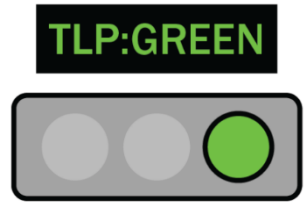


RNEP-GW

MÓDULO TAXONOMIA

fct csirt

RNEP-GW

TAXONOMIA

Classificar incidentes de segurança informática

Necessidade de existência de um referencial comum a todas as equipas

Desenvolvida no âmbito de um Grupo de Trabalho da Rede Nacional CSIRT

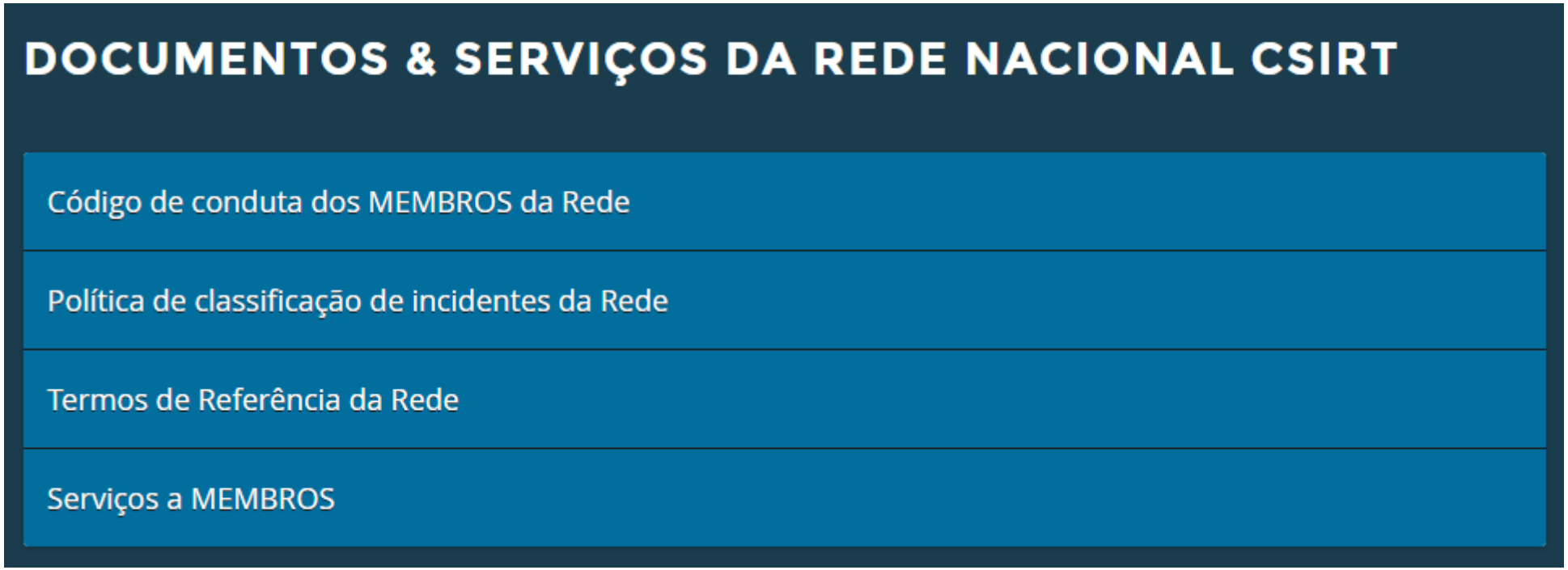
TAXONOMIA

Dezembro de 2023

Versão 3.3

Disponível em:
https://redecsirt.pt/files/RNCSIRT_Taxonomia_v3.3.pdf

REDE NACIONAL CSIRT



https://redecsirt.pt

TAXONOMIA (ENISA)

Janeiro de 2018

Disponível em:

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

TAXONOMIA (EM USO PELA RNCSIRT)

Classes de Incidentes

Tipos de Incidentes

TAXONOMIA: CLASSES

Conteúdo Abusivo

Código Malicioso

Recolha de Informação

Tentativa de Intrusão

Intrusão

Disponibilidade

Segurança da Informação

Fraude

Vulnerabilidade

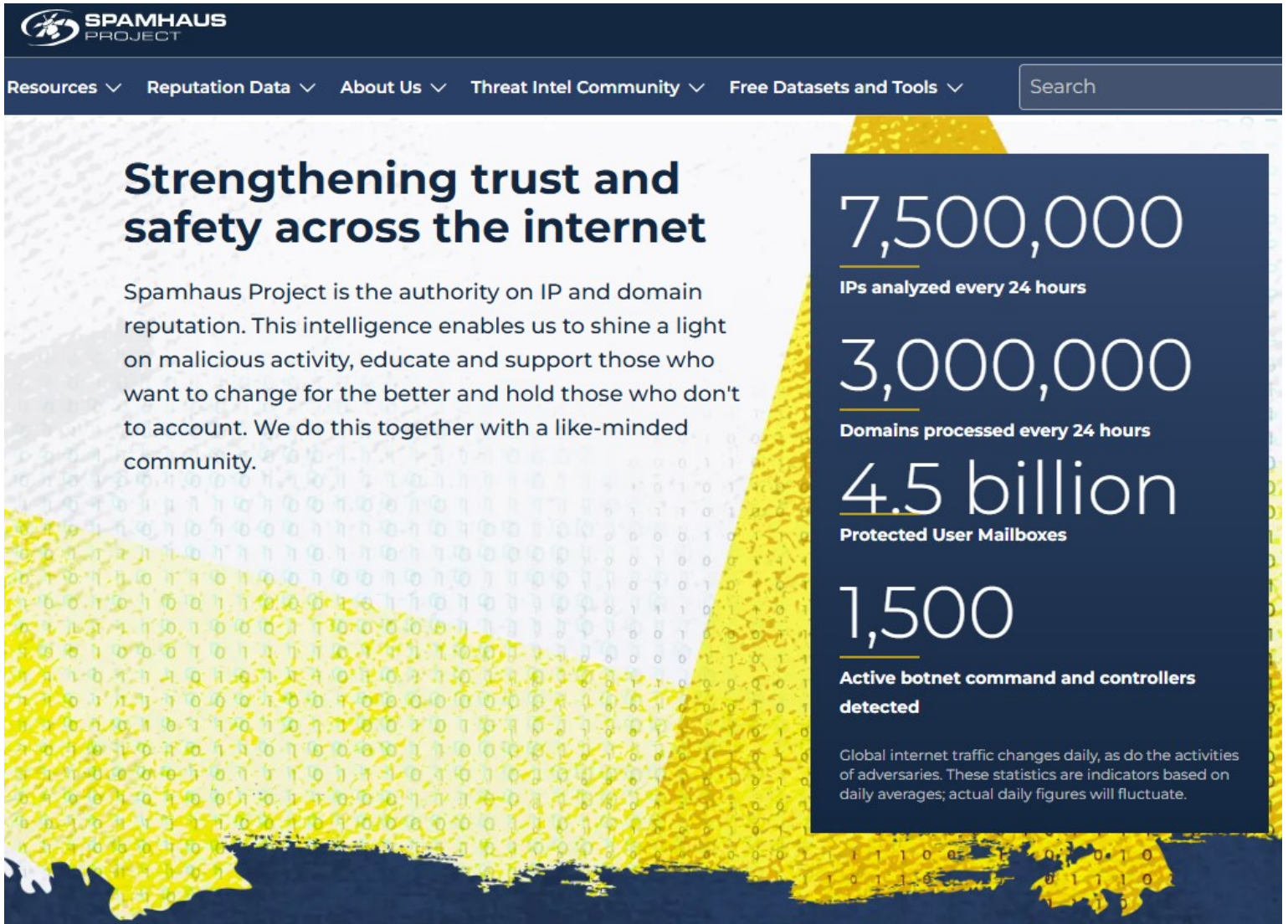
Outro

Teste

CONTEÚDO ABUSIVO

Tipo	Descrição
Spam	Envio massivo de mensagens não solicitadas
Discurso Nocivo	Perseguição ou descriminação, racismo ou ameaças
Exploração Sexual de Menores, Racismo e Apologia da Violência	Conteúdo ilegal conforme definido na Lei (portuguesa)

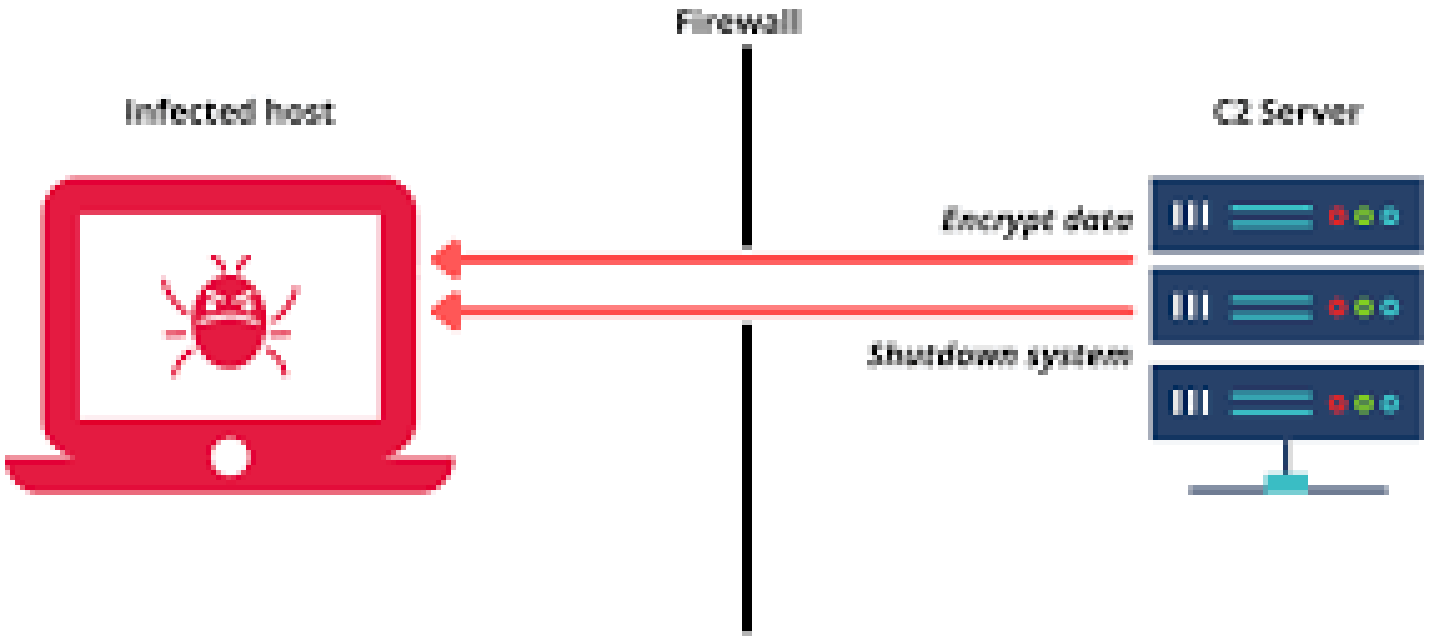
CONTEÚDO ABUSIVO: SPAM



CÓDIGO MALICIOSO

Tipo	Descrição
Sistema Infectado	Infecção com malware, comunicação com servidor de comando e controlo
Servidor C2	Servidor de comando e controlo
Distribuição de Malware	URL usado para distribuir malware, embebido em documentos ou enviado em mensagens
Configuração de Malware	Alojamento de ficheiros de configuração de malware ou código web para injecção de trojans

CÓDIGO MALICIOSO: SERVIDOR C2



RECOLHA DE INFORMAÇÃO

Tipo	Descrição
Scanning	Ataques dirigidos a descobrir vulnerabilidades, recolhendo informações sobre sistemas, serviços e contas. Recurso ao DNS, ICMP, SMTP e varrimento de portos
Sniffing	Observação e/ou gravação de tráfego de rede
Engenharia Social	Recolha de informações através de meios não técnicos

RECOLHA DE INFORMAÇÃO: SCANNING

```
kb@phoenixNAP:~$ nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-05 13:45 CEST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 26.51 seconds
```

TENTATIVA DE INTRUSÃO

Tipo	Descrição
Exploração de Vulnerabilidade	Tentativa de comprometer um sistema através da exploração de vulnerabilidades pré-identificadas (por exemplo CVEs)
Tentativa de Login	Múltiplas tentativas de login, seja num sistema ou numa aplicação
Nova Assinatura de Ataque	Ataque que usa a exploração de uma vulnerabilidade ainda desconhecida

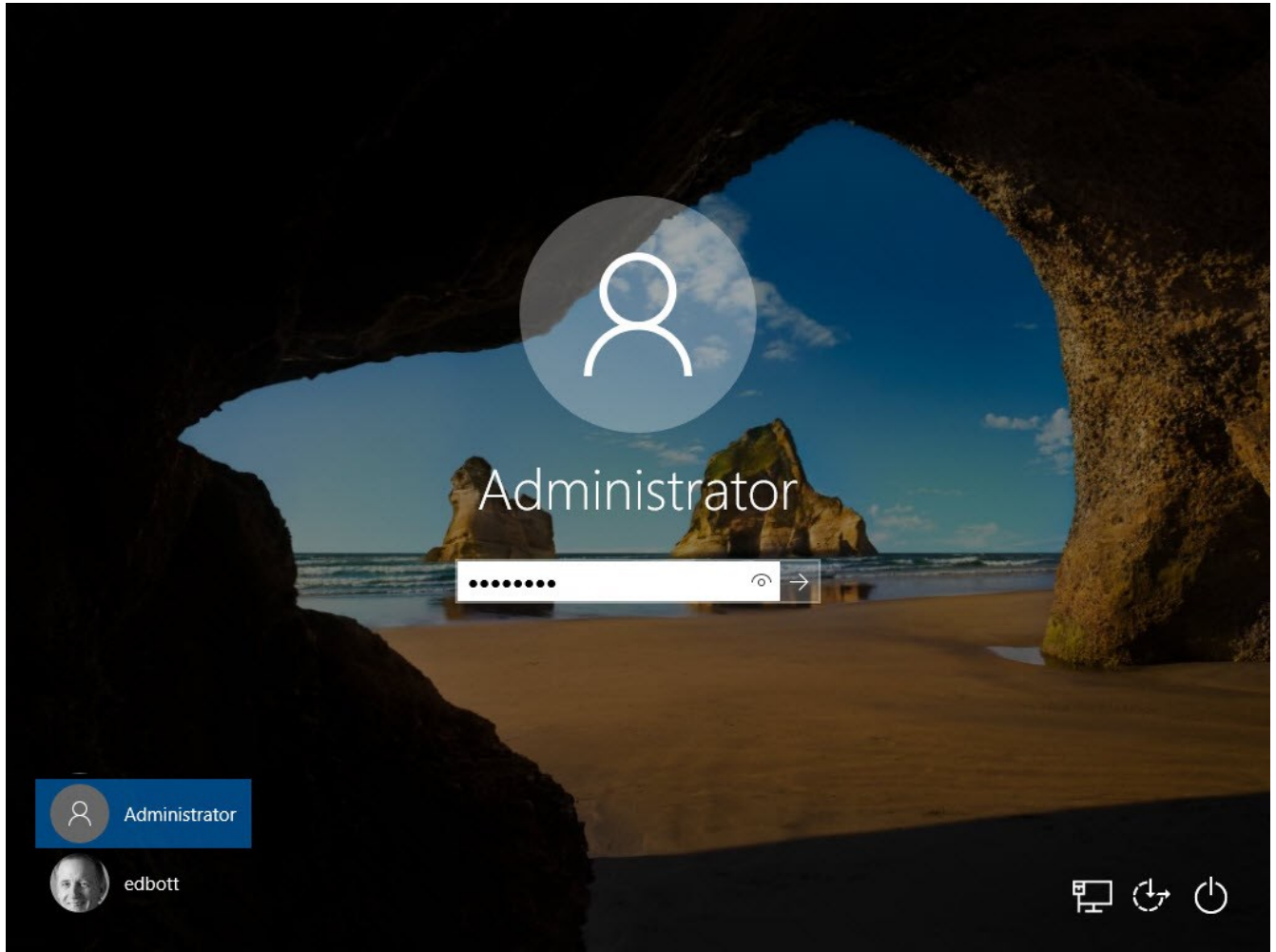
TENTATIVA DE INTRUSÃO: TENTATIVA DE LOGIN

```
Sep  6 22:46:44 digitalocean sshd[9154]: Failed password for root from 116.31.116.26 port 43769 ssh2
Sep  6 22:46:46 digitalocean sshd[9154]: Failed password for root from 116.31.116.26 port 43769 ssh2
Sep  6 22:46:49 digitalocean sshd[9154]: Failed password for root from 116.31.116.26 port 43769 ssh2
Sep  6 22:47:50 digitalocean sshd[9156]: Failed password for root from 116.31.116.26 port 60881 ssh2
Sep  6 22:47:52 digitalocean sshd[9156]: Failed password for root from 116.31.116.26 port 60881 ssh2
Sep  6 22:47:54 digitalocean sshd[9156]: Failed password for root from 116.31.116.26 port 60881 ssh2
Sep  6 22:49:00 digitalocean sshd[9158]: Failed password for root from 116.31.116.26 port 33436 ssh2
Sep  6 22:49:02 digitalocean sshd[9158]: Failed password for root from 116.31.116.26 port 33436 ssh2
Sep  6 22:49:04 digitalocean sshd[9158]: Failed password for root from 116.31.116.26 port 33436 ssh2
Sep  6 22:50:05 digitalocean sshd[9160]: Failed password for root from 116.31.116.26 port 32314 ssh2
Sep  6 22:50:06 digitalocean sshd[9160]: Failed password for root from 116.31.116.26 port 32314 ssh2
Sep  6 22:50:09 digitalocean sshd[9160]: Failed password for root from 116.31.116.26 port 32314 ssh2
Sep  6 22:51:15 digitalocean sshd[9162]: Failed password for root from 116.31.116.26 port 17181 ssh2
Sep  6 22:51:17 digitalocean sshd[9162]: Failed password for root from 116.31.116.26 port 17181 ssh2
Sep  6 22:51:19 digitalocean sshd[9162]: Failed password for root from 116.31.116.26 port 17181 ssh2
Sep  6 22:52:20 digitalocean sshd[9164]: Failed password for root from 116.31.116.26 port 32559 ssh2
Sep  6 22:52:22 digitalocean sshd[9164]: Failed password for root from 116.31.116.26 port 32559 ssh2
Sep  6 22:52:24 digitalocean sshd[9164]: Failed password for root from 116.31.116.26 port 32559 ssh2
Sep  6 22:54:24 digitalocean sshd[9170]: Failed password for invalid user admin from 37.48.93.217 port 40138 ssh2
Sep  6 22:54:26 digitalocean sshd[9172]: Failed password for root from 37.48.93.217 port 45600 ssh2
Sep  6 22:54:29 digitalocean sshd[9174]: Failed password for invalid user guest from 37.48.93.217 port 51124 ssh2
Sep  6 22:54:32 digitalocean sshd[9176]: Failed password for invalid user support from 37.48.93.217 port 55950 ssh2
Sep  6 22:54:35 digitalocean sshd[9180]: Failed password for invalid user user from 37.48.93.217 port 60862 ssh2
Sep  6 22:54:36 digitalocean sshd[9178]: Failed password for root from 116.31.116.26 port 37537 ssh2
Sep  6 22:54:37 digitalocean sshd[9182]: Failed password for invalid user admin from 37.48.93.217 port 38076 ssh2
Sep  6 22:54:38 digitalocean sshd[9178]: Failed password for root from 116.31.116.26 port 37537 ssh2
Sep  6 22:54:40 digitalocean sshd[9184]: Failed password for invalid user admin from 37.48.93.217 port 43454 ssh2
Sep  6 22:54:40 digitalocean sshd[9178]: Failed password for root from 116.31.116.26 port 37537 ssh2
```

INTRUSÃO

Tipo	Descrição
Comprometimento de Conta Privilegiada	Comprometimento de um sistema através de um utilizador com privilégios de administração
Comprometimento de Conta Não Privilegiada	Comprometimento de um sistema através de um utilizador sem privilégios de administração
Comprometimento de Aplicação	Exploração de vulnerabilidades conhecidas ou não
Comprometimento de Sistema	Logins com autenticação roubada bem sucedidos ou execução de comandos não autorizados
Arrombamento	Intrusão física

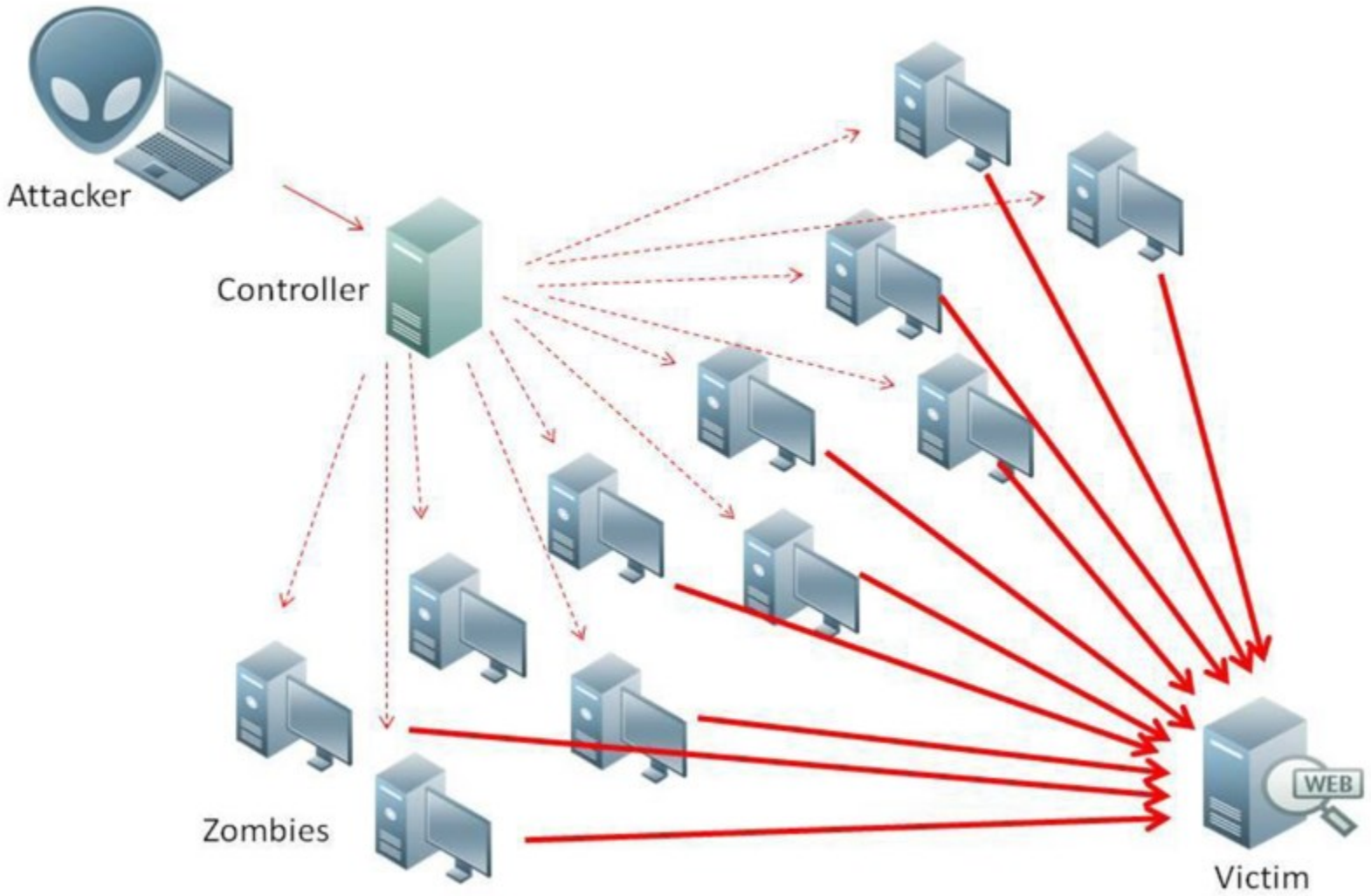
INTRUSÃO: COMPROMETIMENTO DE CONTA PRIVILEGIADA



DISPONIBILIDADE

Tipo	Descrição
Negação de Serviço	Ataque com intuito de causar degradação ou indisponibilidade, enviando por exemplo pedidos em excesso
Negação de Serviço Distribuída	Ataque distribuído com intuito de causar indisponibilidade (syn flods, amplificação, etc)
Configuração Incorrecta	Erros ou falhas de manutenção
Sabotagem	Acções intencionais que causam danos
Interrupção	Provocada por falha de equipamento ou desastre natural

DISPONIBILIDADE: NEGAÇÃO DE SERVIÇO DISTRIBUÍDA



SEGURANÇA DA INFORMAÇÃO

Tipo	Descrição
Acesso Não Autorizado	Obter informação sem ter o devido acesso, pelo uso de credenciais roubadas; intercepção de tráfego
Modificação Não Autorizada	Uso de credencias roubadas para aceder a um sistema; encriptação (ransomware); defacements
Perda de Dados	Perda de informação causada por falha provocada ou roubo físico
Exfiltração de Informação	Obtenção de credenciais, dados pessoais ou informação não pública

SEGURANÇA DA INFORMAÇÃO: MODIFICAÇÃO NÃO AUTORIZADA

FRAUDE

Tipo	Descrição
Utilização Indevida ou Não Autorizada de Recursos	Uso de recursos de terceiros de forma não autorizada, incluindo para fins lucrativos
Direitos de Autor	Distribuição ou instalação de software comercial não licenciado ou conteúdos protegidos por direitos de autor
Utilização de Nome de Terceiros	Impersonificação de outra entidade com o objectivo de daí retirar benefícios
Phishing	Tentativa de obtenção de credenciais alheias

FRAUDE: PHISHING

VULNERABILIDADE

Tipo	Descrição
Criptografia Fraca	Serviços acessíveis a permitir o uso de criptografia fraca
Amplificador DDoS	Serviços passíveis de amplificar ataques DDoS
Serviços Acessíveis Potencialmente Indesejados	Serviços publicamente acessíveis que não deveriam estar expostos (Telnet, RDP, VNC, …)
Revelação de Informação	Serviços publicamente acessíveis expondo informação sensível (SNMP, etc)
Sistema Vulnerável	Sistema exposto a certos ataques; desactualizado ou com configurações permissivas

VULNERABILIDADE: CRIPTOGRAFIA FRACA

OUTRO

Tipo	Descrição
Sem Tipo	Incidentes que não encaixam em nenhum dos tipos previamente descritos
Indeterminado	Classificação desconhecida/indeterminada

TESTE

Tipo	Descrição
Teste	Destinado a testes

WORDWALL

wordwall.net/resource/94768524

IDEIAS CHAVE

- É necessária uma uniformização entre várias equipas na classificação dos incidentes para se estabelecer um quadro situacional coerente
- Existem tipos de incidentes mais frequentes e outros mais raros
- As classificações «Sem Tipo» ou «Indeterminado» são de evitar

Questões?

Obrigado.

csirt.fct.pt/podcast

csirt.fct.pt/mooc

csirt.fct.pt/etc