 roubados 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 efectua 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 efectua 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, emails, etc.), a partir de uma única fonte, a um determinado serviço com o objectivo de afectar o seu funcionamento.
Exploit ou ferramenta para esgotamento de recursos (rede, capacidade processamento, sessões, etc…)	Utilização, a partir de uma única fonte, de software especialmente concebido para afectar 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, emails, etc.), a partir de várias fontes, a um determinado serviço com o objectivo de afectar o seu funcionamento.
Exploit ou ferramenta distribuídos para esgotamento de recursos	Utilização, a partir de várias fontes, de software especialmente concebido para afectar o funcionamento de um determinado serviço através da exploração de uma vulnerabilidade no mesmo.
Vandalismo	Actividades lógicas e físicas que não tenham como objectivo 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	Actividades lógicas e físicas que tenham como objectivo premeditado 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 objectivo de identificar sistemas que estejam activos nessa mesma rede.
Transferência zona DNS	Transferência não autorizada de uma determinada zona de DNS.

Wiretapping	Intercepção lógica ou física de comunicações.
Disseminação de emails de phishing	Envio massivo de emails com o objectivo de recolher dados para efeitos de Phishing das vítimas.
Alojamento de sites de phishing	Alojamento de sites web 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 electrónico, 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 brute-force	Tentativa de Login, sem sucesso, em sistema através da utilização de credenciais sequenciais de acesso.
Tentativa de password cracking	Tentativa de descoberta de credenciais de acesso através da quebra dos mecanismos criptográficos que os 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 afectos.
Utilização ilegítima de nome da instituição ou de terceiros	Utilização de nome da instituição sem autorização da mesma.
Flood de emails	Envio de número anormalmente elevado de mensagens de correio electrónico.
Envio de mensagem não solicitada	Envio de mensagem de correio electrónico não solicitada ou 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.

A ordenação da tabela não reflecte prioridade em casos de múltiplas classificações possíveis para um incidente. A classificação final de um incidente reflectirá a severidade, que poderá variar entre incidentes idênticos, conforme o Membro.

Nesse sentido, e para manter coerência na Rede sobre as estatísticas produzidas, a classificação final de um incidente que envolva mais que um Membro, deverá ser igual entre os Membros envolvidos, devendo o Membro que alterar a classificação, comunicar essa alteração a todos os Membros envolvidos no tratamento desse incidente.

3 TAXONOMIA DE REFERÊNCIA PARA INCIDENTES DE SEGURANÇA [V3.0]

REFERENCE SECURITY INCIDENT TAXONOMY [ENISA V.1002]

Classe de Incidente ***Classification***	**Tipo de Incidente** ***Incident Examples***	**Descrição / Exemplos** ***Description / Examples***
Conteúdo Abusivo *Abusive Content*	Spam *Spam*	Spam ou “email 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 colecção maior de mensagens, todas com conteúdo funcionalmente comparável. Este IOC refere-se a recursos da infra-estrutura de SPAM, tais como verificadores e/ou colectores de endereços, URL em emails 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 a SPAM infrastructure, be it a harvesters like address verification, URLs in spam e-mails etc.*
	Discurso Nocivo *Harmful Speech*	Individualização ou discriminação de alguém, p. ex. através de ciber perseguição, racismo ou ameaças, contra um ou mais indivíduos. *Discretization 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 *(Child) Sexual Exploitation/Sexual /Violent Content*	Exploração Sexual de Menores, conteúdo sexual, glorificação da violência, e outros conteúdos proibidos por lei. *Child Sexual Exploitation (CSE), Sexual content, glorification of violence, etc.*

Código Malicioso *Malicious Code*	Sistema Infectado *Infected System*	Sistema infectado com malware, p. ex. PC, smartphone ou servidor infectados com um rootkit. Na maioria das vezes, refere-se a ligações a um servidor C2 "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 C2 server*
	Servidor C2 *C2 Server*	Servidor de comando e controlo contactado por malware em sistemas infectados. *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 factura falsa, distribuída via spam de malware. *URI used for malware distribution, e.g. a download URL included in fake invoice malware spam.*
	Configuração de Malware *Malware Configuration*	URI de alojamento de ficheiro de configuração de malware, p. ex. código web para injecção 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. Exemplos: fingerd, consultas DNS, ICMP, SMTP (EXPN, RCPT, etc.), 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. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.*
	Sniffing *Sniffing*	Observação e/ou gravação de tráfego de rede (intercepção). *Observing and recording of network traffic (wiretapping).*

	Engenharia Social *Social Engineering*	Recolha de informações de um ser humano através de meios não técnicos (por exemplo, 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.: "buffer overflow", "backdoor", "cross site scripting", etc.) *An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.)*
	Tentativa de *login* *Login attempts*	Múltiplas tentativas de login (adivinha, quebra ou *bruteforcing* de passwords). Este IOC refere-se a um recurso que foi observado a executar um ataque de força bruta sobre um determinado protocolo aplicacional. *Multiple login attempts (Guessing / cracking of passwords, brute force). 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*	Compromisso de Conta Privilegiada *Privileged Account Compromise*	Compromisso de um sistema em que o atacante ganhou privilégios de administração. *Compromise of a system where the attacker gained administrative privileges.*
	Compromisso de Conta Não Privilegiada *Unprivileged Account Compromise*	Compromisso de um sistema usando uma conta não privilegiada (utilizador/serviço). *Compromise of a system using an unprivileged (user/service) account.*

	Compromisso de Aplicação *Application Compromise*	Compromisso de uma aplicação/software através de vulnerabilidades (des)conhecidas, p. ex. *SQL injection*. *Compromise of an application by exploiting (un-)known software vulnerabilities, e.g. SQL injection.*
	Arrombamento *Burglary*	Intrusão física, p. ex. no edifício da entidade ou no datacenter. *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 para uma aplicação web, especialmente concebidos para provocarem 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. *SYN-Flood* ou ataques de reflexão/amplificação. *Distributed Denial of Service attack, e.g. SYN-Flood or UDP-based reflection/amplification attacks.*
	Configuração incorreta *Misconfiguration*	Configuração incorrecta de software que resulta em problemas de disponibilidade de serviço, p. ex. um servidor DNS com a DNSSEC KSK da zona raiz, desactualizada. *Software misconfiguration resulting in service availability issues, e.g. DNS server with outdated DNSSEC Root Zone KSK.*
	Sabotagem *Sabotage*	Sabotagem física, p. ex. corte de cabos ou fogo posto. *Physical sabotage, e.g cutting wires or malicious arson.*
	Interrupção *Outage*	Interrupção provocada p. ex. por falha de ar condicionado ou desastre natural. *Outage caused e.g. by air condition failure or natural disaster.*

Segurança da Informação *Information Content Security*	Acesso não autorizado *Unauthorised access to information*	Acesso não autorizado à informação, p. ex. o abuso de credenciais roubadas para acesso a um sistema ou aplicação, intercepção 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*. *Unauthorised modification of information, e.g. by an attacker abusing stolen login credentials for a system or application or a ransomware encrypting data.*
	Perda de dados *Data Loss*	Perda de dados, p. ex. falha de disco rígido ou furto/roubo. *Loss of data, e.g. caused by harddisk failure or physical theft.*
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 afectos, 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 e-mail 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 (Warez). *Offering or Installing copies of unlicensed commercial software or other copyright protected materials (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 crypto*	Serviços publicamente acessíveis permitindo criptografia fraca, p. ex. servidores web susceptíveis a ataques POODLE/FREAK. *Publicly accessible services offering weak crypto, 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. open-resolvers DNS e servidores NTP com “monlist” activo. *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 (ex.: WPAD), sistemas operativos desactualizados, etc. *A system which is vulnerable to certain attacks. Example: misconfigured client proxy settings (example: WPAD), outdated operating system version, etc.*
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, sugere-se como referência o seguinte modelo relacional entre "Tipo de Evento" e "Tipo de Incidente". Importa, no entanto, que esta associação não é estrita, podendo um determinado Tipo de Evento estar associado a qualquer Tipo de Incidente.

Tipo de Evento	**Tipo Incidente**	**Classe de Incidente**
Flood de emails	SPAM	Conteúdo Abusivo
Envio de mensagem não solicitada		
Publicação de informação com o objectivo 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) infectado(s) com malware permitindo acesso remoto, monitorização de actividades do sistema e recolha de informações	Sistema Infectado	Código Malicioso
Alojamento de servidor C2	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 zona DNS		
Wiretapping	Sniffing	

Informação obtida através de meios não técnicos passível de ser usada em ataques futuros	Engenharia Social	
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		
Furto de credenciais de acesso privilegiado	Compromisso de Conta Privilegiada	Intrusão
Furto de credenciais de acesso	Compromisso de Conta Não Privilegiada	
Entrada não autorizada em instalações físicas	Arrombamento	
Exploit ou ferramenta para esgotamento de recursos (rede, capacidade 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 e sistema	Acesso não autorizado	Segurança da Informação
Acesso indevido à informação		
Exfiltração de dados		
Modificação de informação	Modificação não autorizada	
Eliminação de informação	Perda de dados	
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 emails de phishing	Phishing	
Alojamento de sites de phishing		
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	
RDP exposto	Serviços acessíveis potencialmente indesejados	
Documentos internos acessíveis em partilha pública	Revelação de Informação	

Sistema sem actualizações/correcções de segurança.	Sistema vulnerável	

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

5 LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

- C2 - Command and Control
- CNCS - Centro Nacional de Cibersegurança
- CSIRT - Computer Security Incident Response Team
- DDoS - Distributed Denial of Service
- DNSSEC - Domain Name System Security Extensions
- IOC - Indicator of compromise
- KSK - Key signing key
- NTP - Network Time Protocol
- OS - Operating System
- RDP - Remote Desktop Protocol
- SIEM - Security Information and Event Management
- SMTP - Simple Mail Transfer Protocol
- SNMP - Simple Network Management Protocol
- SOC - Security Operations Center
- SPAM - Sending and Posting Advertisement in Mass
- SSH - Secure Shell
- SSL - Secure Sockets Layer
- URI - Uniform Resource Identifier
- URL - Uniform Resource Locator
- VNC - Virtual Network Computing
- VPN - Virtual Private Network
- WPAD - Web Proxy Autodiscovery Protocol

6 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 actividade 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 fracção de segundo
- Warez - termo cultural global referente a software pirateado que é distribuído pela Internet

7 AGRADECIMENTOS

Esta revisão da Taxonomia Comum da Rede Nacional de CSIRT, é resultado dos trabalhos desenvolvidos pelo Grupo de Trabalho da Taxonomia (GT) 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 GT, que através do empenho dos seus representantes, permitiram incorporar valiosos contributos nos trabalhos e atingir os resultados propostos com sucesso. O GT, à data deste documento, era constituído pelos Membros (por ordem alfabética):

- Coordenação
  - CSIRT.UMINHO
- Membros
  - CERT.PT
  - CSIRT.UA
  - CSIRT.UPORTO
  - CSIRT.UTAD
  - CSIRT-EY
  - DGS-IRT
  - EDP CSIRT
  - Euronext CSIRT
  - LAYER8 CSIRT
  - RCTS CERT
- Observadores
  - PJ UNC3T