



Resposta a Incidentes e Análise Forense

TLP:AMBER



O que é um CERT/CSIRT?

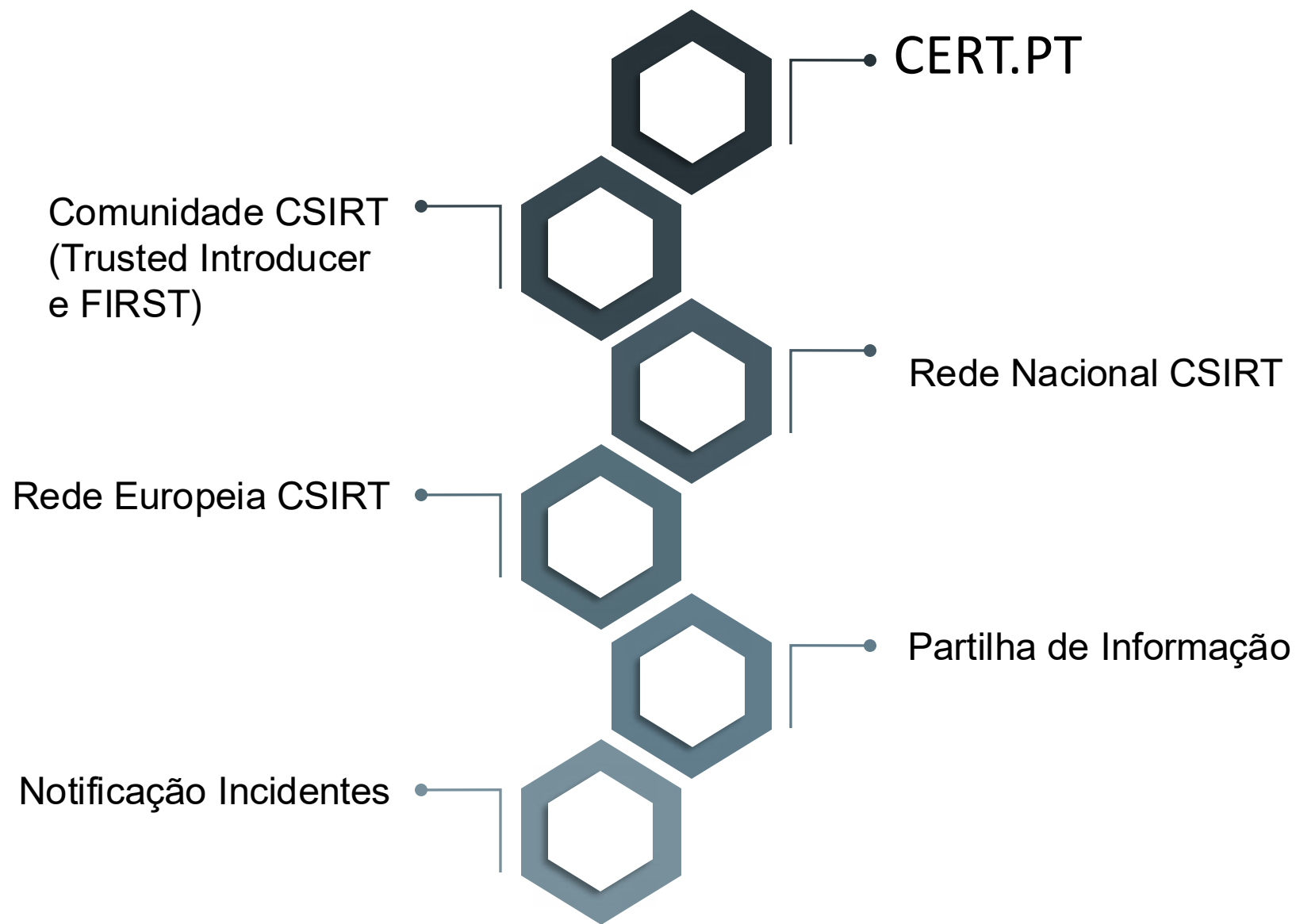
A Lei n.º 46/2018, de 13 de agosto estabeleceu a obrigatoriedade de existência de 'Equipas de resposta a Incidentes de Segurança Informática' em todos os Estados Membros da União Europeia.

O CERT.PT é a Equipa de Resposta a Incidentes de Cibersegurança do Centro Nacional de Cibersegurança.

Consiste numa equipa especializada em segurança informática que tem como objetivo tratar de uma forma eficiente todas as situações perigosas que ocorrem em sistemas de computadores (chamados de "Incidentes").



Ecosistema



Serviços Prestados

- Coordenação de Resposta a Incidentes
- Support On-Site
- Identificação de Vulnerabilidades
- Alertas



Estes serviços são assegurados 24 horas por dia, todos os dias.

Comunidades Servidas

- Administração Pública
- Operadores de Infraestruturas Críticas
- Operadores de Serviços Essenciais
- Prestadores de Serviços Digitais
- Restante Ciberespaço de Interesse Nacional



Serviços prestados e Comunidades Servidas

	Coordenação de Resposta a Incidentes	Suporte On-site	Alertas Identificação de Vulnerabilidades
Administração Pública 			
Operadores de Serviços Essenciais 			
Prestadores de Serviços Digitais 			
Restante Ciberespaço de Interesse Nacional 			

Áreas CERT.PT

Resposta a Incidentes e *Cyber Threat Intelligence*

Duas áreas de atuação do CERT.PT

Resposta a Incidentes



Gestão da
Resposta a
Incidentes

Cyber Threat Intelligence (CTI)



Análise de
informação



Cyber Threat Intelligence (CTI)



Identificar ameaças associadas ao Ciberespaço de interesse Nacional.

Após identificação de evidências, partilha de informação com a Equipa de Resposta a Incidentes.

Identificar padrões ou tipologias comuns entre incidentes/observáveis.

Após identificação partilha com todos os interessados (ex: Protocolos ou RNCSIRT).

Ter indicadores dos Incidentes e Observáveis tratados pelo CERT.PT.

Partilha para o Observatório, Cyberweather e outros fóruns quando requisitado.

Resposta a Incidentes (RI)

Melhorar a eficácia geral da reação a incidentes de cibersegurança em Portugal, facilitando a partilha de informação relevante, coordenando ações de mitigação e de resolução junto das diversas entidades implicadas e articulando com as restantes autoridades, nacionais e internacionais.

<https://www.cncs.gov.pt/pt/certpt/coordenacao-da-resposta-a-incidentes/>



Definição de incidente

Um evento com um efeito adverso real na segurança das redes e dos sistemas de informação.



Que tipo de incidentes um CERT/CSIRT trata?



Taxonomia

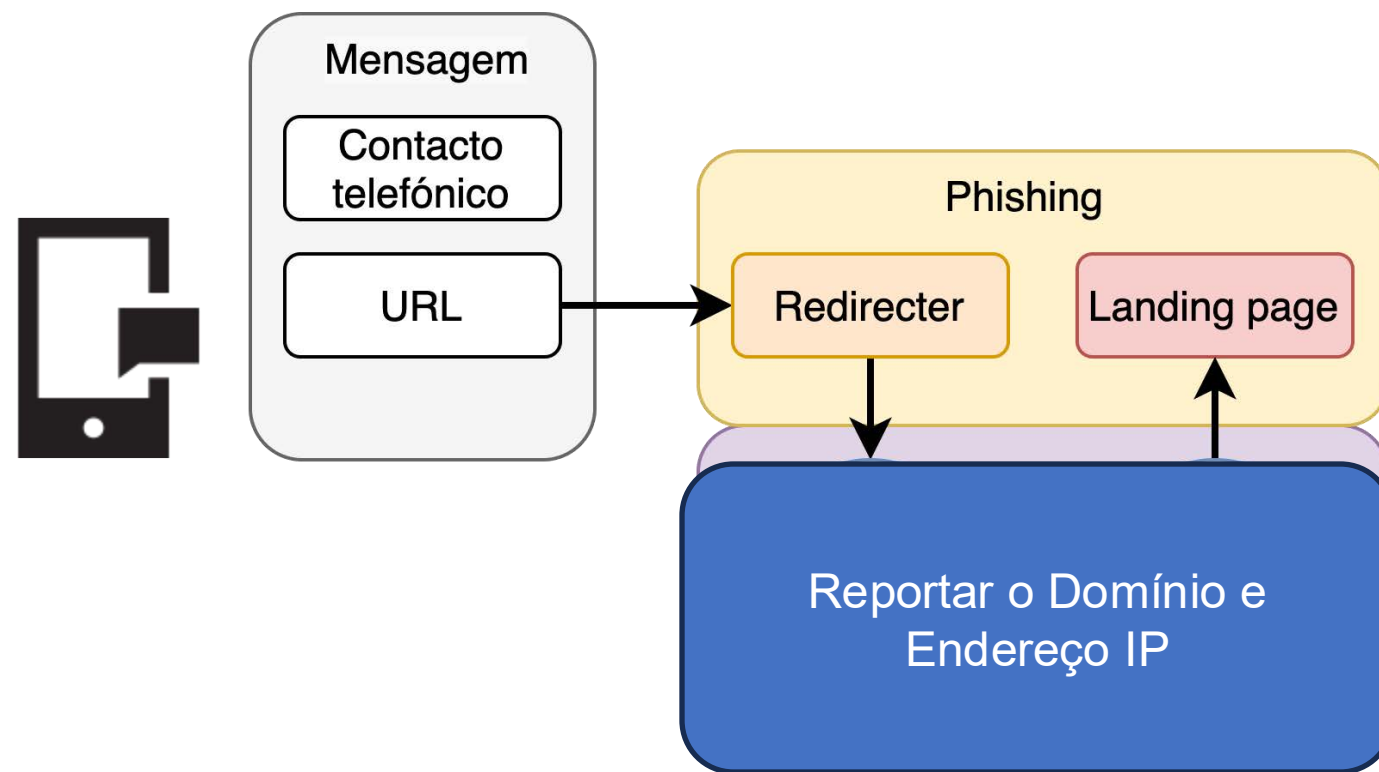
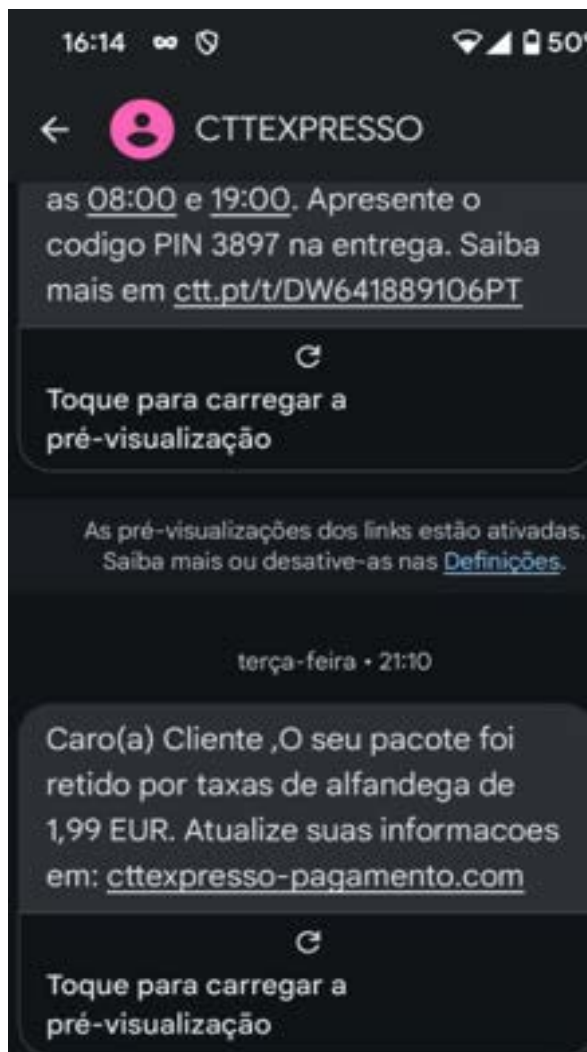
Classe Incidente	Tipo Incidente
Código Malicioso	Sistema Infetado
	Distribuição de Malware
	Servidor C2
	Configuração de Malware
Disponibilidade	Negação de Serviço
	Negação de Serviço Distribuída
	Configuração incorreta
	Sabotagem
	Interrupção
Recolha de Informação	Scanning
	Sniffing
	Engenharia Social
Intrusão	Comprometimento de Conta Privilegiada
	Comprometimento de Conta Não Privilegiada
	Comprometimento de Aplicação
	Comprometimento de Sistema
	Arrombamento

[https://www.cnccs.gov.pt/docs/taxonomia-cnccs.pdf](https://www.cncs.gov.pt/docs/taxonomia-cnccs.pdf)

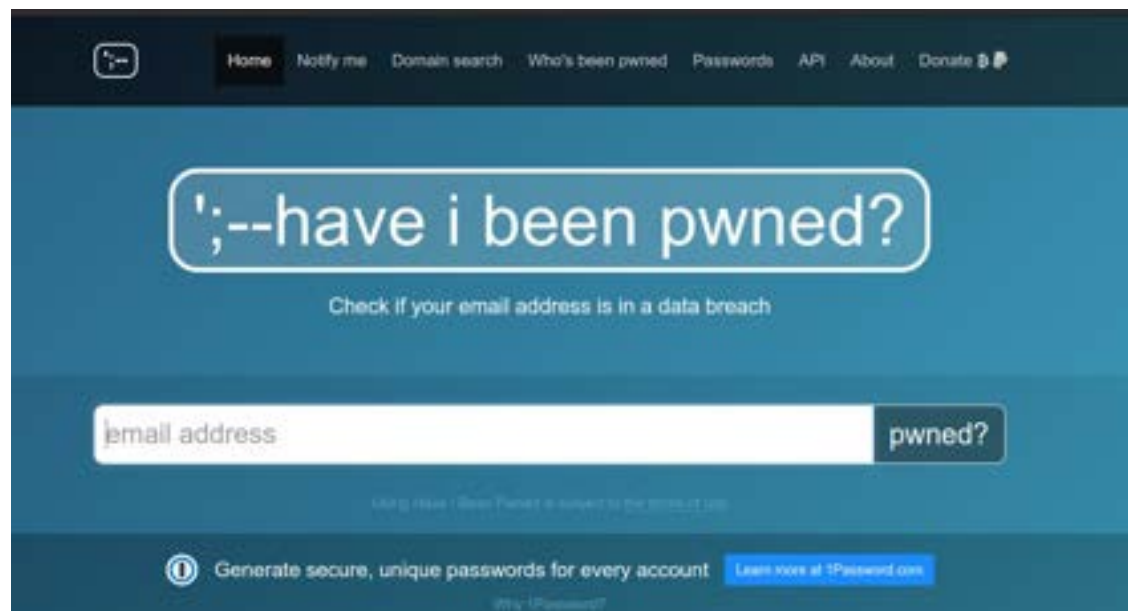
https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.3.pdf

Classe Incidente	Tipo Incidente
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
	Exfiltração de Informação
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

Smishing



Comprometimento de Conta (Não) Privilegiada



Incidentes através de informação que é partilhada connosco.

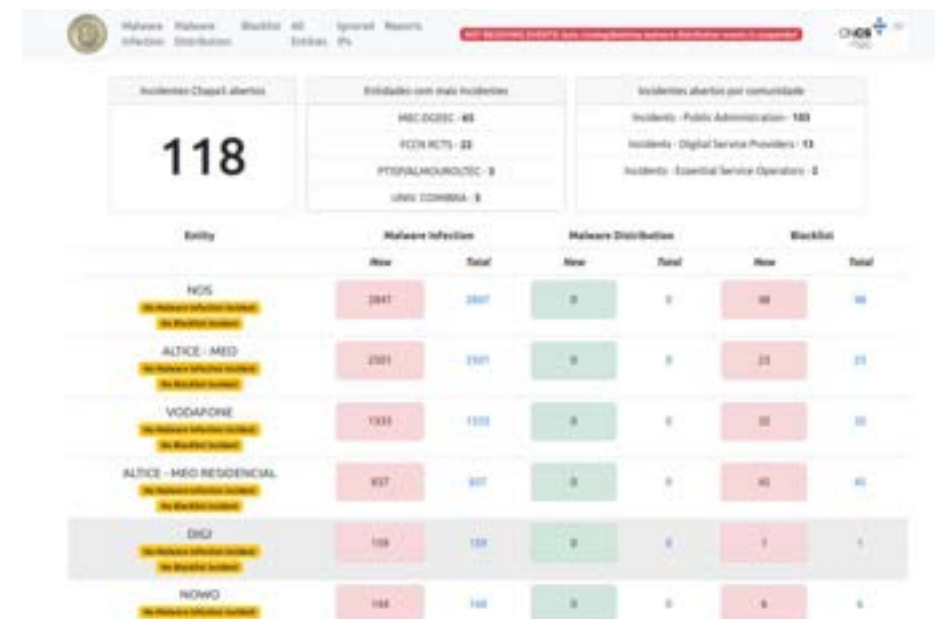
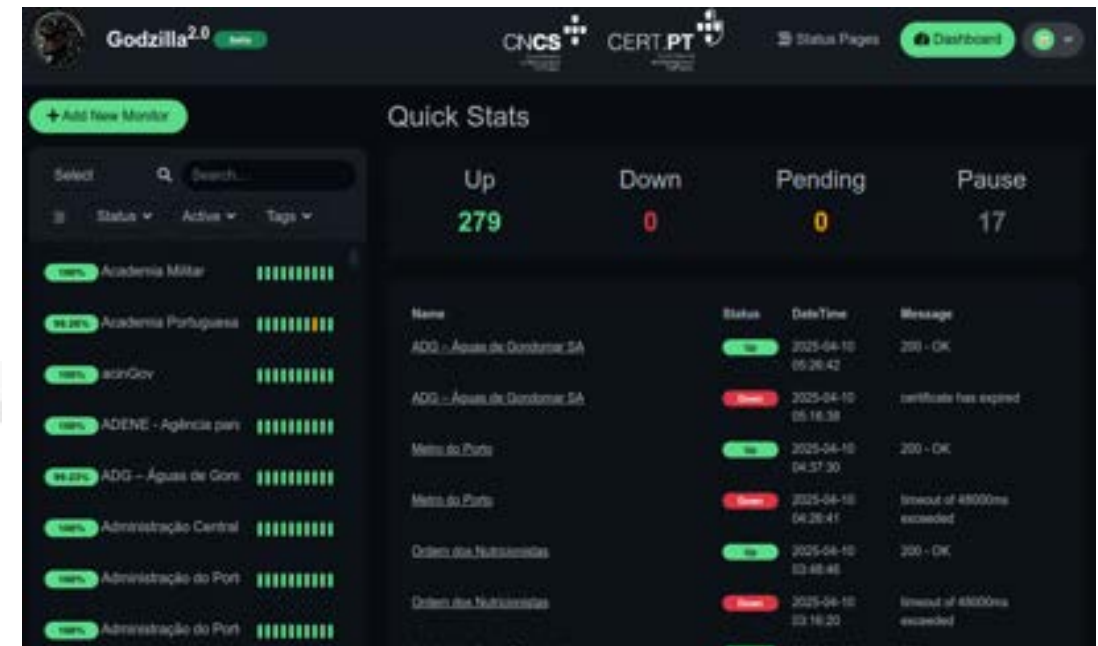
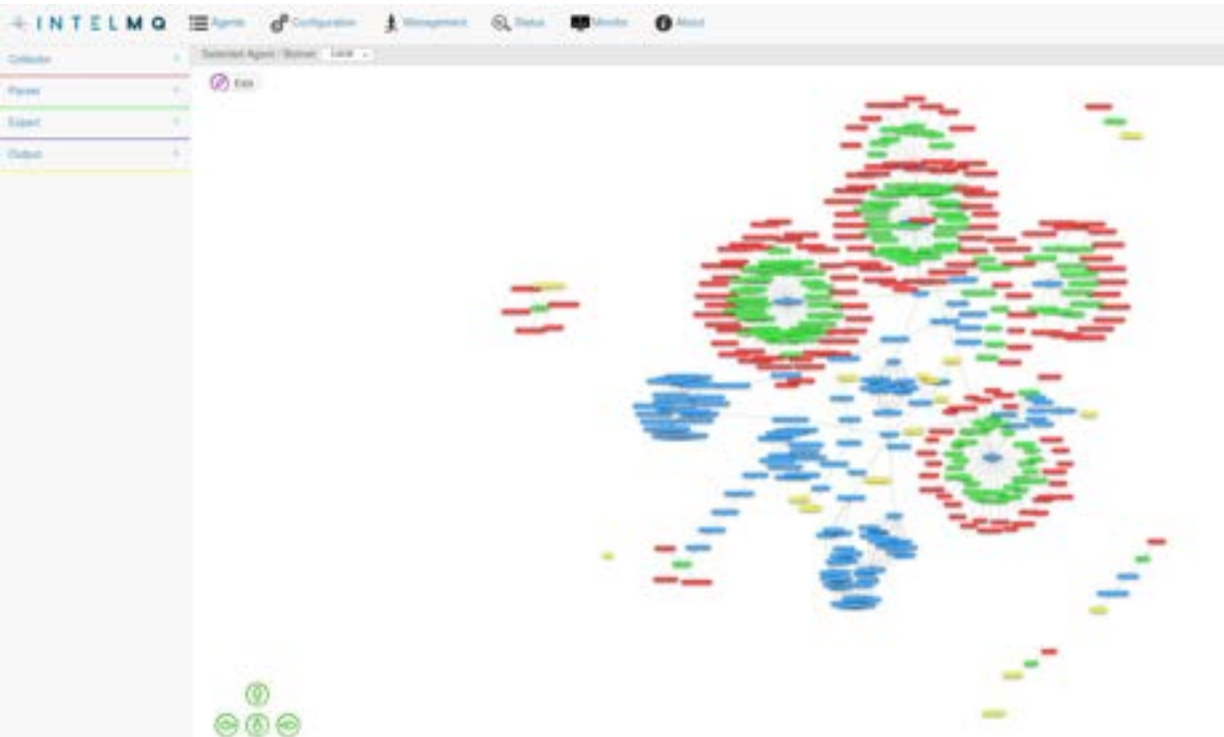
Ex: Entidade A recebe email de phishing de conta comprometida da entidade B.

Medidas Preventivas

Entidades

- Redes resilientes
- Visibilidade
- Políticas de boas práticas, ex: passwords robustas, permissões diferentes para os utilizadores, etc
- Utilização de MFA
- Manter o software atualizado
- Segregação da rede
- Uso de anti-vírus e EDR (deteção e resposta de endpoint)

Ferramentas



Cooperação



Análise Forense

TLP:RED

Taxonomia

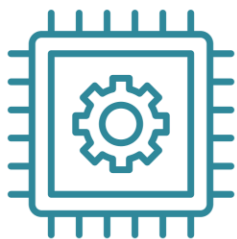
Classe Incidente	Tipo Incidente
Código Malicioso	Sistema Infetado
	Distribuição de Malware
	Servidor C2
	Configuração de Malware
Disponibilidade	Negação de Serviço
	Negação de Serviço Distribuída
	Configuração incorreta
	Sabotagem
	Interrupção
Recolha de Informação	Scanning
	Sniffing
	Engenharia Social
Intrusão	Comprometimento de Conta Privilegiada
	Comprometimento de Conta Não Privilegiada
	Comprometimento de Aplicação
	Comprometimento de Sistema
	Arrombamento

Classe Incidente	Tipo Incidente
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
	Exfiltração de Informação
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

Processo de Análise Forense



Aquisição Digital



Cópia Física

Device to Device: Cópia bit-a-bit do dispositivo original para outro dispositivo previamente limpo de igual ou superior capacidade de armazenamento.

Device to File: Criação de um ou mais ficheiros que contenham, ligados entre si, a imagem idêntica do dispositivo original.



Cópia Lógica

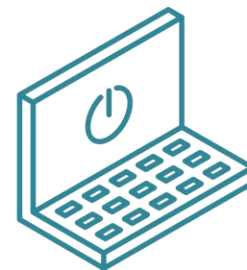
Adquirir o conteúdo de um volume em concreto, de diretorias ou de ficheiros.

Possíveis Cenários de Aquisição Digital



Dead Box Forensics

Encontramos este cenário quando o computador se encontra desligado. Jamais se deve ligar o computador.



Live Data Forensics

Encontramos este cenário quando o computador se encontra ligado. Jamais se deve desligar o computador, exceto em casos em que existe *software* de destruição de dados a correr.



Cenário Virtualizado

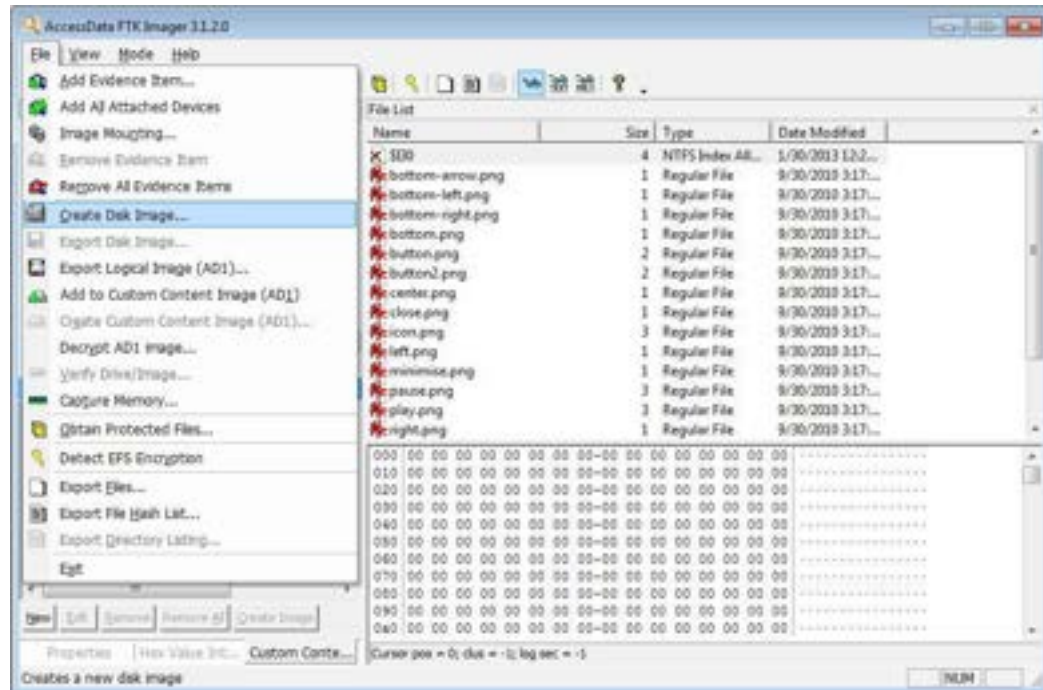
Os sistemas virtualizados devem ser isolados da restante rede, suspensas e ainda deve tirar-se um snapshot das máquinas para que o disco rígido e todos os vestígios sejam preservados num ficheiro separado.



Volumes Cifrados

Quando um dispositivo que se encontra cifrado for envolvido num incidente, procede-se, de qualquer forma, à aquisição da cópia forense para um dispositivo esterilizado, utilizando uma *penbootable*.

Ferramentas de Aquisição Digital



Processamento



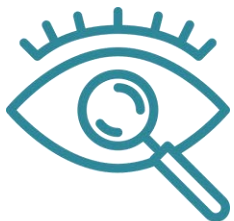
KAPE
(Kroll Artifact Parser And Extractor)

Análise



Análise Automatizada

Realizada através de ferramentas de triagem que assinalam eventos potencialmente suspeitos.



Análise Manual

Realizada após obtermos toda a informação das ferramentas automatizadas, com o objetivo de selecionar os verdadeiros positivos, construir uma timeline, e perceber o workflow do ataque.

Análise Automatizada



Antivírus



THOR APT Scanner



Hayabusa



Eric Zimmerman's
TOOLS



Análise Manual



timesketch
Digital Forensics Timeline Analysis



IRIS

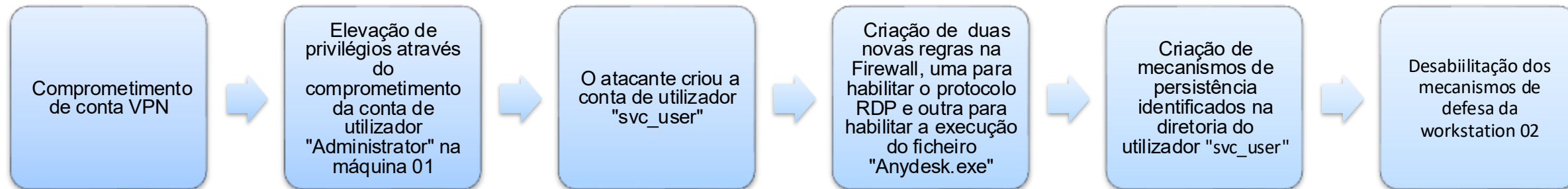
log2timeline/plaso

Super timeline all the things

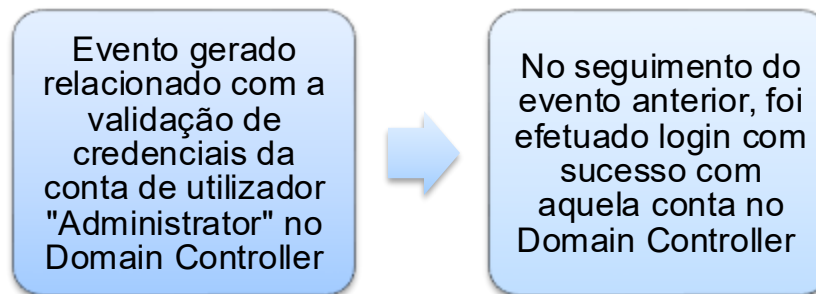


Caso Prático

30 de novembro

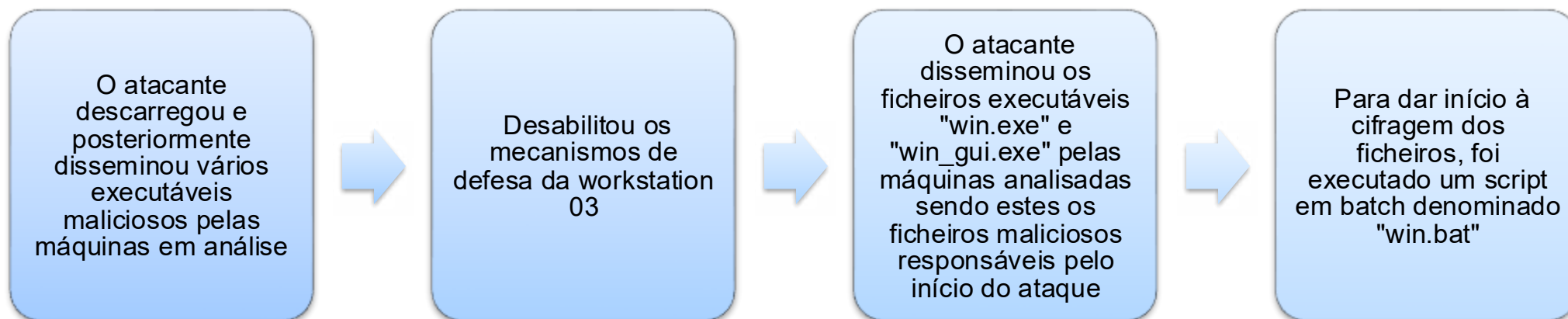


01 de dezembro



Caso Prático

02 de dezembro



E-mail: cert@cert.pt

Telefone: (+351) 210 497 399

Formulário website CNCS: <https://www.cncs.gov.pt/pt/notificacao-incidentes/>

LinkedIn CNCS: <https://pt.linkedin.com/company/centro-nacional-de-ciberseguran%C3%A7a---portuguese-national-cybersecurity-centre>



Catarina Silva

CERT.PT

Centro Nacional de Cibersegurança
Rua da Junqueira, 69 | 1300-342 Lisboa
cncs@cncs.gov.pt | (+351) 210 497 400